Page 979 - 988 **DOI:** *https://doij.org/10.10000/IJLMH.111415*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 4

2021

Cyber Terrorism: A Tool of Mass Destruction

GAGANDEEP SINGH [1]

ABSTRACT

Cyber terrorism essentially denotes the use of technology in achieving terror agendas. This is one of the most common paths taken for indulging into cyber terrorist activities. The cyber terrorism is a way which not only results in virtual data loss; rather it also creates a strong physical impact. The framing procedure of Indian laws on cyber terrorism has been quite latent. Through this research the researcher will highlight the physical impact which is created by cyber terrorism and how it can be used as a tool for mass destruction. Besides this, the researcher will also discuss the legal framework pertaining to cyber terrorism in India. One thing which is seen in this research is that despite of several direct indications regarding the ill-effects of cyber terrorism, the cyber security system in India is significantly poor.

Keyword: *Cyber terrorism, Cyber law, Cyber space, Information Technology.*

I. INTRODUCTION

The term 'cyber' denotes the computer world, information technology, virtual reality, artificial intelligence. This is an intangible space that works over the internet through computers, mobiles, or other devices which allow access to the internet. The world of cyberspace is not a new concept rather it has evolved recently in the 21st century but it is certainly one of the fastest-growing fields in the world. Every day there is the introduction of some new technology, software, programmers, and data into the world of cyberspace. But new ventures bring with them new difficulties. With the growth in the usage of the internet, there was growth in crimes over the internet as well. Crimes that are done with the use of the computer, mobile, laptop, or any other devices used for programming are generally termed cyber crimes.

When the use of the internet had just begun the hackers used to install viruses into the computers of their targets like Trojan horse, root-kit, e-mail bomb, etc. All these fraudulent activities were done to get access to the data of the target computer and later destroy the data. With the passage of time, the nature of cybercrimes also evolved. Nowadays, pornography,

[1] Author is an Assistant Professor at Siddhartha Law College, India.

 [ISSN 2581-5369]

stalking, money laundering, hacking, etc are popular cyber crimes. In today's time, most of the crimes are done over the internet. Cybercrimes are quick, difficult to decode the identity of the wrongdoer, and there are various other aspects that differentiate cyber crimes from traditional crimes, it is further discussed below.

On one hand where cyber crimes are committed to attain personal or individual motives, cyber terrorism is a thing where crimes are committed at a comparatively large extent to attain political motives and ideologies. This is because a terrorist activity can generally be not initiated and successfully completed by a single person single handedly. Cyber terrorism involves technology and internet to execute terror in the society. There have been various instances where the terror attack was backed by the information gathered through the web.

With the growth of cybercrimes in society, there was a need for new laws which could help to govern the illicit activities taking place around Information technology. The Parliament of India passed India's first cyber law in 2000 titled as 'The Information Technology Act, 2000'.

II. MEANING OF CYBER TERRORISM

Cyberspace may be regarded as that e-medium of computer networks which allows online communication for the purpose of interaction among the people belonging to different spheres of life, exchange concepts, impart information, offer social help, undertake businesses, produce inventive media, run games, have political discussion and so on there are chances that the data might get misused. No matter what advantages the technology bring along, it is nearly impossible that its disadvantages are left untouched.

The question here is what is cyber terrorism and how is it harmful for the society at large. According to Federal Bureau of Investigation of the United States of America, "cyber terrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."[2]

In simpler terms, the acts of cyber terrorisms is designed to attain, propagandas or political ideologies through intimidation, extortion, fear, etc. cyber terrorism therefore, is the use of internet to perform illegal activities so much so that it might cause bodily injury or death or person(s). Cyber terrorists tend to attack the computer networks, access the data illegally, destroy networks, and may use the information attained to fulfill their political ideologies.

