A Critical Study on Cyber Terrorism with Reference with 26/11 Mumbai Attack

1Mathiha Nehla Hani and 2Aswathy Rajan

1Saveetha School of Law, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai. nehlahani@gmail.com

2Saveetha School of Law, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai. aswathyrajan.ssl@saveetha.com

Abstract

It is more than evident that the method for directing psychological oppression with the time is winding up more advanced. The cyberterrorism is genuine danger to quick innovation improvement. Potential targets are frameworks which control the country's resistances and foundation. The fear-based oppressor without bounds will win the wars without discharging a shot-just by crushing foundation that fundamentally depends on data innovation. The quick development of the Internet clients what's more, Internet dependence significantly expanded the security dangers, unless there are suitable safety efforts to encourage anticipation. To comprehend digital fear mongering it is critical to take a gander at its experience, to perceive how the psychological oppressor associations or people are utilizing the benefit of innovation and what sort of measures governments are taking to help the battle against digital terrorism. This paper tries to give an illustrative and explanatory picture of digital psychological warfare in India. The paper envisages a comprehension of the nature and viability of digital assaults and attempting to think about and break down the endeavours made by India to address this test and feature what more should be possible. At long last, the paper talks about a portion of the significant occurrences of digital psychological warfare that have desolated the genuine what's more, virtual universes in the ongoing past.

Key Words: Technology, cyber world, terrorism, internet, cyber warfare.
1. Introduction

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 deadliest combination of weapons and technology, which if not properly safeguarded in due course of time, will take its own toll. The damage so produced would be almost irreversible and most catastrophic in nature. In short, we are facing the worst form of terrorism popularly known as "Cyber Terrorism". Cyber-terrorism is starkly different from common Internet crimes like identity theft and money fraud in that it can involve use of technology to divert or destroy systems and infrastructure, cause injury or death and undermine economies and institutions. To accomplish their goals, cyber-terrorists target the computer systems that control air traffic, electric power grids, telecommunications networks, military command systems and financial transactions.

The information technology is a double-edged sword, which can be used for destructive as well as constructive work. Thus, the fate of many ventures depends upon the benign or vice intentions of the person dealing with and using the technology. For instance, a malicious intention forwarded in the form of hacking, data theft, virus attack, etc can bring only destructive results. These methods, however, may also be used for checking the authenticity, safety and security of one's technological device, which has been primarily relied upon and trusted for providing the security to an organisation. For instance, the creator of the "Sassier worm" has been hired as a "security software programmer" by a German firm, so that he can make firewalls, which will stop suspected files from entering computer systems. This exercise of hiring those persons who are responsible for causing havoc and nuisance is the recognition of the growing and inevitable need of "self-protection", which is recognised in all the countries of the world. In fact, a society without protection in the form of "self-help" cannot be visualised in the present electronic era. The content providers, all over the world, have favoured proposed legislations in their respective countries, which allow them to disable copyright infringers' computers. In some countries the software developers have vehemently supported the legislations which allow them to remotely disable the computer violating the terms and conditions of the license allowing the use of the software. This position has, however, given birth to a debate about the desirability, propriety and the legality of a law providing for a disabling effect to these "malware". The problem is further made complicated due to absence of a uniform law solving the "jurisdictional problem ". The Internet recognises no boundaries; hence the attacker or offender may belong to any part of the world, where the law of the offended country may not be effective. This has strengthened the need for a "techno-legal' solution rather than a pure legal recourse, which is not effective in the electronic era.
2. **Aim of the Study**

- Analyse the impact of attack
- Determine the safety measures on prevent cyber terrorism
- To determine the types of techno initiatives the was invented by the Indian government

**Hypothesis**

- **HO:** There is no significance impact on India after the Mumbai attack 26/11
- **HA:** There is significance impact on India after the Mumbai attack 26/11.

3. **Research Methodology**

Doctrinal research is a theoretical study where mostly secondary source of data are used to seek to answer one or two legal propositions or questions or doctrines. Its scope is very narrow and there is no such need of field work. But non-doctrinal research lays lesser emphasis upon doctrines and it is not solely dependent on the traditional or conventional sources for data. Non-doctrinal or empirical research is more concerned with social values and people and thus, primary data are used in this type of research. Here field work is the most important part. Thus, scope is wider. Empirical research tries to find out the effect of legal decisions.

