chapter 3

BULGING DIMENSIONS OF CYBER TERRORISM

3.1 Introduction

Information is power\(^1\). Now it has become reality. Each new technology has its own setbacks in the form of misuse of it. History has seen the use of technology to illicitly appropriate funds, as a tool to aid in illegal practices, and more recently to take forms of derisory discourse in to a virtual arena. Less is known about other forms of deviance that manifest with increasingly populated online environments\(^2\).

The concept of cyber terrorism is that terrorism activities that are carried out entirely in the virtual world. The Internet provides ample of opportunities and ways of anonymously meeting with ‘like minded’ individuals in a (comparatively) safe way\(^3\). Furthermore, a successful cyber terrorism event could require no more prerequisite than knowledge something that is essentially free to the owner once acquired, and an asset that can be used over and over again. Thus, it would be possible that such an environment could facilitate the creation of entirely new terrorist groups, no money is would be required for actions, and members could organize themselves quickly and easily in the anonymity of cyberspace. This is very different from, certain examples given previous chapter, where the computer


can aid the task of the terrorist, but ‘real’ resources are still required to execute the plan. It is this cyber terrorism that most writers mean when they discuss the dangers posed by the cyber terrorist, and this compartmentalization poses a significant barrier to our ability to protect ourselves\(^4\).

The role of computer with respect to terrorism is that of modern thief who can steal more with a computer than a gun. The terrorist may be able to do more damage with a keyboard than with a bomb. As sequel to 11\(^{th}\) September, an intense growth in cyber crimes particularly crimes against property and national might see a substantial increase. Also, an increase in cyber war activities is quite likely, as in the 21\(^{st}\) century wars will be fought on the internet and in cyber space rather than in the real world. Another area might be a transformation in the rules of the games and the way cyber war and cyber terrorism is going to be perceived, over a period of time\(^5\).

Generically, cyber terrorism has been defined as the use of computers and the Internet to engage in terrorist activity\(^6\). On the other hand, it is well settled that cyber terrorist used computer and internet for their unlawful activities and to intimidate the government according to their policy. So it is necessary for better understanding of cyber terrorism, to understand first some related terms.

\(^4\) Ibid.
3.2 Terms Related to the Cyber Terrorism

3.2.1 Terrorism

There is neither an academic nor an international legal consensus regarding the definition of the term ‘terrorism’\(^7\). Various legal systems and government agencies use different definitions of ‘terrorism’. Moreover, the international community has been slow to formulate a universally agreed upon, legally binding definition of this crime. These difficulties arise from the fact that the term ‘terrorism’ is politically and emotionally charged\(^8\).

Terrorism has defined by many scholars and statutes, but there is no consensus on it. According to L. Ali Khan,

“Terrorism sprouts from the existence of aggrieved groups. These aggrieved groups share two essential characteristics: they have specific political objectives, and they believe that violence is an inevitable means to achieve their political ends. The political dimension of terrorist violence is the key factor that distinguishes it from other crimes”.\(^9\)

Daniel D. Novotny defined terrorism,

“An act is terrorist if and only if

---


i. it is committed by an individual or group of individuals privately, i.e., without the legitimate authority of a recognized state;

ii. it is directed indiscriminately against non-combatants;

iii. the goal of it is to achieve something politically relevant;

iv. this goal is pursued by means of fear-provoking violence.”

Section 3 of The Prevention of Terrorism Act, 2002\(^1\) has defined and gives the provisions, who is terrorist and punishment for the act of terrorism-

3. Punishment for terrorist acts-

(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 does any act or thing by using bombs, dynamite or other explosive substances or inflammable substances or firearms or other lethal weapons or poisons or noxious gases or other chemicals or by any other substances (whether biological or otherwise) of a hazardous nature or by any other means whatsoever, in such a manner as to cause, or likely to cause, death of, or injuries to any person or persons or loss of, or damage to, or destruction of, property or disruption of any supplies or services essential to the life of the community or causes damage or destruction of any property or equipment used or intended to be used for the defence of India or in connection with any other purposes of the Government of India, any State Government or any of their agencies, or detains any person and threatens to kill or injure such person in order to

---


\(^{11}\) Section 3, The Prevention of Terrorism Act, 2002.
compel the Government or any or her person to do or abstain from
doing any act;

(b) is or continues to be a member of an association declared unlawful
under the Unlawful Activities (Prevention) Act, 1967 (37 of 1967 ), or
voluntarily does an act aiding or promoting in any manner the objects
of such association and in either case is in possession of any unlicensed
firearms, ammunition, explosive or other instrument or substance
capable of causing mass destruction and commits any act resulting in
loss of human life or grievous injury to any person or causes significant
damage to any property, commits a terrorist act.

Explanation - For the purposes of this sub-section, ‘a terrorist act’ shall
include the act of raising funds intended for the purpose of terrorism.

(2) Whoever commits a terrorist act, shall,-

a. if such act has resulted in the death of any person, be punishable
with death or imprisonment for life and shall also be liable to fine;
b. in any other case, be punishable with imprisonment for a term which
shall not be less than five years but which may extend to
imprisonment for life and shall also be liable to fine.

(3) Whoever conspires or attempts to commit, or advocates, abets, advises
or incites or knowingly facilitates the commission of, a terrorist act or
any act preparatory to a terrorist act, shall be punishable with
imprisonment for a term which shall not be less than five years but
which may extend to imprisonment for life and shall also be liable to
fine.

(4) Whoever voluntarily harbours or conceals, or attempts to harbour or
conceal any person knowing that such person is a terrorist shall be punishable with imprisonment for a term which shall not be less than three years but which may extend to imprisonment for life and shall also be liable to fine: Provided that this sub-section shall not apply to any case in which the harbour or concealment is by the husband or wife of the offender.

(5) Any person who is a member of a terrorist gang or a terrorist organization, which is involved in terrorist acts, shall be punishable with imprisonment for a term which may extend to imprisonment for life or with fine which may extend to rupees ten lakh or with both.

Explanation - For the purposes of this sub-section, ‘terrorist organization’ means an organization which is concerned with or involved in terrorism.

(6) Whoever knowingly holds any property derived or obtained from commission of any terrorist act or has been acquired through the terrorist funds shall be punishable with imprisonment for a term which may extend to imprisonment for life or with fine which may extend to rupees ten lakh or with both.

(7) Whoever threatens any person who is a witness or any other person in whom such witness may be interested, with violence, or wrongfully restrains or confines the witness, or any other person in whom the witness may be interested, or does any other unlawful act with the said intent, shall be punishable with imprisonment which may extend to three years and fine.

The U.S. Code includes the following definition in Title 22, Chapter 38

“Premeditated, politically motivated violence perpetrated against
noncombatant targets by sub-national groups or clandestine agents.”

Title 18 of the U.S. Code (regarding criminal acts and criminal procedure) defines international terrorism as:

The term ‘international terrorism’ means activities that

A. involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State;

B. appear to be intended
   i. to intimidate or coerce a civilian population;
   ii. to influence the policy of a government by intimidation or coercion; or
   iii. to affect the conduct of a government by mass destruction, assassination, or kidnapping; and

C. occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum.

The U.S. Code of Federal Regulations defines terrorism as “the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of

---

political or social objectives.”

Most definitions used by the United States include a variation on two elements:

1. an act of violence; and
2. the attack must be political in nature, seeking to influence governmental decisions;

with some including requirements that the attack must be aimed at civilians or non-belligerents, and/or be conducted by non-state actors. There is sufficient distinction among the cyber terrorism and terrorism so need not be precisely defined. On the other hand the basic elements contained by these two terms needs to be understood. These factors are discussed below.

The very first factor, commonly used that there must be some act which is violent in nature or dangerous to human life. There is no straight jacket formula or measurement relating to the determination of level of violence to qualify terrorism, but it is commonly accepted that that if the violent act intimidate the population at large, not just the subject of the attack. The very character of creating and spreading fear amongst the general public is known as the heart of the terrorism. It is what creates the terror. This very characteristic will be important to understand and examining what type of computer network attack has enough effect on the population to be considered an act of cyber terrorism.

The second factor is that the aim of the attack should be political in nature.

---

14 28 C.F.R. S. 0.85(l).
15 Supra Note 8. p. 34.
Its main objective is to influence a government to accept the unlawful demands through violent actions\textsuperscript{18}. Even though there are several other crimes, having the characteristics of violence except political motivation, some of them are murder and mayhem\textsuperscript{19}. Terrorist organizations typically have defined motivations and stated end goals, such as Al-Qaeda, which advocates for the withdrawal of western nations from the middle-east and the establishment of a global Islamic caliphate.\textsuperscript{20} There are various methods being used by the terrorists for spreading violence and terror, e.g., bomb, chemical/biological weapon, or other violent attack\textsuperscript{21}. This fear and threat of further violence is used by the terrorists to meet the unlawful ends and to motivate a government to change its policy according to the intended plans and aims of the terrorist organization\textsuperscript{22}.

