A Study of Acts of Terrorism through Cyberspace in India

Arzoo
Department of Law
Vivekananda Global University, Jaipur
Email ID: aarzoo.bishnoi@vgu.ac.in

ABSTRACT: ***Cyber crime is a serious threat to national security by giving the architects of terror a shield of anonymity. In civilizations, malicious scripts, malware, worms and other new threats, such as electric pulse bombs and high-energy radio frequency weapons, are now causing mayhem. Since the last decade, India has been subjected to this form of devastation relentlessly. The execution was carried out primarily by an assistant in cyberspace from the 26/11 attacks in Mumbai in 2008 to the Pathankot attack in 2016. China has compromised into India's official networks in countless cases, enabling it to remove such networks throughout any confrontation. Inter-Service Intelligence (ISIS) and numerous non-state Islamic jihadists from Pakistan have terrorized civilians exponentially by manipulating people's mindsets. India lacks a robust law to deal with cyber-terrorism, facing certain challenges. The paper was split into two parts. This paper addresses the increasing cyber terrorism events in India, the definition and principle of the word, the purpose and mechanism behind an attack, and the dangers involved. The legal provisions on the national level, international governance and how cyber terrorism could be a greater threat and the future and how to combat it are discussed as well in this paper as well stating facts briefly about the cyber-crimes. This paper also explains in brief the prevention and remedies.***

Keywords: Crime, Cyber, Law, Section, Terrorism, Law and Order, IPC, Guidelines.

INTRODUCTION

The third release of the 'Worldwide Terrorism Index 2015' positioned India as the 6 th country generally troubled by terrorism out of 162 countries. Terrorism has tormented India since long back and different State and Non-State entertainers can be put to fault. In any case, huge changes in the patterns of terrorism might be noted with the movement in innovation and the expanding reliance of individuals on the equivalent for every one of their exercises [1].

The utilization of web in executing terrorism in India can be followed back to the assault on the Indian Parliament in 2001 when the logo and a ton of other data relating to the Ministry of Home Affairs and the format of the Indian Parliament were taken with the assistance of data innovation. Afterward, a PC was seized through which the email arrangement of the Indian Army was controlled through Pakistan's Internet Service Provider [2].

Since 2006, the Chinese have been threatening the Indian government and private substances by releasing cyber assaults reliably on their PC frameworks, and have been following the authority organizations, accessing the arranged data on various events; which has enabled them not exclusively to abuse such data, yet additionally to handicap any or all the organizations during disparity on any topic and along these lines, get out of line advantage. The Mumbai assault on 26/11/2008 is another case when far reaching awfulness and fear struck the country by the method of data innovation, for example, the utilization of Global Positioning Satellite frameworks, Voice over Internet Protocol, and so on During the 2010 Commonwealth Games in India, the authority sites of the Prime Minister's Office and different Government of India sites with the area name 'nic.in' were hacked. The assault was conceivably sourced by a state-entertainer, maybe having Chinese inception, and had gone on for a very long time thusly prompting tremendous information misfortune and in excess of 70 casualties including various American government workplaces and business [3].

Majority of the assaults on India have so far been accounted for to come from Pakistan, China, Bangladesh, Iran, Brazil, Turkey, Saudi Arabia, UAE, Algeria, Europe and the United States. From 2001 to 2015, India has endure in excess of 57 dread assaults in which cyberspace was the head battleground including the 26/11 Mumbai bloodletting and the Pathankot strike for which basic data was scythed with the assistance of phony Facebook profiles. Another approaching danger is from the Islamic State (ISIS) who have presently been focussing on imparting their messages strategically to the individuals across the world and assemble enthusiastic aficionados by influencing their philosophies about religion, governmental issues, and so on In 2015, a 16 year old young lady structure Pune, Maharashtra was captured by the Anti-Terror Squad who was indoctrinated into leaving the nation to join the Islamic State of Iraq and al-Sham (ISIS) by Sirajuddin, an ISIS enrollment specialist, working at the Indian Oil Corporation, who was likewise captured at Jaipur, Rajasthan [4].

The youngster had been in contact with around 200 IS supporters through cyberspace and uncovered their arrangements of extension outside Syria and a huge assault on the Indian sub-landmass constantly 2020. The young lady was a guiltless youthful juvenile who was an outstanding understudy being taught in a religious circle school. Nonetheless, influenced by the ISIS, she completely changed her method of living and embraced wearing burqa and was controlled to go along with them as a self-destruction aircraft. Another episode includes a 'jihadi suspect', Mehdi Masoor Biswas who was an ally of the IS exercises and posted them on his Twitter account, "Shami Witness" putting the inquiry under the steady gaze of the Indian courts that whether 'open philosophical help' would add up to terrorism. The latest assault on the Indian Defense Personnel was dispatched supposedly, by the Pakistan Intelligence Agencies by fooling them into downloading an application on their telephones, called "SmeshApp" [5].