4. **Review of Literature**

**Anika M. Haseloff** have published his article on—Cyber Cafes and their Potential as Community Development Tools in India

In this paper research was conducted to identify the problems and potential of Cyber Cafe as development tools. It finds out the relationship between Cyber Cafe users, their usage pattern and their reach to Cyber Cafe. The author states that Cyber Cafe plays an important role as internet service provider as a shared access point. It effectively bridges the digital divide for the middle-class people in developing countries. It helps by helping the users of Cyber Cafe to solve the problems like Social Exclusion by communicating with the people, solving Technological skill deficits, accessing internet services etc. The survey was conducted to study internet usage with respect to time, sectors, Language and place of access. It identifies the age and employment status and education of the Cyber Cafe users. The paper put froth’s good point such as Cyber Cafe usage can be measures by not distinguishing between caste, age, sectors and other factors. Even illiterate people can make use of Cyber Cafe without special programs arranged for them to access internet.

**Mustafa KOÇ, Karen Ann FERNEDING** has published in their article on—The consequences of internet café use on Turkish college students’ social capital

This paper presents the potential impacts of Internet café use on Turkish college students. The author states that internet cafe usage has affected the life of
students due to which the students are more interested in online activities rather than spending time with family and friends. Spending of more time at internet cafe has made the students to lead a lonely life and are only virtually connected with the social world. Students prefer to stay online for different purposes. The paper expresses that internet cafe has changed the youth’s lifestyle. The Cyber Cafe is responsible for youth’s loneliness and lack of social activities.

*Derrick J. Neufeld in published in their paper—Understanding Cybercrime*

In this paper the author has analysed U.S. Department of Justice federal Cybercrime cases from 2008 and 2009, categorizes these cases using an applied criminal offense framework developed by the FBI, considers philosophical explanations for criminal motives, and then identifies the apparent motive(s) that led to the commission of each crime. This paper contributes to an improved understanding of what Cybercrime is, and why it is occurring at the individual level, to develop more proactive and effective solutions. The author provides a classification of crimes such as crime against society, property and crime against person taken from National Incident Based Reporting System (NIBRS).

*Cyber crime and cyber terrorism investigator’s handbook by Badak akhgar, syngress publishers 2016:*

Author of this book gives a concept of technological and logistic farm work of cybercrime as well as the social and legal back grounds of its prosecution and investigation.

*Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization: Cyberterrorism, Information Warfare, and Internet Immobilization by Reich and paul.C, IGI Global publisher, 2003:*

This book provides relevant frameworks and best practices as well as current empirical research findings in the area. It is aimed at professionals who want to improve their understanding of the impact of cyber-attacks on critical infrastructures and other information systems essential to the smooth running of society, how such attacks are carried out, what measures should be taken to mitigate their impact and what lessons can be learned from the attacks and simulations of the last few years.

*Policing Cyber Hate, Cyber Threats and Cyber Terrorism by Brian Blakemore, published by Routledge, 2016*

This book brings together a diverse range of multidisciplinary ideas to explore the extent of cyber threats, cyber hate and cyber terrorism. This ground-breaking text provides a comprehensive understanding of the range of activities that can be defined as cyber threats. It also shows how this activity forms in our communities and what can be done to try to prevent individuals from becoming cyber terrorists. This text will be of interest to academics, professionals and practitioners involved in building social capital; engaging with hard to reach individuals and communities; the police and criminal justice sector as well as IT
This book provides relevant frameworks and best practices as well as current empirical research findings for professionals who want to improve their understanding of the impact of cyber-attacks on critical infrastructures.

**Cyber Terrorism and Information Warfare by Dr M N Sirohi, Vij Books India Pvt Ltd, 2015**

Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks 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. Recently, terrorist groups have been conducting more passive forms of information warfare. It is reported that these terrorist groups are using the Internet to conduct their operations by employing email and file encryption and steganography, as well as conducting web defacement attacks. Information Warfare (IW) has been around since the dawn of war. Information warfare has been and remains a critical element in deciding the outcome of military battles. According to Denning, “Information warfare consists of those actions intended to protect, exploit, corrupt, deny, or destroy information or information resources to achieve a significant advantage, objective, or victory over an adversary. This book discusses the nature and impact of cyber terrorism with the methods that have proven to be effective in law enforcement.

### 5. A Study on Cyber Terrorism with Reference to 26/11 Mumbai Attack

The danger of fear-based oppression has represented a monstrous test in the post-Cold War period. Dread assaults in significant urban areas, towns and vacationer resorts over the globe have shown the insufficiency of the State instruments to address this test. Genuine endeavours have been made by Nations to address this test by outlining counter fear-based oppression procedures and hostile to dread instruments. Nonetheless, the majority of these are composed in an ordinary worldview, which may be viable in a customary dread assault. Be that as it may, there are impediments with regards to a fear assault of an offbeat nature. ¹

Data innovation (IT) has presented the client to a tremendous information bank of data with respect to everything and anything. Notwithstanding, it has additionally added another measurement to fear based oppression. Ongoing reports propose that the psychological militant is additionally getting prepared

¹ O., Agrawal, M., & Rao, H. R. (2011) Information control and terrorism: Tracking the Mumbai terrorist attack through...
to use the internet to carry out fear monger assaults. The likelihood of such assaults in future can't be denied. Fear based oppression identified with digital is prevalently known as 'digital psychological oppression'.