The third factor found places in very few definitions of the terrorisms, requires non-belligerents outside the scope of a military conflict to conduct the violence\textsuperscript{23}. When there is direct violence or attack on the military by the terrorists in not considered as terrorism\textsuperscript{24}. Attacks against the military within the scope of a conflict conducted by belligerents are generally considered acts of warfare, even if

\begin{itemize}
  \item \textsuperscript{18} 18 ibid.; and 50 U.S.C. S. 1801(c)(2) (2006) (including a requirement the act intends (A) to intimidate or coerce a civilian population; (B) to influence the policy of a government by intimidation or coercion; or (C) to affect the conduct of a government by assassination or kidnapping).
  \item \textsuperscript{19} 18 U.S.C. S. 1111 (2006). (defining murder generally as the unlawful killing of a human being with malice aforethought).
  \item \textsuperscript{22} Pippa Norris, Montague Kern, & Marion Just, Framing Terrorism: The News Media, the Government and the Public, eds., pp. 3 & 8, Psychology Press, London, UK, 1st ed. 2003. (generally discussing news coverage of terrorism and how it frames public discussion of terrorism).
  \item \textsuperscript{24} 22 U.S.C. S. 2656f (d) (2) (2006) (defining terrorism as “premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents”).
\end{itemize}

101
they mimic terrorist attacks. Examples of attacks on military outside the scope of a conflict include the 9/11 attack on the Pentagon and the 1996 bombing of the Khobar Towers complex in Saudi Arabia and attack on the Indian Parliament in 2001. Cyber attacks against military forces as part of a broader conflict is covered below under the category of armed attack in cyberspace.

Terrorism and the internet are interrelated. The internet has become a forum for terrorist groups and individual terrorists spread their messages of hate and violence and to communicate to the same. Individuals and groups have tried to attack computer network, including these on the internet what had become known as cyber terrorism. Terrorists are using the internet more than they are attacking it. Terrorists use encrypted email to plan acts of internet sites of terrorist group seek to achieve political and ideological agendas. The fear surrounding cyber terrorism is that terrorists and criminals penetrate infrastructure, computer system and endanger human lives by disrupting military networks, telecommunications, etc. A cyber terrorist may be in the system several times before the act takes place for reconnaissance or experimentation.

The dark clouds of stealth and in cognition engulf cyber terrorism, which is the newest face of terror, and it is said that a new breed of terrorism is on the

---

rise\textsuperscript{31}. Given the evolving definitions of the broader categories, it is no surprise that definitions of cyber terrorism have been equally divergent\textsuperscript{32}. The term implies two elements: cyber and terrorism. Both of these are regarded as the two great fears of the late 20\textsuperscript{th} century. Both imply fear of unknown. Fear of random, violent victimization segues well with the distrust and outright fear of computer technology\textsuperscript{33}. Public debates and law makers are waiting for a major cyber attack on information infrastructure for defining and addressing the cyber terrorism. At the same time, without waiting any cyber attack, a minimum legal framework is required which helps to prevent, deter, and defend against a cyber terrorist act.

Many international terrorist groups now actively use computers and the Internet to communicate, and several may develop or acquire the necessary technical skills to direct a coordinated attack against computers\textsuperscript{34}. While there is no published evidence that terrorist organizations are currently planning a coordinated attack against computers, computer system vulnerabilities persist worldwide, and initiators of the random cyber attacks that plague computers on the Internet remain largely unknown. Reports from security organizations show that random attacks are now increasingly implemented through use of automated tools, called “bots”, that direct large numbers of compromised computers to launch attacks through the Internet as swarms\textsuperscript{35}. The growing trend toward the use of more automated attack tools has also overwhelmed some of the current methodologies used for tracking Internet cyber attacks.

\textsuperscript{32} Mohammad Iqbal, “Defining Cyberterrorism”, p. 397, 22 J. Marshall J. Computer & Info. L., 2004. (exploring the different definitions of Cyberterrorism that have been suggested).
\textsuperscript{34} Supra Note 6.
\textsuperscript{35} Ibid.
3.2.2 Computer Network Attack

Computer network attack (CNA) used in very broad way and it included any unauthorized access, or exceeding of one’s access, to an information system that results in damage, enables potential future damage, or allows for future unauthorized access to information, on any information system. Computer network attack is a broad term which tries to cover the complete range of malicious activity that a perpetrator may take against an information system.

The Department of Defence defines Computer Network Attack as

“actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.”

The definition excludes using information systems to collect intelligence, which the DoD defines as Computer Network Exploitation (CNE).

A computer network attack may be defined as actions directed against computer systems to disrupt equipment operations, change processing control, or corrupt stored data. Different attack methods target different vulnerabilities and involve different types of weapons, and several may be within the current capabilities of some terrorist groups. Three different methods of attack are identified in this report, based on the effects of the weapons used. However, as

---

36 Ibid.
38 Ibid.
40 “Information Warfare and Cyberwar: Capabilities and Related Policy Issues.” CRS Report RL31787. All methods of computer attack are within the current capabilities of several nations.
technology evolves, distinctions between these methods may begin to blur.

A computer network attack (CNA), usually involves malicious code used as a weapon to infect enemy computers to exploit a weakness in software, in the system configuration, or in the computer security practices of an organization or computer user. Other forms of CAN are enabled when an attacker uses stolen information to enter restricted computer systems.

While Computer Network Attack and Electronic Attack threats are less likely than physical attacks, they could actually prove more damaging because they involve disruptive technologies that might generate unpredictable consequences or give an adversary unexpected advantages.

3.2.3 Electronic Attack (EA)

Electronic attack, most commonly referred to as an Electromagnetic Pulse (EMP), disrupts the reliability of electronic equipment through generating instantaneous high energy that overloads circuit boards, transistors, and other electronics. EMP effects can penetrate computer facility walls where they can penetrate...
erase electronic memory, upset software, or permanently disable all electronic components. Some assert that little has been done by the private sector to protect against the threat from electromagnetic pulse, and that commercial electronic systems in the United States could be severely damaged by limited range, small-scale or portable electromagnetic pulse devices. Some military experts have stated that the few countries, including United States are perhaps the nation most vulnerable to electromagnetic pulse attack.

3.2.4 Information System

Information system is an integrated set of components for collecting, storing, and processing data and for delivering information, knowledge, and digital products. Business firms and other organizations rely on information systems to carry out and manage their operations, interact with their customers and suppliers, and compete in the marketplace. For instance, corporations use information systems to reach their potential customers with targeted messages over the Web, to process financial accounts, and to manage their human resources. Governments deploy information systems to provide services cost-effectively to citizens. Digital goods, such as electronic books and software, and online services, such as auctions and social networking, are delivered with information systems. Individuals rely on information systems, generally Internet-based, for conducting much of their personal lives, for socializing, study, shopping, banking, and


48 Ibid.
In other words, information system is any machine, network, or electronic device that contains stored information or is capable of processing data. Hardware systems are primarily composed of computers. For better understanding US Code has given it meaning and components as:

“an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.”

Cyberspace includes any form of network those hardware systems operate on, and is defined by the DoD as the

“global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”

Cyber terrorists needs no internet access for committing the terrorist attack on the information structure, because latest attacks on Unites States using thumb drives, has proved it. For the security reasons many critical infrastructure

---

50 18 U.S.C. S.1030(e) (1)
components and computers are deliberately not connected to the Internet as a safety and security reason, even though they remain vulnerable to cyber attack.\(^{53}\)

### 3.2.5 Critical Infrastructure\(^{54}\)

The systems and networks that make up the infrastructure of society are often taken for granted, yet a disruption to just one of those systems can have dire consequences across other sectors.\(^{55}\) The precise definition of critical infrastructure is given by the Critical Infrastructures Protection Act of 2001:

> “systems and assets, physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters.”\(^{56}\)

This is very precise definition of critical infrastructure and it generally includes the primary repositories of economic data, power grid, air traffic control, telecommunication lines and towers, port controls.\(^{57}\)

Last decades of 20\(^{th}\) century and 21\(^{st}\) century witnessed the unexpected

---


\(^{54}\) See Chapter 4.


advancement in the information technology system. The dependency of critical infrastructures on the information technology and internet is increasing. As all the sectors of government and private companies become more efficient in the operations of critical infrastructure, these components become increasingly dependent on computer controls and networks for their operation. This increasing dependency on computer systems made it more vulnerable to cyber attack. Recently, the Government of India, through the Ministry of Information and Technology has taken an increased role in protection of critical infrastructure information systems by announcing National Cyber Security Policy, 2013.