The application is empowered to assemble all the data including telephone logs, instant messages, messages and area through the GPS and conceivably photos can clandestinely be taken from the debased telephone. The application is considered to have perhaps helped the Pathankot assault in January 2016. The expanding quantities of forceful assaults in the cyberspace plainly demonstrate that terrorism is not, at this point limited to the customary techniques for self-destruction bombings, explosives and mass decimation. Alongside the headway of innovation and expanding dependence of the individuals everywhere on the world on the web, even terrorism has advanced with new risky angles. These cases obviously show that the psychological militants have discovered the absolute worst use for the most trend setting innovations. These demonstrations of execution of terrorism in the cyberspace that regularly bring about real demolition of life and property can be named as 'cyber terrorism' [6].

THE CONCEPT OF CYBER TERRORISM

Each analyst understands various thoughts regarding cyber terrorism. Be that as it may, the most acknowledged comprehension of the idea is the utilization of web for doing psychological oppressor exercises. As per Dorothy Denning, a main master in the field, cyber terrorism can be alluded to the "unlawful assaults or dangers of assaults against PCs, organizations, and data put away in that, when finished with the aim to scare or constrain an administration or its kin, or in facilitation of political or social destinations". The definition centers around the unapproved clients who access data by various methods of cyber assaults with the expectation to undermine and make hurt the public authority and the general public, and accomplish political and social goals. Such assaults might be made inside or outside the association by utilization of inner or outer organizations. Different definitions by various specialists center upon shifted viewpoints, for example, source and focus of the assault, goal of the psychological militants, implies utilized in this way and the results of the assault.

The Federal Bureau of Investigation gives an understanding as, "the terrorizing of regular citizen endeavor using high innovation to achieve political, strict, or philosophical points, activities that bring about crippling or erasing basic foundation information or data." The arrangement for the offense of cyber terrorism in India

has been given under Section 66F of the Information Technology Act, 2002 endorsing detainment stretching out to life as discipline for the equivalent.

It characterizes the demonstration of cyber terrorism as:

A. "Whoever with expectation to undermine the solidarity, trustworthiness, security or sway of India or to strike dread in the individuals or any section of the individuals by—

(i) Denying or cause the refusal of admittance to any individual approved to get to PC asset;

(ii) Endeavoring to infiltrate or get to a PC asset without approval or surpassing approved admittance;

(iii) Introducing or causing to present any PC foreign substance

Furthermore, by methods for such lead causes or is probably going to make passing or wounds people or harm to or pulverization of property or upsets or realizing that it is probably going to cause harm or disturbance of provisions or administrations fundamental for the existence of the local area or antagonistically influence the basic data framework determined under Section 70; or

B. Purposely or deliberately enters or gets to a PC asset without approval or surpassing approved admittance, and by methods for such direct acquires admittance to data, information or PC data set that is confined for reasons of the security of the State or unfamiliar relations; or any limited data, information or PC data set, with motivations to accept that such data, information or PC data set so got might be utilized to cause or liable to make injury the interests of the sway and uprightness of India, the security of the State, amicable relations with unfamiliar States, public request, respectability or ethical quality, or corresponding to disdain of court, criticism or induction to an offense, or to the upside of any far off country, gathering of people or something else, submits the offense of cyber terrorism."

The degree and degree of the idea in the Indian resolution has been explained upon in the second piece of the paper. In any case, it very well may be found that cyber terrorism involves assaults made through PC frameworks and organizations against the public authority or residents of the country, with certain social, philosophical or political reasons and the thought process to undermine, scare or cause actual decimation to life and property and execute fear and savagery in the general public which may bring about blasts, devastation of life and property and basic monetary misfortunes.

THE MOTIVE AND METHOD BEHIND AN ATTACK

The ‘cyber terrorists’ may have multiple agendas behind cyber-attacks such as to send out their message to the government and the society, recruit supporters or brainwash the innocent, raise funds for their unlawful activities, demand ransom, gather critical information so as to enable them in further acts of terrorism, preparation for physical attacks, destruction of critical or classified information so as to disable the government to take measures or actions against them or harm the governance system, peace and order in the nation. The most vulnerable targets to cyber terrorism includes the government, military, critical national infrastructures, social and national identity and private entities. Cyber terrorism can take distinctive forms. In December 24, 2008, the official website of the Indian Eastern Railways was hacked into by Whackerz-Pakistan.

The website displayed unusual and offensive notes including threats for future cyber attacks and ‘to save the motherland from turning into pieces.’ The visitors to the website were also attacked by the Trojan virus and it had taken nearly three hours to secure the site. Such a method of cyber attack is often used by ‘hacktivists’ who hack into the websites or database of multinational corporations or government as a hostile response to their actions and make political statements, threats or demands or sometimes for the purposes of fraud, identity theft or to steal information. The attacker often vandalizes the authorized content displayed on the official website and puts on view the messages he wants to convey. Such an act amounts to ‘website defacement’. Besides hacking into a system or a website, an attacker might remotely control programs

installed on a system through 'bots' and gain control over a large number of computers which, after gaining control over them, are called 'zombies'[7].