[2] Definition by FBI U.S.A. Available at https://searchsecurity.techtarget.com/definition/cyberterrorism (Last visited on 12/06/2021

 [ISSN 2581-5369]

III. IMPACT OF CYBER TERRORISM ON THE PHYSICAL WORLD

Many scholars believe that cyber terrorism cannot be used as a weapon of physical mass destruction. Physical destruction refers to the terror activities involving loss of lives, attacks on humanity, destruction of property and population; for example, the attack of 09/11/2001 on the world trade centre in the United States of America, or the attack on the Taj hotel in Mumbai, India on 26/11/2008, etc. Some people are of the view that cyber terrorism cannot do a physical attack or destruction like the above two examples of physical destruction.

Instead of directly and physically attempting an attack, the cyber terrorists create a path for mass destruction. The famous attack of Chernobyl held in 25th and 26 April, 1986 are the classic examples of a cyber attack causing mass destruction in the physical world. The monitoring system at the nuclear plant was automatically operated by computer devices, which were claimed to be hacked illegally, ultimately resulting in a destructive blast. This disaster was backed by a cyber attack into the monitoring system at Chernobyl, thus, making it possible for an act of cyber terrorism to have affects in the physical world.

The high-profile terrorist attack at the world trade centre within the United States on Sept. 11, 2001 was also followed by an act of cyber terrorism. The terrorist attacks done via internet or other computer devices/ networks for the purpose of sabotaging important infrastructures so as to risk human life or inflict convulsion on a national lead to additional media coverage of the potential threats of cyber terrorism. Such acts might be direct or indirectly depending upon the target they wish to achieve. For example, the attacks on the infrastructure may be counted as direct attacks while the ones on the financial growth may be considered as indirect attacks.

Probably every individual has an easy as well as uninterrupted access to ill-gotten involvement inside the internet. The web of internet guarantees the merger of virtual as well as physical worlds which impact both the areas of reality; some consultants see this to be a strong incentive for nations to use it as substitute of terrorist groups in furtherance of achieving their personal/ political objectives. Various nations use their political powers and resources to meet their political agendas but since the scale of operation is high their reality is likely to be released, with the use of cyber terrorism it is most likely that the identities are hidden which makes it an attraction among such people.

IV. INDIAN CONTEXT OF CYBER TERRORISM

The cyber terrorism awareness is quite poor in India. This whole dark network is a breeding

 [ISSN 2581-5369]

ground for several activities that fall under cyber terrorism. In the year 2010 the website of India's prominent investigation bureau, The Central Bureau of Investigation, was hacked by some Pakistani hackers called 'Pakistani Hacker Army'. Besides this, the former Indian President while delivering his lecture in 2005 did laid emphasis on the problem of cyber terrorism. Yet India's approach towards this problem has been latent and there has been no profound system to be regarded as the cyber security system.

In the summer of 2011, India was hit by a virus attack at the newly constructed Terminal T3 of Indira Gandhi International Airport situated in New Delhi. "The check-in counters, transfers counters and boarding gates at the IGI are operated using the Common Use Passengers Processing System (CUPPS), maintained by Aeronautical Radio Incorporated (ARINC). The CUPPS operates on a common software-and-hardware platform that integrates all information such as an airlines reservation system, the expected time of departure and the capacity at waiting lounges. The problem in CUPPS started at 2.30 am on June 29 due to which check-in counters of all airlines at T3 became non-operational. This forced the airlines to opt for manual check-in and as a result passengers had to wait. There are around 172 CUPPS counters and only a third was functioning online, said an official. The investigation revealed that someone had hacked into the main server of the CUPPS and introduced a virus."[3] After 12 hours, with the help of several tech companies, the system was revived.