3.2.6 Cyber Attack

A computer network attack, or cyber attack, disrupts the integrity or authenticity of data, usually through malicious code that alters program logic that controls data, leading to errors in output. Computer hackers opportunistically scan the Internet looking for computer systems that are mis-configured or lacking necessary security software. Once infected with malicious code, a computer can be remotely controlled by a hacker who may, via the Internet, send commands to spy on the contents of that computer or attack and disrupt other computers.

Cyber attacks usually require targeted computer have some pre-existing system flaw, such as a software error, a lack of antivirus protection, or a faulty system configuration, for the malicious code to exploit. However, as technology evolves, this distinguishing requirement of computer network attack may begin to fade. For example, some forms of electronic attack can now cause effects nearly identical to some forms of computer network attacks. For example, at controlled

power levels, the transmissions between targeted microwave radio towers can be hijacked and specially designed viruses, or altered code, can be inserted directly into the adversary’s digital network\(^{59}\).

### 3.3 Evolution of Cyber Terrorism

Cyber terrorism can be traced from June 1944 attack on the communication lines and logistic support of Germany. From 1945 the end of Second World War to 1991 the two super powers started to influence other nations through their dominant military force. It is known as cold war. The two ‘super powers’ were (1) the United States of America (USA) and (2) the Soviet Union\(^{60}\).

By that time in 1960s to 1980s hackers took their own shape in Information Super Highway, in 1986, West German hackers accessed Department of Defense Systems of the USA. In 1988 Osama Bin Laden established ‘AL-Qaeda’ based on ‘Jihad’. Thereafter, ‘Gulf War’ was first Information War or I-war through Information Way or I-way. The USA passed the National Infrastructure Protection Act, 1990 to control cyber terrorism. In Europe the I-way become popular in the year 1998. The United Kingdom (UK) established the Defense Evaluation and Research Agency in the year 1998. Then Sweden, Norway Finland, Switzerland, Germany, France came forward to combat cyber war.

By 1990 Internet became popular through World Wide Web (WWW). World Wide Web become very popular in India in 1995 but before that LTTE

\(^{59}\) David Fulghum, “Network Wars,” *Aviation Week & Space Technology*, p.91, Oct. 25, 2004. Some forms of EA are intended to overpower a radio transmission signal to block or “jam” it, while other forms of EA are intended to overpower a radio signal and replace it with a substitute signal that disrupts processing logic or stored data.

groups work was depend on website and Internet. In the era of information and communication technology almost all countries internet networks, fax networks and radio waves were notified about the possible conspiracy programme of terrorists against government. In India LTTE group’s works depend mostly on network, websites and internet connectivity. Aftab Ansari’s attack on American Centre, Kolkata was based on their organization through internet and websites. Even from Dubai he was able to communicate with his group. Therefore, in the contemporary communication convergence era cyber terrorism has become the most complex and national as well as an international problem.

Terrorists have moved into cyberspace to facilitate traditional forms of terrorism such as bombing. They use the Internet to communicate co-ordinate events and advance their agenda. While such activity does not constitute cyber terrorism in the strict sense, it does show that terrorists have some competency in using the new information technologies.

Cyber terrorism is a phrase used to describe the use of Internet based attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses.  

There are two concepts of cyber terrorism;

i. When terrorist use information technology to attract their audience by creating violence, through defacement of web site, denial of service attack, hacking, cracking, tampering source code, flowing viruses etc. where computer is used as target or weapon and which go against Government or national security.

Another is terrorized use of information technology i.e., cyber pornography, cyber fraud, cyber theft, spamming etc. which causes terror or threat in the mind of people. Here the new technology is also tool of terrorism.

3.4 Definitions and Analysis of Cyber Terrorism

Cyber terrorism and the misuse of Internet for terrorist purposes represent a serious threat, since many essential aspects of today’s society are completely dependent upon the functioning of computer systems and the Internet. The trends of the recent past shows that politically motivated hacking groups have increased. These groups are more equipped and daring to commit a sophisticated in their attacks. There is no hesitation to assume that these kinds of groups also enjoy the gray area of Internet for their unlawful motives and as an instrument of terror. Use of Internet as a weapon to spread the terror and vindicate the government is cheap, unidentified, and universal. On the other hand States are becoming more reliant on information technology to manage and control critical infrastructure, both physical and informational.

Barry C. Collin, a senior research fellow at the Institute for Security and Intelligence in California, in the 1980s gave the original definition of cyber


63 Ibid.

64 Supra Note 6, Clay Wilson, (arguing that given the confluence of the United States’ overwhelming military superiority, and its reliance on technology, future adversaries are likely to attempt acts of Cyberterrorism).

terrorism. He analyzed cyber terrorism as one in which attacks conducted through computers mirrored the effects of traditional acts of terrorism.\textsuperscript{66}

The traditional form of terrorism has changed its shapes and now the terrorists are using the latest technology to break into subway computer systems to cause a collision or use computers to tamper with power grids or food processing. Unlike, the traditional methods of suicide bombers and roof-top snipers have changed with the new technology. Now cyber terrorists attack can be completed from the comfort of home and can attack more than one target at a time worldwide by using cyberspace. Cyber terrorism can be far more damaging, and far more violent, than a fighter lane attack. The ease and low cost of cyber terrorism combine to offer an attractive tool for once-conventional sociopaths.\textsuperscript{67}

The definitions of cyber terrorism are based on two general factors: effects and intent.\textsuperscript{68} The current definitions are based on only one factor or neglect the other factor of cyber terrorism. With the help of below given definition for cyber terrorism try to understand the real nature and factors consisted by it.

Information Technology (Amendment) Act, 2008\textsuperscript{69} define and give the provision punishment for cyber terrorism,

Section 66F

(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

\textsuperscript{66} Supra Note 32.
\textsuperscript{67} Supra Note 7
\textsuperscript{68} Supra Note 6.
\textsuperscript{69} Section 66F the Information Technology Act, 2000.
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 authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons for the security of the State or foreign relations, or any restricted information, data or computer database, 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.

Cyber terrorism is sometimes referred to as electronic terrorism or information war. The deliberate, large-scale disruption of networks of computers, especially of personal computers attached to the Internet, by means of viruses etc.

Therefore, cyber terrorism may be defined as use of computer as weapon or target to cause violence to population or which go against national interest and Government’s computer system.

In USA, though not explicitly defined as cyber terrorism, a form of it is contained in the U.S. Code. 18 U.S.C. § 2332B(g)(5) defines the federal crime of terrorism and includes as predicate offenses two Computer Fraud and Abuse Act, 2006 (hereinafter CFAA) provisions, one relating to cyber-espionage and one related to computer damage. If one of those two CFAA provisions is violated, and if that CFAA violation ‘is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct, then it meets this definition of terrorism.

In this definition of cyber terrorism motivational element has cover in the federal crime of terrorism. However, it fails to sufficiently define the scope of the attack’s effects. Despite this recognition of cyber terrorism in the criminal code, most government agencies have developed their own definitions of cyber terrorism.

70 18 U.S.C. S. 1030 (a) (1) (relating to cyber-espionage); and 18 U.S.C. S. 1030(a)(5)(A) resulting in damage as defined in 18 U.S.C. S. 1030(c)(4)(A)(i)(II) through (VI) (requiring damage to national security related computers or if the damage involves 10 or more computers).
The Federal Emergency Management Agency (FEMA) has defined cyber terrorism as

“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.”72

This definition incorporates an adequate intent element that appears in most definitions of terrorism and cyber terrorism alike. It requires the attacker’s objective to be political or social coercion against a government or its people. The weakness of this definition again comes in the effects element, making no requirement as far as scale of attack goes. Under this definition, the lone wolf who hacks a web-page to post a political message, such as ‘Stop the War in Iraq’73 or temporarily takes down a Department of Justice public website to protest an arrest would be guilty of cyber terrorism.

The National Infrastructure Protection Center (NIPC) defines Cyber terrorism as

“a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies.”74

74 Ron Dick, “The Truth about Cyberterrorism”, NIPC. Scott Berinato, March 15,2002,
This definition of cyber terrorism focuses more on the effects of a test, with the result that it is extremely narrow. It can be said that this definition is unnecessary because all the factors has already covered by definitions of terrorism. In a definition of cyber terrorism there are certain key factors must be included, for example, takedown of economic systems or corruption of massive amounts of national security data, as this is where the unique capabilities of cyber terrorism lie.

William L. Tafoya, writing in the FBI Law Enforcement Bulletin, defines cyber terrorism as

“the intimidation of civilian enterprise through the use of high technology to bring about political, religious, or ideological aims, actions that result in disabling or deleting critical infrastructure data or information.”

Here Tafoya has given good effect approached definition of cyber terrorism while using the computer and disable or delete the critical information of any nation and the purpose is to intimidate the government according to the policy of cyber terrorists. However, any definition of cyber terrorism should similarly include attacks on critical data systems.