Over the most recent few decades India has cut a specialty for itself in IT. The greater part of the Indian keeping money industry and budgetary organizations have grasped IT to its full advancement. Reports recommend that digital assaults are naturally coordinated toward monetary and money related foundations. Given the expanding reliance of the Indian monetary and budgetary organizations on IT, a digital assault against them may prompt an unsalvageable crumple of our financial structures. What's more, the most startling idea is the incapability of proportional courses of action or the nonattendance of options.

The articles envisage an understanding of the nature and effectiveness of cyber-attacks and trying to study and analyse the efforts made by India to address this challenge and highlight what more could be done². The article is structured as given below:

● Definition of Cyber Terrorism.
● Methods of Attack.
● Tools of Cyber Terrorism
● Challenges to India's National Security.
● Existing Cyber Security Initiatives.
● Challenges and Concerns.
● Recommendations.

**Definition of Cyber Terrorism**

As the Nation ended up effective in uncovering fear-based oppressor systems engaged with the as of late completed dread assaults, the most exceptional component was the utilization of the instruments of the data age like messages, mobile phones, satellite telephones and so forth to remain associated. The stressing viewpoint was the utilization of present day devices drawing out that the psychological militant isn't just fixated on IEDs and AK-47 however has likewise aced the utilization of workstations and tablet PCs to offer artfulness to his loathsome outlines. As psychological militant associations understand its capacity and potential for troublesome endeavours at bring down costs they will turn out to be increasingly innovation smart and their methodologies and strategies will have a mechanical introduction.

**One of the Definitions of Cyber Terrorism States that**

'Cyber terrorism is the convergence of terrorism and cyber space. It is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and 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.

² Pg-242, Vakul Sharma- Information technology
or property or at roast 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 upon their impact. Attacks that
disrupt non-essential services or that are mainly a costly nuisance would not

This is one of the most comprehensive definitions of cyber terrorism. But even
this has a limitation. It states that for an attack to qualify as a cyber-attack it
should lead to violence. This is more conventional. Terrorist may direct an
attack only to disrupt key services, if they create panic by attacking critical
systems/infrastructure there is no need for it to lead to violence. In fact, such
attacks can be more dangerous.  

**Methods of Attacks**

The most popular weapon in cyber terrorism is the use of computer viruses and
worms. That is why in some cases of cyber terrorism is also called 'computer
terrorism'. The attacks or methods on the computer infrastructure can be
classified into three different categories.

- **Physical Attack.** The computer infrastructure is damaged by using
  conventional methods like bombs, fire etc.

- **Syntactic Attack.** The computer infrastructure is damaged by modifying
  the logic of the system to introduce delay or make the system
  unpredictable. Computer viruses and Trojans are used in this type of
  attack.

- **Semantic Attack.** This is more treacherous as it exploits the confidence
  of the user in the system. During the attack the information keyed in the
  system during entering and exiting the system is modified without the
  user’s knowledge to induce errors,

Cybercrime isn’t just constrained to deadening PC foundations, yet it has gone a
long way past that. It is additionally the utilization of PCs, Internet and data
portals-to help the customary types of fear-based oppression like suicide
bombings. Web and email can be utilized for sorting out a psychological
militant assault too. Most regular utilization of Internet is by planning and
transferring sites on which false purposeful publicity can be glued. This goes
under the classification of utilizing innovation for mental fighting.  

**Tools of Cyber Terrorism**

Cyber terrorists use certain tools and methods to unleash this new age terrorism.
These are:

- **Hacking.** The most popular method used by a terrorist. It is a generic
  term used for any kind of unauthorized access to a computer or a
  network of computers. Some ingredient technologies like packet

---

3Press trust of India (2012, Aug

Yar (Eds.), Handbook of Internet Crimes (pp. 214 - 229). Cullumpton: Willan Publishing
sniffing, tempest attack, password cracking and buffer outflow facilitates hacking.