Despite the fact that the complexity of digital crimes has the power to gain digital criminologists from all around the world, digital law officials and social science experts in India do not initiate enough investigations to unravel the massive issue of virtual psychological oppression. The 26/11 attacks on the Taj Hotel in Mumbai may also be viewed as a wake-up call indicating the necessity for effective protocols to oversee cyber-terrorism attacks. According to an investigation into the 26/11 Mumbai attacks, Pakistani militants gained access to the property via web sources that revealed the map, floor layout, number of guests attending, and other details. Besides this the clear majority of the 26/11 location composition was likely to be organized fastidiously with Google Earth. Not only did the terrorists used the wed to plan or plot their attack but they also used other technical tools through which they could possibly convert 'audio signals into full fledged data' all this hindered the endeavors of Indian commandos to break the source from which the information is getting leaked. .

Despite the media's portrayal of an astounding fear-based autocrat assault on heavy traffic

[3] Tripathi Rahul (2011, September 25). 'Cyber Attack Led to IGI Shutdown'. *The Indian Express Newspaper*. Available at https://indianexpress.com/article/news-archive/web/cyber-attack-led-to-igi-shutdown/ (Last visited on 17/06/2021)

 [ISSN 2581-5369]

conditions and Jewish encampments in Mumbai, the Indian Ministry of Home Enterprises revealed a clear link between advanced media and fanatics' misuse of it in their annual report (2010); satellite telephones, GPSs, and various sites were all commonly used to carry out the terrorist mission. As per the information available for the 26/11 attacks, the perpetrators gained entry to the open computer properties at the Taj and Trident hotels. They accessed the hotel's computers to obtain information about the hotel's guests, notably the subjects from the United States and the United Kingdom that had remained there. Their goal was to target in-person guests by obtaining their room numbers from the INS computer's database. From the perspective of section 66F, the culprits purposefully disrupted India's unity, respectability, protection, or sway by infiltrating or accessing a PC asset without its authorization, striking fear, killing or wounding the person, and damaging or destroying property. The Information Technology Act of 2000 (as altered in 2008) has made strenuous attempts to protect, secured frameworks, as defined by Section 70. "By notification in the Official Gazette, the fitting government may declare any PC asset that specifically or round abruptly affects the Critical Information Infrastructure office to be a secured framework Furthermore, government efforts, such as the Information Technology (Cyber Cafe Guidelines) Rules, 2011, under the IT Act, include the death of tenets. The legislature had to strike a delicate balance between the fundamental rights to defence guaranteed by the Indian Constitution and the requirements of national security. With the rapid improvements in the digital field, digital fear-based oppression will take on new forms. With the growth and wide-spread use of long-range informal communication destinations and computerized media, India is facing new challenges in digital fear mongering. In the wake of conversational bits when the Assam prevalent uncovers the force of the latest face of digital psychological warfare in the country, India's parliament limited a total of eighty websites.

(A) Legal Provisions Dealing With Cyber Terrorism In India

The bomb explosion in 2010 at Varanasi followed by the bomb explosion in 2011 at Zaveri Bazaar of Mumbai pressurized the government for adapting a strong cyber security mechanism. Stirred by this, the govt. of India found the simplest way to bolster the digital security, including restriction of cyber terrorist exercises through the web by amending the present Indian Information Technology Act, 2000.

With the amendment in the Information Technology Act, 2000 India became the twelfth country in the world to administer digital law. Its major sections covering cyber terrorism is listed below:

 [ISSN 2581-5369]

1. SECTION 66F[4]: It was introduced in the IT Act, 2000 by way of the Indian Information Technology (Amendment) Act 2008. This section reads that,

1) "Whoever,—

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

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

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

(iii) introducing or causing to introduce any computer contaminant,

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under Section 70; or

B. knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, 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.]"[5]

2. SECTION 84B[6] – "Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act.

[4] Section 66F Punishment for cyber terrorism, Information Technology Act, 2000
[5] *Id.*
[6] Section 84B PUNISHMENT FOR ABETMENT OF OFFENCES, Information Technology Act, 2000

 [ISSN 2581-5369]

Explanation.--An act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment."[7]