The United Nations Counter-Terrorism Implementation Task Force (CTITF), not directly using the term cyber terrorism, but pointed out the ways of any terrorist groups may

“use of the Internet to perform terrorist attacks by remotely altering


76 Ibid.
information on computer systems or disrupting the flow of data between computer systems.”\textsuperscript{77}

The UN CTITF explains: \textsuperscript{78}

“any cyber attack qualifying as ‘terrorist’ would ultimately still have to cause damage in the ‘real world’: for example, by interfering with a critical infrastructure system to the extent of causing loss of life or severe property damage. However, as dependence on online data and services increases, an attack that resulted only in widespread interruption of the Internet could, in future, cause sufficient devastation to qualify as a terrorist attack. However, categorizing such attacks as terrorist remains controversial. The damage resulting from such attacks, while potentially economically significant, to date their impact has been more on the level of a serious annoyance.”

This definition of the United Nations Counter-Terrorism Implementation Task Force (CTITF) gives very wide meaning and definition of cyber terrorism. It does an excellent job of recognizing that not only should violent attacks be included, but attacks on data may also serious enough to rise to the level of terrorism.

Activists in Pakistan have come heavily on an ordinance to curb electronic crime. The government’s move of prohibiting the use of internet and SMS is being seen as curtailment of freedom of expression and civil liberties. An ordinance introduced to curb electronic crime has come under criticism for clauses that seem


\textsuperscript{78} Ibid.
to be aimed at censoring free speech and cutting civil liberties\textsuperscript{79}. The government claims that the main objective of this new law is to increase security, safety and protection for those segments of society that use or deal with information technology (IT).

Cyber terrorism has been defined by ordinance thus:

“Any person, group or organization who, with terrorist intent utilizes, accesses or causes to be accessed a computer or computer network or electronic or electronic device or by any available means, and thereby knowingly engages in or attempts to engage in a terrorist act commits the offence of cyber terrorism.”\textsuperscript{80}

The ordinance also declares the sending of unsolicited short messages over cell phones (SMSs), pictures taken without the permission of the person photographed, and e-mails carrying obscene material as cyber crimes. The law gives officers of the Federal Investigation Agency (FIA) full powers to confiscate equipment and arrest anyone who is deemed by the government to be acting against the ‘integrity of Pakistan’ or having terrorist intent, says Asif Bhatti, a software engineer based in Lahore. But many believes that in reality the new law will be used to crack down on free expression on the internet because it prohibits the use of internet and cell phones to criticize authorities or send out calls for rallies. Blog sites and short messaging service were used extensively by Pakistanis inside the country and abroad to condemn the imposition of a state of emergency, gagging of independent media and other ‘unconstitutional’ acts of the Musharraf


\textsuperscript{80} Ibid.
Their use increased exponentially after the government imposed restrictions on electronic channels through certain amendments in the Pakistan Electronic Media Regulatory Authority Ordinance in June, 2006. The new Ordinance has been criticized by human rights bodies, business community and citizen group as a piece of legislation that has too many loopholes for misuse. In a statement, the South Asian Free Media Association (SAFMA) said that,

“against the backdrop of the use of internet and cell phones to criticize authorities or send calls for rallies, the ordinance is liable to be interpreted as drastic measure, aimed at putting curbs on civil rights.”

Security expert Dorothy Denning, describe cyber terrorism in academic form in these words:

Cyber terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean 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. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their

---

81 Ibid.
82 Dorothy E. Denning, “Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism”, Committee on Armed Services, U.S. House of Representatives, Available on http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf, Retrieved on 12 March 2010. (arguing that a definition of Cyberterrorism should involve a component of violence or harming of critical infrastructure, and that, at the time, it was mostly theoretical but could arise in the future).
impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

The Center for Strategic and International Studies (CSIS) defined Cyber terrorism as

“the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population.” \(^{83}\)

Kelly Gable provided a similar definition, including “efforts by terrorists to use the Internet to hijack computer systems, bring down the international financial system, or commit analogous terrorist actions in cyberspace.” \(^{84}\) Kelly’s definition of cyber terrorism focuses mainly on the international finance system, but it ignored the critical infrastructure. This definition is useful in for the purpose of that any disturbance into the financial system can cause drastic effects on the sovereignty of a nation.

The concept of cyber terrorism is complex. There are implications regarding the definition of cyber terrorism. Ballard et. al., discuss some of the issues related to the definition of cyber terrorism. They present three points that may explain the difficulty in defining cyber terrorism. First, because the technology develops so rapidly the operational definition of cyber terrorism may change\(^{85}\).

Second, the definition of cyber terrorism may be biased because of

\(^{83}\) Supra Note 58.


researchers’ personal perspectives as to what cyber terrorism is. They may define cyber terrorism based solely on their specialized areas of expertise. Finally, there might be legitimate concerns regarding the validity, reliability, and accuracy of the research.

By stating, “no single or globally accepted definition of terrorism exists” indeed Ballard et. al., indicate the difficulty of defining cyber terrorism in the first place. Nevertheless, they identified three different methods used by researchers to define cyber terrorism:

i. adapting the existing definition of terrorism to define cyber terrorism,

ii. using the existing laws and authorities to define what actions represent cyber terrorism, and

iii. defining cyber terrorism by using specific actions.

Conway, in her article, “What Is Cyber terrorism?” defines the cyber terrorism as “premeditated, politically motivated attacks by sub-national groups or clandestine agents against information, computer systems, computer programs, and data that result in violence against noncombatant and targets.” By this definition, Conway excludes cybercrime activities, including stealing credit card information, sending emails having pornographic content, or hacking a web site. Some researchers in this area characterize an act as cyber terrorism only if the act results in destruction, death, and/or injury, and creates fear among the public. Furthermore, some also claim that we have not witnessed the destructive aspect of

86 Id.
87 Ibid.
88 Ibid. p-992-993.
89 Ibid p. 436.
cyber terrorism yet, and therefore, they suggest that cyber terrorism does not exist at all\textsuperscript{91}.

In terms of witnessing cyber terrorism, the claim might be considered to be an accurate one; however, there is also evidence indicating that terrorist organizations have been considering attacking information infrastructures and other communication networks by engaging in cyber terrorism\textsuperscript{92}. Brenner and Goodman strongly assert “the fact that cyber terrorism is a real possibility, if not an imminent probability…and … it is necessary to consider both the threat level of the target and the sophistication of the perpetrator.”\textsuperscript{93}

Also, FEMA reveals the distinction between cybercrime and cyber terrorism (2002).

Cyber terrorism is distinct from computer crime, economic espionage, and ‘hacktivism’ although terrorists may employ any of these forms of computer abuse to further their agendas. The weapons of cyber terrorism computers differ from weapons of mass destruction such as biological agents, chemical agents, and radiological agents in that they don’t directly cause death and injury.

However, acting indirectly, they can cause serious consequences to individuals, businesses, industry, government, and the public at large. Depending on how they are used, they can lead to injury and death. An action that generates fear in the public may become a means for terrorists; in other words, a politically motivated attack which results in a tremendous amount of fear and panic in the public may well be characterized as cyber terrorism even though it does not lead to physical injury or death.

\textsuperscript{91} Ibid.
\textsuperscript{93} Ibid. p. 52.
Congress defined cyber terrorism as,

“the use of computers as weapons, or as targets, by politically motivated international or sub-national groups or clandestine agents who threaten or cause violence and fear in order to influence an audience or cause a government to change its policies.”^94

Like terrorism, cyber terrorism involves the purposeful threat or use of violence to achieve apolitical or social goal. However, cyber terrorism is perpetrated through a different medium, computers. Thus, cyber terrorism includes the use of computers as weapons and computers as targets of conventional weapons or other computers.

Cyber terrorism must be considered to include the full range of threats, vulnerabilities, risks, and technological matters that anyone employing IT systems at the core and even on the periphery of their business must contend with today.\(^5\) Cyber attacks by individuals, such as hackers and other criminal entities provide strong evidence that the Internet can be a tool for terrorists who attempt to exploit every possible means available to them for their cause.

### 3.5 Characteristics of Cyber Terrorism

Cyber terrorism has several distinct characteristics. These characteristics help to better differentiate the fine line between a cyber-terror attack versus a cyber attack or activities of a hacker. Cyber terrorism will and may display the following signs:

---

^94 Supra Note 6.

Attack is predefined and victims are specifically targeted\textsuperscript{96}.

i. Attack has an objective to destroy or damage specific targets such as political, economic, energy, civil and military infrastructures.

ii. Attack may even target specific opposing religious group’s information infrastructures to insight religious pandemonium.

iii. The purpose of any attack is to create fear of the group’s intentions and further their own political agenda or goals or gain fellowship by succeeding in their attacks.

iv. Destroy the enemy’s capabilities to further operate or operate within their own arena.

v. Persuade others to believe that the victim or victims are vulnerable and their stability negligent.

vi. Create increased loyalty and pride within the group based on their successes.