- Trojans. Programmes which pretend to do one thing while actually they are meant for doing something different, like the wooden Trojan Horse of the 12th Century BC.
- Computer Viruses. It is a computer programme, which infects other computer programmes by modifying them. They spread very fast.
- Computer Worms. The term ‘worm’ in relation to computers is a self-contained programme or a set of programmes that can spread functional copies of itself or its segments to other computer systems usually via network connections.
- E-Mail Related Crime. Usually worms and viruses must attach themselves to a host programme to be injected. Certain emails are used as host by viruses and worms. E-mails are also used for spreading disinformation, threats and defamatory stuff.
- Denial of Service These attacks are aimed at denying authorized persons access to a computer or computer network.
- Cryptology. Terrorists have started using encryption, high frequency encrypted voice/data links etc. It would be a Herculean task to decrypt the information terrorist is sending by using a 512-bit symmetric encryption.⁵

**Challenges to India’s National Security**

As brought out earlier India has carried a niche for itself in the IT Sector. India’s reliance on technology also reflects from the fact that India is shifting gears by entering facets of e-governance. India has already brought sectors like income tax, passports visa under the realm of e-governance. Sectors like police and judiciary are to follow. The travel sector is also heavily reliant on this. Most of the Indian banks have gone on full-scale computerization. This has also brought in concepts of e-commerce and e-banking. The stock markets have also not remained immune. To create havoc in the country these are lucrative targets to paralyze the economic and financial institutions. The damage done can be catastrophic and irreversible. Existing Counter Cyber Security Initiatives⁶.

**National Informatics Centre (NIC)**

A premier organisation providing network backbone and e-governance support to the Central Government, State Governments, Union Territories, Districts and other Governments bodies. It provides wide range of information and communication technology services including nationwide communication Network for decentralized planning improvement in Government services and wider transparency of national and local governments.

---


⁶ M. Cereijo, Cuba the threat II: Cyberterrorism and Cyberwar, 16 Maj 2006: http://www.lanuevacuba.com/archivo/manuel-cereijo-110.htm
Indian Computer Emergency Response Team (Cert-In)

Cert-In is the most important constituent of India's cyber community. Its mandate states, 'ensure security of cyberspace in the country by enhancing the security communications and information infrastructure, through proactive action and effective collaboration aimed at security incident prevention and response and security assurance'.

14. National Information Security Assurance Programme (NISAP). This is for Government and critical infrastructures, Highlights are:

- Government and critical infrastructures should have a security policy and create a point of contact.
- Mandatory for organizations to implement security control and report any security incident to Cert-In.
- Cert-In to create a panel of auditor for IT security.
- All organizations to be subject to a third-party audit from this panel once a year.
- Cert-In to be reported about security compliance on periodic basis by the organizations.

Indo-US Cyber Security Forum (IUSCSF)

Under this forum (set up in 2001) high power delegations from both side met, and several initiatives were announced. Highlights are:

- Setting up an India Information Sharing and Analysis Centre (ISAC) for better cooperation in anti-hacking measures.
- Setting up India Anti Bot Alliance to raise awareness about the emerging threats in cyberspace by the Confederation of Indian Industry (CII).
- Ongoing cooperation between India's Standardization Testing and Quality Certification (STQC) and the US National Institute of Standards and Technology (NIST) would be expanded to new areas.
- The R&D group will work on the hard problems of cyber security, Cyber forensics and anti-spasm research.
- Chalked the way for intensifying bilateral cooperation to control cybercrime - between the two countries.

Challenges and Concerns

Some challenges and concerns are highlighted below:

- Lack of mindfulness and the way of life of digital security at individual and additionally institutional level.
- Lack of prepared and qualified labour to execute the counter measures.
- Too numerous data security associations which have turned out to be frail because of 'turf wars' or money related impulses.
- A feeble IT Act which has turned out to be excess due to non-abuse and age old digital laws.

---

7 Veerasamy 2009 4th International Conference on Information Warfare and Security 26-27 March
- No email account strategy particularly for the guard powers, police and the office faculty. (f) Cyber-assaults have come from fear mongers as well as from neighbouring nations hostile to our National advantages.

Proposals. Certain Recommendations are given below
- Need to sensitize the common citizens about the dangers of cyber terrorism. Cert-in should engage academic institutions and follow an aggressive strategy.
- Joint endeavours by all Government offices including protection powers to pull in qualified gifted faculty for usage of counter measures.
- Cyber security not to be given more lip benefit and the associations managing the same ought to be given all help. No bureaucratic strength ought to be allowed.
- Agreements identifying with digital security ought to be given an indistinguishable significance from other traditional ascension.
- More interest in this field as far as fund and labour. (f) Indian organizations working after digital security ought to likewise keep a nearby vigil on the advancements in the IT segment of our potential foes.