3. SECTION 84C[8] – "Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence, or with both."[9]

V. OTHER GUIDING PRINCIPLES

1. "Implementation of Information Technology (It) Security Guidelines, 2000.
2. Information Technology (Certifying Authorities) Rules, 2000.
3. The Information Technology (Procedure and Safeguard for Interception Monitoring and Decryption of Information) Rules, 2009.
4. The Information Technology (Procedure and Safeguard For Blocking For Access Of Information By Public) Rules, 2009.
5. The Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009.
6. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
7. The Information Technology (Guidelines for Cyber Cafe) Rules, 2011.
8. The Information Technology (Electronic Service Delivery) Rules, 2011.
9. The Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties Rules, 2013."[10]

VI. INTERNATIONAL CONTEXT

Because of the continuous globalization, it has gotten simpler than before for psychological militant associations working on the national outskirts to share/ propagate data and collaborate with different associations, obtain geographic entries, and gain ammunitions from within the

[7] *Id.*
[8] Section 84C PUNISHMENT FOR ATTEMPT TO COMMIT OFFENCES, Information Technology Act, 2000
[9] *Id.*
[10] All these legislative Acts derive validity and authentication from the IT Act, 2000. These are established within the meaning of different sections of the IT Act, 2000.

country or beyond it. Right now, associations, including Islamic radical gatherings, are leading demonstrations of psychological warfare for the most part in nations and areas where the political circumstance is unsteady what's more, the administration is frail. In any case, it is said that the target of exercises and the capacities contrast from association to organization. A portion of those associations is attempted to be verifying assets through wrongdoings, for example, unlawful exchanges and kidnappings. In the case of Al-Qaeda, that is widely believed to have orchestrated the 9/11 attacks in 2001, Osama Bin Laden, the group's leader who was hiding in Pakistan, was assassinated in a US-directed operation. Regardless, the assassination of Bin Laden has not eliminated the possibility of Al-Qaeda attacks. While the Al-Qaeda initiative's ability to maintain order and control has deteriorated, it has been noted that other groups with the moniker "Al-Qaeda" in their name are expanding their dominance and fear-mongering mostly across North Africa and the Middle East. Other Islamic extremist fear-based oppressor organizations linked to Al-Qaeda are spearheading psychological oppression demonstrations mostly in North Africa and the Middle East, but also in many parts of South Asia and Southeast Asia. Those organizations are reported to have the potential to traverse national borders that are not well regulated and to conduct demonstrations of psychological warfare in countries other than those where they have bases of activity in Algeria, Libya, Mali, Iraq, Egypt, and Syria. When it comes to associations, it has been stated that they have amassed a large number of weapons, which multiplied when Libya's Gaddafi regime fell.

VII. MAJOR CYBER TERRORISM INCIDENTS

1. In the year 2008, the Ahmedabad bombings were a progression of twenty-one bomb impacts that hit the city on twenty-six Gregorian schedule months 2008, at interims a range of seventy minutes. Fifty-six people were executed and over 200 people were wounded. Ahmedabad is the social and mechanical heart of Gujarat state, and a larger than average piece of western India. The impacts were pondered to be of low force and were much the same as the city impacts, territory that happened the day preceding. Numerous TV channels previously mentioned they'd got an Associate in a Nursing email from a fear outfit alluded to as Indian group force asserting obligation regarding the dread assaults; monotheism aggressor bunch Harkat-ul-Jihad-al-Islamic, be that as it may, has asserted obligation regarding the assaults. The Gujarat police latent the suspected genius, Mufti Abu Bashir, related to 9 others, in association with the bombings.
2. Iraqi programmers upset troop arrangements during the Gulf War - In 1994, a 16-year-early English kid brought down nearly 100 U.S. protection frameworks. In 1997, 35 PC masters utilized hacking instruments uninhibitedly accessible on 1,900 sites to close down

enormous portions of the US power network. They likewise hushed the order and control arrangement of the Pacific Command in Honolulu. Since December 1997, the Electronic Disturbance Theater (EDT) has been directing web protests against different destinations on the side of the Mexican Zapatistas. At an assigned time, a great number of protestors guided their programs toward an objective site utilizing programming that floods the focus with quick and rehashed download demands. EDT's product has additionally been utilized by basic entitlements bunches against associations said to mishandle creatures. Electro - hippies, another gathering of hackers, directed web protests against the WTO when they met in Seattle in late 1999.