3.6 Who are Cyber Terrorists?\textsuperscript{97}

But who are the cyber terrorists, are they existing terrorist groups or are they new organizations. While there are some groups of cyber terrorists in operation in the world the main threat would seem to come from groups that have historically operated in the ‘real’ world\textsuperscript{98}. In this information age, terrorist organizations, which is generally get no access to television or radio communications, can easily broadcast via the internet\textsuperscript{99}. They maintain their


\textsuperscript{98} Supra Note 1. p. 480.

\textsuperscript{99} Alexander, Yonah Swetman, Michael S., Cyber Terrorism and Information Warfare: Threats
Exchanges, which are often perceived as a lynchpin of each nation’s economy and hold something of an iconic status, have become seen as ‘fair game’ for attacks from almost every type of cyber terrorist, according to experts. But who are the man behind the masks?\textsuperscript{100} Experts distinguish cyber terrorists into four main categories, as below:

i. **Criminal Gangs**

   Historically, hostile cyber activity in the financial services sector has involved criminal gangs targeting retail bank platforms in a bid to steal customer funds. Increasingly, these gangs have looked to target exchanges with a view to manipulating markets and profiting from wild swings in the price of securities. In May, a major Distributed Denial of Service attack was successfully mitigated by protection service provider Prolexic\textsuperscript{101}. The target was an unnamed financial exchange platform, and the motive of the attack was market manipulation, according to a person close to Prolexic\textsuperscript{102}.

ii. **Hacktivists**

   Recent trends on the internet and attacks shows that politically motivated ‘hactivists’ such as anonymous have become more active. The protests they attempt largely take the form of disrupting online services. Exchanges have become seen as ‘fair game’ for attacks among these groups, according to Stephen Bonner, a partner in KPMG’s Information Protection and Business Resilience practice. He said, “Radical environmentalists or human rights groups tend to not target corporate, but the companies or infrastructure that support them, such as

\textsuperscript{101} Supra Note 97.
\textsuperscript{102} Ibid.
\textsuperscript{102} Ibid.
iii. State-Sponsored Groups

State-sponsored cyber terrorists are also known to be on the rise and are attacking ‘iconic’ pieces of market infrastructure such as exchanges. Last year, Israel’s Tel Aviv Stock Exchange was attacked by pro-Palestinian computer hackers and this offensive disrupted the exchange’s website. Saudi Arabian hacking group “Nightmare” claimed responsibility for this cyber attack, it came during a period of heightened political tension in the region.

iv. Disgruntled Insiders

The downsizing of the financial sector can leave many former employees with an axe to grind, but for market infrastructure providers it can have dramatic consequences. Bonner said, “When exchange staff leave, they take knowledge of risks and controls with them, as well as, potentially, software code.” He recommended that exchanges review the e-mail history of all technology leavers in the period up to their departure. In November 2010, the London Stock Exchange issued a statement that a 127 minute trading outage on its Turquoise platform was caused by ‘human error that may have occurred in suspicious circumstances’. However, following a full internal investigation, the incident was found to be just the result of human error.

From American point of view the most dangerous terrorist group is Al-Qaeda which is considered the first enemy for the U.S. According to US

103 Ibid.
105 Supra Note 97.
106 Al-Qaeda (The Base) is an international alliance of Islamic militant organizations founded in
Officials’ data from computers seized in Afghanistan indicate that the group has scouted systems that control American energy facilities, water distribution, communication systems, and other critical infrastructure. After April 2001 collision of US navy spy plane and Chinese fighter jet, Chinese hackers launched Denial of Service (DoS) attacks against American web sites. A study that covered the second half of the year 2002 showed that the most dangerous nation for originating malicious cyber attacks is the United States with 35.4% of the cases down from 40% for the first half of the year. South Korea came next with 12.8%, followed by China 6.2% then Germany 6.7% then France 4%. The UK came number 9 with 2.2%. According to the same study, Israel was the most active country in terms of number of internet users.\(^{107}\)

3.7 Magnetism of Cyber Terrorism

It is difficult to determine the level of interest, or the capabilities of international terrorist groups to launch an effective cyber attack. A 1999 report by The Center for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School concluded that it is likely that any severe cyber attacks experienced in the near future by industrialized nations will be used by terrorist groups simply to supplement the more traditional physical terrorist attacks.\(^ {108}\)

Some observers have stated that Al Qaeda does not see cyber terrorism as important for achieving its goals, preferring attacks which inflict human casualties.\(^ {109}\) Other observers believe that the groups most likely to consider and

---


\(^{109}\) The Ashland Institute for Strategic Studies has observed that Al Qaeda is more fixated on
employ cyber attack and cyber terrorism are the terrorist groups operating in post-industrial societies (such as Europe and the United States), rather than international terrorist groups that operate in developing regions where there is limited access to high technology.

However, other sources report that Al Qaeda has taken steps to improve organizational secrecy through more active and clever use of technology, and evidence suggests that Al Qaeda terrorists used the Internet extensively to plan their operations for September 11, 2001. Al Qaeda cells reportedly used new Internet based telephone services to communicate with other terrorist cells overseas. Khalid Shaikh Mohammed, one of the masterminds of the plot against the World Trade Center, reportedly used special Internet chat software to communicate with at least two airline hijackers. Ramzi Yousef, who was sentenced to life imprisonment for the previous bombing of the World Trade Center, had trained as an electrical engineer, and had planned to use sophisticated electronics to detonate bombs on 12 U.S. Airliners departing from Asia for the United States. He also used sophisticated encryption to protect his data and to prevent law enforcement from reading his plans should he be captured.


Khalid Sheikh Mohammed was a member of Osama bin Laden's al-Qaeda organization, leading al-Qaeda's propaganda operations from around 1999 until late 2001. He confessed to United States agents to a role in many of the most significant terrorist plots over the last twenty years, but the means of interrogation put his confession into question.

Ramzi Yousef is one of the main perpetrators of the 1993 World Trade Center bombing, bombing of Philippine Airlines Flight 434, and a co-conspirator in the Bojinka plot. In 1995, he was arrested at a guest house in Islamabad, Pakistan while trying to set a bomb in a baby doll by the Pakistani Inter-Services Intelligence (ISI) and U.S. Diplomatic Security Service, then extradited to the United States.

3.7.1 Lower Risk

Tighter physical security measures now widely in place throughout the United States may encourage terrorist groups in the future to explore cyber attack as way to lower the risk of detection for their operations. Also, linkages between networked computers could expand the effects of a cyber attack. Therefore, a cyber attack directed against only a few vulnerable computers could multiply its effects by corrupting important information that is transmitted to other downstream businesses.

3.7.2 Less Dramatic

However, other security observers believe that terrorist organizations might be reluctant to launch a cyber attack because it would result in less immediate drama and have a lower psychological impact than a more conventional act of destruction, such as a bombing. These observers believe that unless a cyber attack can be made to result in actual physical damage or bloodshed, it will never be considered as serious as a nuclear, biological, or chemical terrorist attack.

3.7.3 Cheaper

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

115 Supra Note 58.
3.7.4 Anonymous

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 policies forces to track down the terrorists’ real identity. And in cyber space there are no physical barriers such as checkpoints to navigate, no borders to cross, and no customs agents to outsmart.

3.7.5 Enormous Targets

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. They share number and complexity of potential targets guarantees 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.

3.7.6 Remotely Conducted

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.
3.7.7 More Effective

It has been proved by the ILOVEYOU virus\textsuperscript{116} that cyber terrorism has the potential to affect directly a large number of people than traditional terrorist’s methods, thereby generating greater media coverage, which is ultimately what terrorists want.

3.8 Modes of Cyber Terrorism

3.8.1 Cyber Terrorism is the Forerunner of Warfare

In the era of information and communication technology (ICT) one nation causes terrorist violence by using new technology against other nation or nations. These are not the conventional way of war rather cyber war or net war between two or more nations which are very much unpredictable. For e.g., net war between Israel and Pakistan, India and Pakistan, China and USA.

3.8.2 International Cyber Terrorist Attack

When International Organizations of terrorists link or communicate between them through internet and attack any nation, it is called international cyber terrorist attack. For e.g. 11\textsuperscript{th} September 2001 attack on World Trade Centre and Pentagon; immediately after that 13\textsuperscript{th} December 2001 attack at Indian Parliament.

3.8.3 Use of Computer System and Internet Facilities

Use of computer system and Internet facilities by terrorists group to develop own websites and network to send messages to each other worldwide are

\textsuperscript{116} The worm, first discovered in Hong Kong, arrived in e-mail boxes on May 4, 2000 with the simple.
effective mode of cyber terrorism\textsuperscript{117}.