Indian Interpretation of Cyber Terrorism

Even though the issue of digital fear mongering has pulled in immense consideration from digital criminologists, digital law authorities and sociology analysts, not very many examines have been improved the situation breaking down the legitimate issues engaged with digital psychological oppression in India. A moment investigation of the 26/11 Mumbai assaults would demonstrate that digital correspondence between the psychological militants and use of digital technology by them to be familiar with the objective populace and the place, made comparable wrecking brings about India. It was watched that the clear majority of the 26/11 arranging was likewise arranged carefully with Google Earth. The psychological militants made utilization of "mobile phone systems for order and control, and web-based life to track and obstruct the endeavours of Indian commandos. More worryingly, the fear mongers showed ability which bore signs of an expert group. They figured out how to change over sound signs to information before transmission. This made it relatively difficult to Indian security powers identify and capture given their present level of foundation and capacities.

In July 2011, the computerized innovation was additionally utilized for bomb impacts in a jammed city showcase in Zaveri Bazaar, Mumbai. The 2010 Varanasi impact case likewise observed the use of digital correspondence wherein the Indian Mujahidin asserted obligation regarding the impact. Stirred by this, the Government of India found a way to reinforce the digital security, including restriction of psychological militant exercises through the internet by

---

method for altering the current Indian data Technology Act, 2000. India was the twelfth country on the planet to administer on digital law, receiving an IT Act, despite the fact that the expression "digital fear based oppression" is missing from the phrasing of the Act, as IT Act 2000 was first actualized by the Indian government to for the most part "give lawful foundation to electronic business in India, and to encourage electronic recording of reports with Government organizations" However, because of reactions of the absence of enactments in ITA, Information Technology Amendment Act (ITAA) which contains a more all-encompassing arrangement of cybercrime laws, for example, incorporation of tyke erotica and digital psychological oppression was then passed by the Parliament in 2008. Further GOI has likewise realized corrections to the Indian Penal Code (IPC) and the Indian Evidence Act to help in digital wrongdoing examination. The arrangement that was particularly embedded in this law making body for this reason for existing was segment 66F which characterizes and depicts digital psychological oppression From the area 66F, it could be derived that, digital fear based oppression is a demonstration of hacking, blocking and/or PC tainting to confine lawfully approved people to get to PC assets when all is said in done, and/or to pick up or get unapproved access to any data which is a „restricted information“ with the end goal of security of the state, or remote connection and so forth. These are grim acts which is finished with a goal to undermine the security, sway and respectability of India or strike dread in the brains of individuals or an area of individuals; and which may bring about death and damage to individuals, harm to properties, interruption of common administrations which are basic to the life of a network, and furthermore influences the basic data framework.

For expounding these qualities, I take up the 26/11 Mumbai dread assault case. Even though the media had featured the incredible fear-based oppressor assault on critical business and Jewish settlements in Mumbai, the Indian Ministry of Home undertakings in their yearly report (2010) had discharged a definite nexus between computerized innovation and the abuse of the same by fanatics, satellite telephones, GPS and different sites were broadly utilized for satisfying the mission of the extremists. according to the actualities accessible regarding 26/11 assaults, the culprits accessed the PC assets accessible at Taj Hotel and Trident Hotel. They got to the Hotel PCs to download data about the inn visitors, particularly the US and UK subjects remaining by then of time. Their goal was to execute the inn visitor specifically by acquiring their room numbers from inns PC database. What culprit did? From area 66F point of view, the culprits purposefully debilitated the solidarity, respectability, security, or sway of India and struck fear and made demise or wounds the individual and harmed or devastation of property by infiltrating or getting to a PC asset without authorisation. Therefore, the demonstration of culprit of 26/11 may fall under

10 Cyber Law & Information Technology (2011) by Talwant Singh, Additional District & Sessions Judge, New Delhi, India
the classification of digital fear mongering\textsuperscript{11}.

Faces The Information Technology Act, 2000 (corrected in 2008) had meticulously taken endeavours to secure ensured frameworks, which is characterized by Section 70. "The fitting Government may, by notice in the Official Gazette, proclaim any PC asset which specifically or in a roundabout way influences the office of Critical Information Infrastructure, to be an ensured framework". Additionally, activities of government incorporate the death of tenets, for example, the Information Technology (Guidelines for Cyber Cafe) Rules, 2011 under the umbrella of the IT Act. In doing as such, the legislature has needed to walk a fine harmony between the essential rights to protection under the Indian Constitution and national security prerequisites. Digital fear-based oppression increases new faces in pace with the developing advancements in the digital field. India different difficulties of digital fear mongering with the development and far reaching utilization of long range informal communication destinations and computerized medium. Altogether more than 80 web pages were restricted by the legislature of India in the wake of gossipy titbits after the Assam occurrence uncovers the force of new face of digital psychological warfare in the nation.

**Tackling Cyber Terrorism in India**

Even though the acts of cyber coercion have multiplied in lots and bounds, the Parliament of Republic of India is however to enact any legislation that specifically addresses the problem of cyber coercion. However, sure existing legislations are amended to incorporate it at intervals its horizon the crime of cyber coercion\textsuperscript{12}.