3. In 1998, a 12-year-old kid effectively hacked into the controls for the enormous Roosevelt Dam on the Salt River in Arizona, USA. He was in a situation to discharge rising waters that would have immersed Mesa and Tempe, jeopardizing in any event 1 million individuals.
4. In 1998, Spanish protestors barraged the Institute for Global Communications (IGC) with a great many counterfeit email messages. Email was attached up and undeliverable to the ISP's clients, furthermore, bolster lines were tied up with individuals who couldn't get their mail. The protestors too spammed IGC staff and part accounts, stopped up their Web page with fake charge card requests, and took steps to utilize similar strategies against associations utilizing IGC administrations. They requested that IGC quit facilitating the site for the Euskal Herria Journal, a New York-based distribution supporting Basque freedom. Protestors said IGC bolstered fear-mongering in light of the fact that an area on the Web pages contained materials on the psychological oppressor bunch ETA, which asserted duty regarding deaths of Spanish political and security authorities, and assaults on army bases. IGC at long last yielded and pulled the site due to the "mail bombings".
5. In 1998, ethnic Tamil guerrillas overwhelmed Sri Lankan government offices with 800 messages per day over a fourteen-day time span. The messages read, "We are the Internet Black Tigers and we're doing this to upset your interchanges". Knowledge specialists portrayed it as the first known assault by fear-based oppressors against a nation's PC frameworks.
6. NATO PCs were struck with email bombs and disavowal of administration assaults by hackers fighting the NATO bombings during the Kosovo conflict in 1999. According to reports, organizations, open groups, and educational foundations received highly politicised virus-laden communications from a variety of Eastern European countries. Destruction of the web sources was also common.

 [ISSN 2581-5369]

7. In 2001, in the scenery of the downturn in US-China connections, the Chinese programmers discharged the Code Red infection into nature. This infection contaminated a large number of PCs around the world and afterward utilized these PCs to dispatch forswearing of administration assaults on US sites, noticeably the site of the White House.

VIII. CONCLUSION

Change is inescapable, and the challenges that progress in technology brings can't be kept at a strategic distance. Currently, lawbreakers have changed their tactics and began relying on cutting-edge technology, as well as the overall public, the lawful, and thus the implementation experts, quasi organizations and associations will discover a workable pace with their system to combat it. Another aspect that must be featured is that a culture of persistent digital training and learning must be instilled among the legitimate and in this manner the authorization specialists on account of data the data dynamics might be able to maintain a secure web security system.

The prelude of the Information Technology Act, 2000 furnishes that the Act was passed with the focus to offer lawful acknowledgment for exchanges managed by proposes that of electronic data trade and diverse proposes that of online business, additionally other Acts have conjointly made changes to the Indian penal code,1860, Indian Evidence Act 1872, The Bankers Books Evidence Act 1891, for encouraging legitimate acknowledgment and guideline of the business exercises in spite of the fact that this goal of the Act isn't to stifle the crime, anyway this demonstration has sketched outbound offenses and punishments to overwhelm such exclusions, that is known to return inside the portrayal of cybercrimes.

From this, it might be surmised that the law can't bear to be static; it is ought to change with the dynamical occasions and viz. with the technological advancement the country had introduced supporting laws. But the point of concern is that this area of cyber terrorism is still taken very casually by the authorities. Despite the fact that the major attacks are made possible by technological support, this field has never been on priority.

The general population should be made aware of the dangers of the cyber world and the ways in which a person may combat a dark situation bred from cyber terrorism. The government must introduce measures that can go an all-encompassing strategy in setting up a safe digital territory wanted by the voters.

*****

 [ISSN 2581-5369]