3.8.4 Cyber Terrorists use Encryption Programme and Digital Signature

Cyber terrorists use encryption programme and digital signature to coordinate themselves using e-mail service which cannot be read by any one. Even the National Security Agency through their super computing system failed to crack terrorist group’s code. The USA is fighting against these attacks since 1990s.

3.8.5 Terrorists Now Using Information and Communication Technology (ICT) Including Satellite Transmission

Terrorists now use ICT including satellite transmission, cell phones, wireless etc. to communicate with each other and organize for terrorist attack.

3.8.6 Flowing Worm, Virus, Trojan Horse

Flowing worm, virus, Trojan horse etc. are used to collapse Government departments such as defence, intelligence, commerce, academic and health. Access to Global electronic network and information is one way which facilitates cyber terrorism.

3.8 Forms of Cyber Terrorism

There can be many forms of cyber terrorism, and some are discussed to understand the term better.

i. Cyber terrorists often commit acts of terrorism simply for personal gains.

\textsuperscript{117} Muktesh Chander, “Cyber Terrorism: A Myth or Possibility”, \textit{Indian Police Journal}, July-September, 2003, p. 25.
Such a group, known as the Chaos Computer Club, was discovered in 1997. They had created an Active X control for the internet that can trick the Quicken accounting program into removing money from a user’s bank account. This could easily used to steal money from users all over the world that have the Quicken software installed on their computer. This type of file is only one of thousands of types of viruses that can do everything from simply annoying users, to disable large networks, which can have disastrous results.

ii. Cyber terrorists are many times interested in gaining publicity in any possible way. For example, information warfare techniques like Trojan horse viruses and network worms are often used to not only do damage to computing recourses, but also as a way for the design of the virus to ‘show off’. This is a serious ethical issue because many people are affected by these cases. For one, the viruses can consume system resources until networks become useless, costing companies’ lots of time and money. Also, depending on the type of work done on the affected computers, the damage to the beneficiaries of that work could be lethal. Even if the person never meant to harm someone with their virus, it could have unpredictable effects that could have terrible results.

iii. In one of its more unusual forms, cyber terrorism can be used for an assassination. In one case, a mob boss was shot but survived the shooting. That night while he was in hospital, the assassins hacked into the hospital computer and changed his medication so that he would be given a lethal injection. He was dead a few hours later. They then changed the medication order back to its correct form, after it had been incorrectly administered, to cover their tracks so that the nurse would be blamed for the ‘accident’. There are many ethical issues involved in a case like this. Most obviously, a man was killed by the hacker’s actions. Also, the life of the nurse was probably ruined, along with the reputation of the hospital
and all its employees. Thus, there are often more stockholders in a terrorist situation that the immediate recipient of the terrorism.

iv. Terrorism can also come in the form of disinformation. Terrorists can many times say what they please without fear of reprisal from authorities or of accountability for what they say. In recent incident, the rumor that a group of people was stealing people’s kidney for sale was spread via the internet. The rumor panicked thousands of people. This is an ethical issue similar to screaming ‘Fire’ in a crowded theater. In case like this, the number of people affected is unlimited. Thousands of people were scared by this and could have suffered emotionally.

v. Minor attacks come in the form of ‘data diddling’, where information in the computer is changed. This may involve changing medical or financial records or stealing of passwords. Hackers even may prevent user who should have access to the machine. Ethical issues in this case include things like invasion of privacy and ownership conflicts. It could be even more serious if, for instance, the person who needed to access to the machine was trying to save someone’s life in a hospital and couldn’t access the machine. The patient could die waiting for help because the computer would not allow the necessary access for the doctor to save his or her life.

### 3.9 Most Infamous Attacks in Cyber Space

The cyber space provides a space to one and all without any discrimination where everyone can access out to one another in any case of time and distance obstacles. It has given a new meaning to the life, but has its limitations and negative repercussions as well. Most use the internet and cyberspace for their legitimate needs, but, others use it for their own dubious schemes, as they target individuals, companies, banks and even the military and government agencies. The following cyber attacks in the history of cyber space are well known which
were committed large-scale cyber terrorism and affected whole sovereign nations, which may have said to create some ‘terror’ are given below:

3.9.1 Cyber Attacks in Middle East

The Middle East has become a hotspot for cyber attacks, experts warn, amid an escalation of computer-led warfare across the globe.\textsuperscript{118} With the Middle East Conflict at a very heated moment between bordering countries Pro-Palestinian and Pro-Israel Cyber Groups have been launching an offensive against websites and mail services used by the political sectors the opposing groups show support for\textsuperscript{119}. The attacks had been reported by the NIPC (National Infrastructure Protection Center) in October of 2000 to U.S. Officials. The attacks were a volley of e-mail floods, DoS attacks, and Ping flooding of such sites as the Israel Foreign Ministry, Israeli Defense Forces, and in reverse, sites that belonged to groups such as Hamas and Hezbollah\textsuperscript{120}.

3.9.2 Cyber attacks between Pakistan and India

As tensions between the neighbouring regions of India and Pakistan over Kashmir grew overtime, Pro-Pakistan cyber-terrorists and recruited hackers began to target India’s Internet Community. Just prior to and after the September 11\textsuperscript{th} attacks, it is believed that the sympathizers of Pakistan (which also included members of the Al Qaeda Organization) spread of propaganda and attacks against Indian Internet based communities. Groups such as G-Force and Doctor Nuker


\textsuperscript{119} Supra Note 96.

have defaced or disrupted service to several major entities in India such as the Zee TV Network, The Indian Institute of Science and the Bhabha Atomic Research Center which all have political ties. The Group, Pakistani Hackerz Club also went as far as to target the United States Air Force Computing Environment and the Department of Energy’s Website. The Hindu reported on January 29 “Hackers defaced more than 2,000 Indian websites 2,118 to be exact on Republic Day (January 26) in what is being termed as ‘a major cyber attack’ and ‘the attackers’ internet protocol (IP) address was traced to Pakistan.

3.9.3 Retaliation in China

In May 1999 the accidental bombing of a Chinese embassy in Yugoslavia by U.S. Bombers, led to a massive web site defacement and e-mail bombardment attack on American companies and agencies. Pro-Chinese hackers and political groups executed the attacks to gain sympathy for the Chinese cause US Government sites such as the U.S. Departments of Energy and the Interior, and the National Park Service were all hit and had web sites defaced along with the White House web site. The site was downed for three days by continual e-mail bombing. Although the attack was rather random and brief and affected a small number of U.S. sites, the effects could have been worse.

3.9.4 Cyber Attack by Tamil Tigers

In 1998, with surges of violence committed in Sri Lankan over several years, attacks in cyber-space were the next area to target. The group known as the Tamil Tigers, a violent guerrilla organization, bombarded Sri Lankan embassies with over 800 e-mails a day. This was carried out over a two-week period. The attack by the e-mail message conveyed the message, “We are the Internet Black Tigers and we’re doing this to disrupt your communications.” After the messages created such major disruption the local Intelligence authorities were dispatched to investigate. The authorities declared the attack as the first known attack on the Sri Lankan by the terrorists on any computer system in the nation.\(^{124}\)

In 1999, Denning said that ‘Ethnic Tamil Guerillas were said to have swamped Sri Lankan embassies with thousands of e-mail messages. The message was thus “we are the Internet Black Tigers and we are doing this to disrupt your communications, an off-shoot of the Liberation Tiger of Tamil Elam (LTTE)."

Nowadays most of the terrorist groups have their own websites or information way (Iway). For e.g., one of the Al-Qaida based websites in Arabic language is http://www/mojahedoon.net which has link with Osama Bin Laden. Information and Communication Technology are very much used by terrorists in India for attack against the nation. Telephone, mobile phone, wireless, computer facilities are available almost everywhere in India. That is why terrorists are able to communicate with each other even being in remote rural area. They can control the entire group activities from remote areas. For e.g, Dawood Ibrahim controlling operations of his group from Gulf Country and from Pakistan. In 2000, within 4 months almost 131 Indian websites were defaced and this number was increased in 2001 by 160. The hacker group called ‘Silver Lords’ hacked about 23 Indian

\(^{124}\) Supra Note 96.

\subsection{Yugoslavia Conflict}

When NATO air strikes hit Former republic of Yugoslavia in Kosovo and Serbia, NATO web servers were subjected to sustained attacks by hackers employed by the Yugoslav military. All NATO’s 100 servers were subjected to ‘ping saturation’\footnote{One common form of DOS and DDOS attacks use a technique known as ping saturation. Ping is a simple Internet utility used to verify that a device is available at a given Internet address. Ping saturation occurs when ping is used in an attack to overwhelm a system. The intent in these types of attacks is to disrupt services on a network or system by flooding it with requests.} DDoS assaults and bombarded with thousands of e-mails, many containing viruses. The attacks on NATO servers coincided with numerous website defacements of American military, government, and commercial sites by Serbian, Russian, and Chinese sympathizers of Yugoslavia. These attacks cause serious disruption of NATO communications infrastructures.