The legislations are:

**Information Technology Act**

The salient provisions of the IT Act in relevancy preventing cyber act of terrorism are:

Section 66F of the IT Act defines cyber act of terrorism. This Section has been introduced by means of modification to the Act within the year 2008. This modification was the result of the notorious 26/11 terror attack in Asian country. The terrorists, during this case, created use of the communication services to assist the terrorists UN agency dispensed a series of twelve shooting attacks throughout town of metropolis. This tragedy could be a classic example of act of terrorism mistreatment the cyber network.

This Section conjointly prescribes the social control for people who commit or conspire to commit cyber act of terrorism. consistent with the Section, such folks shall be punishable with imprisonment which can reach imprisonment for keeps.

\textsuperscript{11} Introduction to Indian Cyber Law (2008) by Rohas Nagpal, Asian School of Cyber Laws, Pune, India

However, it’s pertinent to notice that the cyber house is evolving each day and new loopholes have emerged during this definition of cyber act of terrorism.

**Cyber Security Policy 2013**

For the primary time in history, within the year 2013 India introduced its national level cyber security policy. This policy lays down the broad framework for upholding and protective the cyber area security. the most aim of this policy is to make a broad umbrella of cyber security framework within the country in order that the Indian cyber area is secure and free from any quite attacks each by terrorists and different anti-social components. However, there’s a necessity to amend this policy to cover newer ways of guaranteeing the security of the ever-evolving cyber area

**Blocking access to Information**

Section 69A of the IT Act conjointly empowers the Central government or any of its authorised staff to direct any agency of the govt. to dam access by the public any info from a pc resource within the interests of sovereignty and integrity of the state.

**Indian Computer Emergency Response Team (“CERT-In”)**

As per Section 70B of the IT Act, the CERT-In team is ready up that provides immediate alerts of incidents difficult cyber security and conjointly lists out the emergency measures for handling incidents threatening cyber security of the state.13

### 6. Case Laws Relating to Cyber Terrorism

#### Ahmedabad Bomb Blast Case 2008

The 2008 Ahmedabad bombings were a series of twenty-one bomb blasts that hit Ahmedabad, India, on twenty-six Gregorian calendar months 2008, at intervals a span of seventy minutes. fifty-six individuals were killed and over two hundred individuals were bruised. Ahmedabad is that the cultural and industrial heart of Gujarat state, and an oversized a part of western India. The blasts were thought-about to be of low intensity, and were just like the metropolis blasts, province that occurred the day before.

Many TV channels aforesaid they’d received Associate in Nursing e-mail from a terror outfit referred to as Indian cluster force) claiming responsibility for the fear attacks; monotheism militant group Harkat-ul-Jihad-al-Islamic, however, has claimed responsibility for the attacks. The Gujarat police inactive the suspected mastermind, Mufti Abu Bashir, in conjunction with 9 others, in affiliation to the bombings.14

---

Warning of Attacks through e-mail

Several news agencies described about receiving a 14-page e-mail five minutes before the explosions with the subject line: "Await 5 minutes for the revenge of Gujarat", apparently referring to the 2002 Gujarat violence which took place after the Godhra train burning incident. The e-mail was sent by the group known as Indian Mujahideen on 26 July at around 6:41pm IST.

The message given through the e-mail warned of attacks in 5 minutes: “In the name of Allah the Indian Mujahideen strike again! Do whatever you can, within 5 minutes from now, feel the terror of Death!”

The e-mail also contained threats against Chief Minister of Maharashtra, Vilasrao Deshmukh, and his deputy, R.R. Patil, with the claim, “We wonder at your memory. Have you forgotten the evening of 11 July 2006 so quickly and so easily?”

Furthermore, the threats went on to warn Indian businessman Mukesh Ambani of Reliance Industries to “think-twice” before “usurping and building a citadel on a land in Mumbai that belongs to the Waqf board...lest it turns into horrifying memories for you which you will never ever forget.”

The e-mail also reportedly threatened several Bollywood actors, asking them to stop acting.

People who were Arrested

Maulana Abdul Halim, a suspected Students Islamic Movement of Republic of India activist, was in remission from Dani Limda within the heart of Ahmedabad on twenty seven July 2008. He was presupposed to be concerned in instigating the Muslim youth once the 2002 Gujarat violence and causation them to province for terror coaching. Charges have additionally been ordered on him for causation thirty-three youths for terror coaching to Asian nation in 2003. once his arrest, he was remanded to a 14-day police custody by the Metropolitan adjudicator in Ahmedabad.