The Indian metros across various cities including Mumbai, Delhi, Bangalore, Cochin, Hyderabad and Pune have reported an alarming rate of 65% of infection. In 2014, India ranked as 16th most bot-infected country in the world. Another mode of attack may involve use of a software program, such as key logger, which observes and registers the keystrokes of a user and passes the classified information to the accessed data such as passwords, to the attacker. In January 2015, the American chain of Hyatt Hotels Corporation were attacked worldwide with a malware to collect details of the payment card of its customers, including 20 out of the 23 hotels in India. This is an instance of a cyber attack through malwares or viruses whereby the invader infects the network by means of e-mails, attachments, or even a Wi-Fi connection. Another mode of attack may involve Denial of Service (DoS) or Distributed Denial of Service (DDoS) whereby the attacker floods the targeted system with traffic, junk data etc, so as to prevent the access to the targeted website or computer which usually crashes down and is rendered inoperative for effective communication [8].

Usually, the attack originates from multiple sources and it becomes difficult to detect the legitimate user traffic making it impossible to obstruct the overwhelming requests to the targeted system by blocking the IP address. In April 2015, the Telecom Regulatory Authority of India (TRAI) had released a consultation paper for the citizens to assert their opinions on the debate of net neutrality. Over 1 million of the names email addresses of people who posted their views on the debate were leaked by the TRAI. Subsequent to that, a group called 'AnonOpsIndia' brought the website down and disclosed that they launched a DDoS attack as revenge for leaking the details and making those people vulnerable to hackers and spammers.[9] These attacks are no longer restricted to websites or computer systems anymore. The threat has reached to the 'Internet of Things (IoT) or internet connected devices' including smart TVs, refrigerators, printers, etc. Very recently, 25,000 CCTV cameras were usurped to jeopardize other services 'from 105 countries with an aggregate of 25,513 unique IP addresses within a few hours'. The researchers claimed it to be a massive 'Layer 7 DDoS attack that overwhelmed Web servers, occupying their resources and crashing websites'[10].

CONCLUSION

Technology dependency and internet dependence have provided terrorists with a new medium for targeting and causing large-scale damage in a very easy, low-cost and high-speed way. The idea of targeting a country's national security electronically would seem more plausible when an attacker is permitted to work remotely from anywhere in the world and it would be virtually difficult to identify him. Computer protection breaches will go undetected unless there is very good security software that denies unwanted access to sensitive data. Cyber terrorism can not only cause destruction on computers or the internet but can cause large scale devastation, cost thousands of lives and demolition of property which may lead to grave damage to the financial state of a nation and complete breakdown of the nation's critical infrastructure denoting "all those assets or parts thereof which are essential for the maintenance of critical societal functions, including the supply chain, health, safety, security, economic or social well-being of people whose importance is such that any entire or significant loss or impairment of function could cause serious damage to human welfare, environment and to the national security or economy.

Cyber-terrorism, though, is not entirely a mental speculation. And if it is known that terrorists have not triggered a large-scale attack to the point of totally destroying a country and terrorizing the population at its heart, it cannot be assured that it will be absolutely unlikely in the near future. To date, cyberspace has proved to be a successful tool for physically demolishing extremely casualty-rate national sensitive infrastructure or pressuring a government to extort ransom or satisfy any demand by terrorists for any stipulation. Since cyberspace has a great deal of potential to cause widespread damage without the possibility of publicity at costs far lower than real terrorism, with evolving technology, terrorists will invest in developing modern and lethal 'cyber weapons.' The government should not set its feet up in the

expectation that cyber warfare is not likely to be undertaken by terrorists as a way of striking and can devote money to develop steps to curb the potential for cyber threats of any sort.

REFERENCES

[1] N. Kshetri, "Diffusion and effects of cyber-crime in developing economies," *Third World Q.*, 2010, doi: 10.1080/01436597.2010.518752.

[2] H. S. Lallie *et al.*, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the paandemic," *arXiv*. 2020.

[3] A. Bendovschi, "Cyber-Attacks – Trends, Patterns and Security Countermeasures," *Procedia Econ. Financ.*, 2015, doi: 10.1016/s2212-5671(15)01077-1.

[4] R. Broadhurst, "Developments in the global law enforcement of cyber-crime," *Policing*, 2006, doi: 10.1108/13639510610684674.

[5] K. Dashora and P. P. Patel, "Cyber Crime in the Society: Problems and Preventions," *J. Altern. Perspect. Soc. Sci.*, 2011.

[6] A. Guinchard, "Between Hype and Understatement: Reassessing Cyber Risks as a Security Strategy," *J. Strateg. Secur.*, 2011, doi: 10.5038/1944-0472.4.2.5.

[7] P. M. Tehrani, N. Abdul Manap, and H. Taji, "Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime," *Comput. Law Secur. Rev.*, 2013, doi: 10.1016/j.clsr.2013.03.011.

[8] B. Akhgar, A. Staniforth, and F. Bosco, *Cyber Crime and Cyber Terrorism Investigator's Handbook*. 2014.

[9] Detica, "The cost of cyber crime," 2011.

[10] C. Wilson, "Cyber crime," in *Cyberpower and National Security*, 2011.