\subsection{Result of China Fighter Plane Collision with American Spy Plane}

On April 1, 2001, there was a mid-air collision between an American surveillance plane and a Chinese fighter aircraft. Chinese hacker groups, such as the Honker Union of China and the Chinese Red Guest Network Security Technology Alliance, organized a massive and sustained week-long campaign of cyber attacks against American targets in retaliation for the death of Chinese pilot Wang Wei. Chinese hackers used Internet postings and IRC to plan and coordinate their assault against US systems. Approximately 1,200 U.S. sites, including those belonging to the White House, the U.S. Air Force, U.S. Geological Survey, and the Department of Energy, had been subjected to DDoS attacks or defaced with
pro-Chinese images. A number of recent Internet worms including Lion, Adore, and Code Red are suspected of having originated in China\textsuperscript{127}.

### 3.9.7 Attack on the Indian Parliament

On 13\textsuperscript{th} December 2001 attack on the Indian Parliament was with the help of Information Technology. It was a cyber attack; attackers used new technology and committed forgery to fulfill their end. They forged the gate pass and for attack they downloaded the official logo of Ministry of Home Affairs, other documents and the layout of the Parliament building. Police found a laptop from main accused Mohammed Afzal and Shuaket Hussain Guru. Police found out that they accessed the internet through Pakistan based ISPs. Investigating officers also found incoming and outgoing cell phone call numbers of deceased terrorists which were very much helpful for the police investigation. Police also found out a satellite connection with deceased terrorists cell phone\textsuperscript{128}.

### 3.9.8 Israeli Espionage Ring

In the wake of the Sept. 11, 2001 terrorist attack, the FBI has stumbled on the largest espionage ring ever discovered inside the United States. The U.S. Justice Department is now holding nearly 100 Israeli citizens with direct ties to foreign military, criminal and intelligence services. The spy ring reportedly includes employees of two Israeli-owned companies that currently perform almost all the official wiretaps for U.S. local, State and federal law enforcement. The U.S. law enforcement wiretaps, authorized by the Communications Assistance for Law Enforcement Act (CALEA), appear to have been breached by organized

\textsuperscript{127} Andrew M. Colarik, Cyber Terrorism: Political and Economic Implications, Idea Group, U.S., 2006. See also Supra Note 1, p.489.

crime units working inside Israel and the Israeli intelligence service, Mossad\textsuperscript{129}. The spy ring enabled criminals to use reverse wiretaps against U.S. intelligence and law enforcement operations. The illegal monitoring may have resulted in the deaths of several informants and reportedly spoiled planned anti-drug raids on crime syndicates\textsuperscript{130}.

3.9.9 Moonlight Maze

Moonlight Maze is the U.S. Government’s designation given to a series of alleged coordinated attacks on American computer systems in 1999. The attacks were traced to a main frame computer in Moscow but it is not known if that is where they originated. It was claimed that these hackers had obtained large stores of data that might include classified naval codes and information on missile guidance systems, though it was not certain that any such information had in fact been compromised\textsuperscript{131}.

3.9.10 Cyber Attack on Estonia

In April of 2007, Estonia was cyber-attacked from Russia\textsuperscript{132}. Ever since the government of the Baltic state decided to remove a war memorial to the Red Army from a square in the capital, Tallinn, Russian outrage has ensued. This took the form of demonstrations and even riots. But then something extraordinary happened quickly, and wholly without warning, the whole country was subjected to a barrage of cyber warfare, disabling the websites of government ministries, political parties, banks and newspapers. Techniques normally employed by

\textsuperscript{129} The Mossad (The Institute), is Israel’s intelligence agency and is responsible for intelligence collection, counter-terrorism, covert operations such as paramilitary activities.
\textsuperscript{130} NEWSMAX, Cited in Dr. R. K. Chaubey, Supra Note 1, p. 489.
cybercriminals, such as huge remotely-controlled networks of hijacked computers, were used to cripple vital public services. NATO has sent its top cyber-terrorism experts to Tallinn, with western democracies caught on the hop over the implications of such an attack.

The Estonian defense ministry said: “We’ve been lucky to survive this. If an airport, bank or state infrastructure is attacked by a missile, it’s clear war. But if the same result is done by computers, then what do you call it? Is it a state of war? These questions must be addressed.” Estonia has blamed Russia, predictably enough - which, if true, would mean this is the first cyber attack by one sovereign state upon another. The Estonian attacks were more likely to be the work of angry young Russian hackers working alone than any sort of organized blitz by the Kremlin. But either way, the implications are serious.133

On first week of September 2007, the Pentagon and various French, German and British government computers were attacked by hackers of Chinese origin. The Chinese government denies any involvement. Jeff Green the senior vice president of McAfee Avert Labs was quoted as saying, “Cybercrime is now a global issue. It has evolved significantly and is no longer just a threat to industry and individuals but increasingly to national security.” They predicted that future attacks will be even more sophisticated. “Attacks have progressed from initial curiosity probes to well-funded and well-organized operations for political, military, economic and technical espionage.”134

3.9.11 The Original Logic Bomb

During the cold war in 1982, the CIA disrupted the operation of operation of a Siberian gas pipeline of Russia using logic bomb. They use a portion of code in the computer system used in managing and controlling the gas pipeline and blast it. This was the worst use of logic bomb in the history. The chaos that ensued was so monumental that the resulting fire was even seen from space.

3.9.12 Titan Rain

In 2004, Shawn Carpenter discovered a series of coordinated ‘cyber raids’ in what the FBI believed to originate from government-supported cells in China. Chinese hackers, the People’s Liberation Army, attacked on the computer networks of British government departments, the Guardian has learned. The attackers have hit the network at the Foreign Office as well as those in other key departments, according to Whitehall officials. It was said as ‘Titan Rain’. Hackers infiltrate many important computer networks including, NASA and the Lockheed Martin, Redstone Arsenal, and Sandia National Laboratories. It was considered as one of the biggest cyber attacks in history. It also making off the all the systems and military intelligence but also leaves the backdoors or ‘jombify’ the machines.

3.9.13 Epsilon

One of the costliest cyber attacks in history, the data breach in Epsilon, the world’s largest provider of marketing and handling services to industry giants such as JP Morgan Chase, Best Buy, and other major financial services, retailers and other major companies in 2011, has an estimated damage cost that ranged

from $225 million to $4 billion dollars.

Names and email addresses were stolen from Epsilon, the world's largest email marketing firm in 2011, which handles more than 40 billion emails every year more than 2,000 brands worldwide including Marks and Spencer. The company faced a spear phishing attack, a sophisticated fraud which aims to gather user details through sending emails from a trusted company with many users, such as PayPal. So in the attack the hackers targeted the email addresses that they can use for their criminal activities, making its implications a lot greater than estimated\textsuperscript{136}.

3.9.14 Michael Calce

An ordinary boy, Michael Demon Calce, of 15 years knows as ‘MafiaBoy’ in the cyber world. He is from West Island, Quebec. He created a big problem by hacking the business and websites of the big business giant include computer giant Dell, Yahoo, Fifa.com, Amazon, Ebay and CNN with estimated damages of $1.2 billion dollars, not including his attacks in 9 out of 13 root name servers. However, he only received eight months of ‘open custody,’ one year of probation, a small fine and restricted use of internet by the Montreal Youth Court.

3.9.15 TJX

Massachusetts-based retailing company TJX, owner of such well-known chains as TJ Maxx and Marshalls, was taken for a ride by a group of cyber fiends with a fetish for electronics. Albert Gonzales and a group of hackers from the Shadowcrew were able to get their hands on over 45 million credits and debit card numbers, a selection of which they then used to fund a multi-million dollar

spending spree from Wal-Mart’s stock of electronics equipment. The data breach has resulted in $250 million in damages as Gonzales and 10 of his crew seek their targets while wardriving and looking for vulnerabilities in wireless networks along US Route 1 in Miami.\textsuperscript{137}

\subsection*{3.9.16 Operation Shady Rat}

Operation Shady Rat have hit at least 72 organizations worldwide including the International Olympic Committee, the United Nations, businesses, and defense contractors. It was an ongoing series of cyber attacks that started in mid-2006. Discovered by Dmitri Alperovitch, Vice President of Threat Research of McAfee in 2011, it was assumed that the People’s Republic of China was behind this. The operation was derived from the common security industry acronym for Remote Access Tool (RAT) and was behind the cyber attack on the 2008 Summer Olympics.\textsuperscript{138}

\subsection*{3.9.17 Stuxnet}

Iran was subjected to cyber attacks on June 2010 when its nuclear facility in Natanz was infected by Stuxnet, a cyber worm that was believed to be a combined effort of Israel and the United States, though no one claimed responsibility for its inception. The worm destroyed Tehran’s 1000 nuclear centrifuges and set back the country’s atomic program by at least two years, as it spread beyond the plant and infected over 60,000 computers as well. The Iranian government was also accused of its own cyber attacks to the United States, Israel

\begin{footnotes}

\end{footnotes}
and other countries in the Gulf Arabs, including their alleged involvement in the hacking of American banks in 2012.