On fifteen August, the Gujarat police in remission Mufti Abu Bashir, and 9 others, in association to the bombings. Bashir belongs to Binapara village in Azamgarh district of Japanese province and was believed to be a SIMI activist.

On twenty four Oct, a SIMI activist, Abdul Razik Mansuri, a resident of Gomtipur space Nagda district, Madhya Pradesh, had been in remission in conjunction with Harun Rashid, a Gujrat residence and send to Gujarat for questioning. The Joint Commissioner of Police for the crime branch, Ashish Bhatia, said: "He was in remission from the Nagda district in Madhya Pradesh by our team. He was there staying with several his relative. we've brought him to Ahmedabad for interrogation.” He added that Mansuri was seemingly to be
made before a court in Ahmedabad to be remanded to judicial custody.\(^{15}\)

On 11 November, the Madhya Pradesh Anti-Terror Squad (ATS) in remission Qayamuddin Kapadia, a superior member of SIMI and a key felon and fiduciary of the attack, in Ujjain. Police claimed that Kapadia admitted his involvement within the Ahmedabad blasts, which he, in conjunction with Abdul Subhan Qureshi alias Tauqeer of Bombay and Riaz Bhatkal of Mysore, collaborated with the SIMI cell led by Atif to hold out the Delhi blasts. Atif was later killed in association degree encounter with special cell of Delhi Police.

On thirteen Gregorian calendar month, Rafiuddin Kapadia, the brother of the key defendant, Qayamuddin Kapadia, was in remission by the town police of Ahmedabad. His arrest took the toll of the full control by the police to forty-three. The Joint Commissioner of Police, Ashish Bhatia, WHO is heading the probe within the serial blasts case, said: "We have in remission Rafiuddin Kapadia, brother of Qayamuddin. He was gift at the SIMI coaching camp in Halol close to Vadodara. He originally hails from Vadodara and was in remission these days from Ahmedabad by the crime branch officers.

On twenty-six March 2012, Maharashtra ATS in remission one blast suspect Muhammad Abrar adult male Khan alias Abrar Shaikh in an associate degree encounter in Sambhajinagar. Khaleel Qureshi was killed and Muhammad Shakeer was wounded within the encounter. All area unit pre supposed to be members of FTO Indian military unit. A policeman was additionally disjointed throughout the firing.

On nineteen June 2016, Gujarat Anti-Terrorism Squad, in remission Nasir Rangrez from Belgaum.\(^{16}\)

**Legal Case**

Controversy arose within the court case of the twenty-six defendants because the state was speculated to have suppressed the legal rights of the defendant. On twenty-three Gregorian calendar month lawyers of the defendant walked come in protest the stand taken by the Metropolitan functionary. The lawyers wished to full fill the defendant alone, however, they'd touched Associate in Nursing application stating that police didn't enable them to full fill their shoppers alone which the Court ought to direct the police to not stay gift whereas they were reproof the defendant. The Metropolitan functionary countered that it had been unimaginable as police had to be with the defendant. he's same to own hinted at collusion between the lawyers and therefore the defendant, inflicting a walk out by the accused's lawyers. The next day, in 2 completely different cases, the selected Metropolitan Court remanded all the twenty-six defendants to police

\(^{15}\) Ahmedabad blasts claim two more victims”. Hindustan Times. HT Media Ltd. 1 August 2008. Archived from the original on 10 August 2008. Retrieved 1 August 2008

custody until thirty-one Gregorian calendar months.

As per the legal rules police got to file a day book in any case before ninety days of the primary arrest of the case. However, on Martinmas, concerning 3 months when blasts and therefore the late July arrest, the Gujarat police filed a day book, touching on the town civil hospital blast and L G hospital blast case, in an exceedingly court naming twenty-six folks, all with alleged linked to SIMI, as accused within the case. A 2,000-page day book was filed within the court of the Metropolitan functionary, G M Patel. The defendant enclosed SIMI activists Mufti Abu Basher, Safdar Nagori and Sajid Mansuri. The day book additionally listed the names of fifty absconders, which police had thus far examined 511 potential witnesses.

**Mumbai Attack 26/11**

**Facts**

Ten Pakistani men related to the phobia cluster terrorist group stormed buildings in Bombay, killing 164 individuals. 9 of the gunmen were killed throughout the attacks, one survived. Mohammed Ajmal Kasab, the lone living gunman, was dead in Nov 2012.

They travelled from Karachi, West Pakistan to Bombay via boat. on the manner, they hijacked a fishing trawler and killed four crew members, throwing their bodies overboard. They conjointly slit the captain's throat.

The terrorists docked at the Bombay city district close to the entryway of Republic of India monument. They hijacked cars, together with a police wagon, and split into a minimum of 3 teams to hold out the attacks, in step with police. The attackers used automatic weapons and grenades.