3.9.18 India

Despite the country reputation for being an IT and software powerhouse, India has reported 13,301 cyber security breaches in 2011. However, the biggest cyber attack that the country has faced occurred on July 12, 2012 where hackers penetrated the email accounts of 12,000 people, which include high officials from Defense Research and Development Organization (DRDO), the Indo-Tibetan Border Police (ITBP), Ministry of Home Affairs, and the Ministry of External Affairs.\textsuperscript{139}

3.9.19 July 2009 Cyber Attacks

These were a series of coordinated attacks against major government, financial websites and news agencies of both the United States and South Korea involving the activation of botnet. This involved a number of hijacked computers that caused servers to overload due to the flooding of traffic called DDoS attack. The numbers of hijacked computers varied depending on the sources and include 50,000 from the Symantec’s Security Technology Response Group, 20,000 from the National Intelligence Service of South Korea, and more than 166,000 from Vietnamese computer security researchers as they analyzed the two servers used by the invaders.

3.9.20 The Spamhaus Project

Spamhaus was considered as the biggest cyber attack in history. A filtering

\textsuperscript{139} Phil Muncaster, “10,000 Indian Government and Military Emails Hacked”, \textit{The Register}, http://www.theregister.co.uk/2012/12/21/indian_government_email_hacked/, Retrieved on 12 January 2013.
service used to weed out spam emails, was subjected to cyber attacks wherein home and business broadband router owners became unsuspecting participants when their routers have been threatened. Thousands of Britons used Spamhaus on a daily basis determine whether or not to accept incoming mails. On March 18, 2013, Spamhaus added Cyberbunker to its blacklisted sites and Cyberbunker and other hosting companies retaliated by hiring hackers to put up botnets, which also exploited home and broadband routers, to shut down Spamhaus’ system.

3.10 Cyber Terrorism as a Force Multiplier

Conventional terrorist tactics, such as car bombings, assassinations, suicide bombings, kidnapping, and hijacking may never be replaced by cyber attacks. However, as a force multiplier, cyber terrorism can create more effect if it is executed in concert with other traditional terrorist actions. A good example can be the scenario created by CSIS involving detonation of a bomb as a conventional terrorist act and a denial of service attack as a force multiplier.  

Brenner and Goodman analyze the characteristics of cyberspace and the advantages that it provides for terrorists and other criminal entities. The first characteristic of cyberspace is that “cyberspace is borderless.” As the CIA Director George Tenet affirms, cyberspace gives terrorists the operational flexibility and greater security which could be capitalized by them in many ways, including establishing networks with other terrorist organizations and members, communicating between members, and facilitating use of the Internet as a

propaganda mechanism\textsuperscript{142}.

Cyber terrorists can target more than one target at one time, which can increase the significance of the attack. An interesting perspective by two authors, Brenner and Goodman, is that cyber attacks can act as ‘terror multipliers,’ which is a term for force multiplier\textsuperscript{143}. Terror multiplier can be explained as an effect of cyber attack which is created by the anonymous nature of the attack source and the consequences of the attack.

Terrorists will attack vulnerable targets, as opposed to the well protected ones, in order to be successful in their actions and create appropriate conditions which will serve their cause. Vulnerability of critical infrastructure represents one of the most important concepts of this research. Therefore, the next chapter\textsuperscript{144} focuses on the definition and detailed explanation of critical infrastructure.

3.11 Current State of Attack

Cybercrime continues to diverge down different paths with each New Year that passes. In 2013, cybercriminals are changing the way they organize and targeting new users and new platforms, online transaction-based activities continue to be exploited, and hacktivism related attacks continue to rise as a way to commit corporate espionage, push political agendas or cause reputational damage\textsuperscript{145}. Despite significant investment in technology and infrastructure, cyber terrorism represents one of the greatest challenges in combating terrorism\textsuperscript{146}.

\textsuperscript{142} Ibid. p. 13-14.
\textsuperscript{143} Ibid. p. 26.
\textsuperscript{144} Chapter 4.
Every day the Internet and countless other computer systems are under attack. In the 2014 research study conducted by the PWC\textsuperscript{147} in USA, 77\% of respondents detected computer security breaches within the last twelve months\textsuperscript{148}. In another more recent study conducted by KMPG\textsuperscript{149} in India, 49\% of companies have experienced computer attacks and/or breaches in the last 12 months\textsuperscript{150}. It was found that 89\% are the major threat. In the past, it has also come out for this survey, that these cyber attacks are politically motivated. This survey report also reveals that cyber attacks are increasing frequently\textsuperscript{151}. If that is not shocking enough, security professionals are worried about the increased sophistication of threats against computer systems. Most studies to date have shown that critical information infrastructures are potentially vulnerable to a cyber terrorist attack. These attacks not only disrupt the IT services but have financial implications as well. The increasing complexity of information systems creates new vulnerabilities and challenges for IT management. Even if the technology is armor plated, insiders acting alone or in concert with other terrorists may be able to exploit their access capabilities to wreak considerable harm\textsuperscript{152}.

\begin{flushright}
\textsuperscript{147}PricewaterhouseCoopers (now PwC), formed in 1998 from a merger between Price Waterhouse and Coopers & Lybrand, has a history in client services that dates back to the nineteenth century. Both accounting firms originated in London during the mid 1800s. Today, PwC serves 26 industries. Our industry-focused services in the fields of assurance, tax, human resources, transactions, performance improvement and crisis management have helped resolve complex client and stakeholder issues worldwide. We also bring our expertise and talents to help educational institutions, the federal government, non-profits, and international relief agencies address their unique business issues.
\end{flushright}

\begin{flushright}
\end{flushright}

\begin{flushright}
\textsuperscript{149}KPMG was formed in 1987 with the merger of Peat Marwick International (PMI) and Klynveld Main Goerdeler (KMG) and their individual member firms. Spanning three centuries, the organization's history can be traced through the names of its principal founding members - whose initials form the name 'KPMG' Retrieved on 2 January 2015.
\end{flushright}

\begin{flushright}
\end{flushright}

\begin{flushright}
\textsuperscript{151}Ibid. p. 5
\end{flushright}

\begin{flushright}
\end{flushright}
3.12 New Perspective for Cyber Terrorism

Cyber terrorism requires some new perspectives. The following concepts must be considered in order to fully understand cyber terrorism threats:

i. The motivation behind a cyber terrorist may be the same as any other type of terrorist attack.

ii. The individuals or organizations executing these acts may not necessarily be those committed to the outcome of the act. Cyber terrorism can require technical expertise that exists outside the realm of a terrorist organization. Frequently, a system cracker may be hired to execute the cyber terrorism act. This may be a professional looking for money or they may be a teenager, looking for challenge. The recruitment process may or may not include ‘the cause’.

iii. In case of cyber attacks, there may not be any warning. However, with cyber terrorism, one may not even know that the act has taken place until sometime after the attack. Many times the penetration to computer goes unnoticed and they choose for attack the right time to attack, much like a bomb timer, set to execute when a certain time span or a certain event take place.

iv. The cost of such an attack is minimal, and the tools and information are ubiquitous. While tracing terrorist ‘payloads’ is often possible with nuclear, biological or even some chemical weapons, cyber terrorism require only an expensive personal computers, modem, phone line, and software tools-tools which are available free and in multiple locations on the internet. Tracing the terrorists equipment, or even his activities, are complex and frequently near impossible to accomplish in real time.

v. Intelligence gathering on cyber terrorism is difficult, as it is complicated

by virtual meetings, drop sites, encryption, and steganography.

vi. Finally, the prevention of cyber terrorism requires more coordination than almost any other form of terrorism.

The explosion of inter-networks, the connection of trusted to non-trusted systems and myriad other factors, along with reliance and dependence on computerized systems, makes cyber terrorism one of the most difficult threats to prevent. The bottom line is that as cyber terrorism relates to traditional counter terrorism, while many of the players may be the same, the playing field, and some of the rules of the game, has changed.

3.13 Conclusion

In conclusion, it can be said that 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, world is facing the worst form of terrorism, popularly known as cyber terrorism. 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 definition in a straightjacket formula or pigeons
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 have to take care of the problems originating at the international level because the Internet, through which these terrorist activities are carried out, recognizes no boundaries. Thus, a cyber terrorist can collapse the economic structure of a country from a place with which a country may not have any reciprocal arrangements, including an ‘extradition treaty’. 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.