**How did Mumbai 26/11 Took Place**

The attackers had planned the attack many months previous time and knew some areas to an adequate degree to fade and re-emerge once security forces had left. Many sources have quoted Kasab telling the police that the cluster received facilitate from urban centre residents.

The attackers used a minimum of 3 SIM cards purchased on the Indian aspect of the border with Asian country there have been conjointly reports of a SIM card purchased within the USA state New Jersey, if this is often the case, then this may return to Iraqi Intelligence Services and Al Qaeda from 9/11 or Jemmah Ismaliyah and Egyptian monotheism Jihad through Iraqi Intelligence from leader Hussein's previous network of militants that was ne'er proved. Police had conjointly mentioned that Faheem Ansari, associate degree Indian Lashkar operative United Nations agency had been inactive in Feb 2008, had scouted the urban centre targets for the November attacks. Later, the police inactive 2

---

Indian suspects, Mikhtar Ahmad, United Nations agency is from Srinagar in Cashmere, and Tausif Rehman, a resident of Kolkata. They equipped the SIM cards, one in urban center, and therefore the alternative in national capital.

The attackers used a satellite phone and cell phones to speak to every alternative moreover as their handlers that were primarily based in Pakistan. In transcripts intercepted by Indian authorities between the attackers and their handlers, the handlers provided the attackers with encouragement, plan of action recommendation, and knowledge gained from media coverage. The attackers used each personal cell phones and people obtained from their victims to speak with one another and therefore the journalism. though the attackers were inspired to murder hostages, the attackers were in communication with the journalism via cell phones to create demands reciprocally for the discharge of hostages. This was believed to be worn out order to more confuse Indian authorities that they were handling primarily a captive.

7. Conclusion

Change is inevitable and therefore the dilemmas that advancement in technology poses cannot be avoided. the reality is that the criminals have modified their strategies and have started hoping on the advanced technology, and to subsume them the society, the legal, and therefore the enforcement authorities, the non-public companies and organizations will get to modification their mechanism to combat it. additional such consultants should not solely be knowledgeable however should even be given necessary technical hardware’s and computer code in order that they will expeditiously fight the cyber criminals. Thus, necessary facilities should be established in varied components of the country in order that crime within the virtual world may be controlled'. Another facet that must be highlighted is that a culture of continuous cyber education and learning must be inculcated amongst the legal and therefore the enforcement authorities because of information the data) Technology field terribly is extremely is incredibly) dynamic because the knowledge of nowadays becomes obsolete during a very short time. last the preamble of the knowledge Technology Act, 2000 provides that the Act was passed with the target to offer legal recognition for transactions administered by suggests that of electronic information interchange and different suggests that of e-commerce, additional the Act has conjointly created amendments to the Indian legal code 1860, Indian proof Act 1872, The Bankers Books of proof Act 1891, and therefore the banking concern of Bharat Act, 1934 for facilitating legal recognition and regulation of the business activities. although this objective of the Act isn't to suppress the criminal activity, however this act has outlined bound offences and penalties to overpower such omissions, that is known to return inside the characterization of cybercrimes. From this, it may be inferred that the law cannot afford to be static, it should be modification with the dynamical times and viz. cyber house. this is often a lot of of needed, that a lot of applications of the technology may be used for the betterment of the
humankind, equally it equally true that such application can even be used for the
damage of the humankind as has been incontestable by the Spy-cam case. The
bottom-line is that the law ought to be created versatile in order that it will
simply fits the requirements of the society and therefore the technological
development.

The legal systems round the globe are, with each passing year, attempting to
implement new measures to combat cyber act of terrorism. However, with a lot
of innovative ways that of operating within the cyber area, a lot of loopholes are
shaped which can get to be crammed in by the countries by amending the
procedures and the laws in effect to tackle cyber act of terrorism. Moreover, a
unified international framework ought to be in situ to combat this world issue.
Further, the public ought to be created conscious of the threats and the ways that
and means that of dissemination and the way to deal just in case of terrorist
attacks. All these measures can go an extended method in establishing a secure
cyber area desired by the voters.

References

Records

Delhi, India.

[3] Cyber Law & Information Technology (2011) by Talan Singh,

[4] Additional District & Sessions Judge, New Delhi, India.

School of Cyber Laws, Pune, India

Press, New Delhi, India.

Journal of Cyber Law, Vol. 1, No. 1 (November) 75 at p.77.


[9] Indian Penal Code (1860).

Delhi: Dominant Publishers & Distributors, pg3


[12] https://cybercrimelawyer.wordpress.com/category/66c-
punishmentfor-identity-theft/


[16] www.ncpc.org