How to Cite:
Chanda, A., & Verma, M. (2022). Critical evedenciarcy analysis of 26/11 attacks with reference to cyber-terrorism. *International Journal of Health Sciences*, *6*(S2), 10011–10025. https://doi.org/10.53730/ijhs.v6nS2.7663

Critical evedenciarcy analysis of 26/11 attacks with reference to cyber-terrorism

Abhijit Chanda
Research Scholar, Sharda University

Muskaan Verma
Legal Researcher

***Abstract*---**By thorough analysis of Mumbai terrorist attacks of 26/11, it was observed that the attacks were form of Cyber terrorism as it was done to convey particular destructive message to the government, sending of threatening emails, defacing of government websites, hacking and cracking of crucial government systems. 'Protected systems' were compromised and civil amenities were disrupted. Digital information systems computer networks which not only affected governing system but also the population of a target area was affected to create a panic or situation of threat. Computer and digital communication networks were main tools of extremists in this case. Also, Supreme Court judgement on Mumbai Attacks case, in para number 57 specifies about use of Google Earth, tampering with telecommunication networks and digital networking shows that the Attack was done by was done by Hi-Tech offenders. Although electronic eavesdropping often yields valuable data, even tantalizing clues can be missed if the technology is not closely monitored, the intelligence gleaned from it is not linked with other information, or analysis does not sift incriminating activity from the ocean of digital data as traced by Inteligence agencies of US, UK and India during investigation of attacks.

***Keywords*---**critical evedenciarcy, cyber-terrorism, Mumbai attacks case.

Introduction

Cyber terrorism has been a risk since the advent of the Internet. In the age of information technology, the terrorist has acquired expertise to produce the lethal combination of weapon and technology which has taken method of terrorism to new dimensions which are more destructive and deadly. To accomplish the goal, cyber terrorist targets the computer system that control air traffic, electric power

grids, telecommunication networks, military command system and financial transactions. By targeting these methods cyberterrorism is now used to plan many terrorist attacks. The term of cyberterrorism refers specifically to different actions, including transmitting online propaganda, manipulating or deleting information, and even planning and conducting terrorist attacks through the use of communications networks.

The paper will analyse the attacks of the 26/11 Mumbai which would show how the usage of cyber technology by terrorists to target the population and places, created devastating results. The meticulous planning done with Google Earth and use of "cellular phone networks" for command and control to track and thwart the efforts of Indian commandos. The conversion of audio signals into data before transmission left Indian security forces clueless to detect and intercept the attack at given level of infrastructure and capacities. The paper envisages a comprehension of these terrorist activities which took place in Mumbai from 26 November to 29 November, 2008. The series of digital assaults, collection and admissibility of evidences and aftermath of the attack on Indian cyber security system.

Nexus between 26/11 and Cyber Terrorism

Concept that conjuring up images of vicious terrorist unleashing catastrophic attacks against computer networks, wreaking havoc and paralyzing nations. Cyber terrorism, two greatest fear of modern times from a psychological perspective are combined to form this[1]. The fear of random, violent victimization segues well with the distrust and outright fear of computer technology. In recent times, terrorists maybe more dangerous with keyboard then with bomb[2].The concept of Cyber terrorism is not new to the world, the issue has been raised in 9/11, in Kosovo Conflict in 2001 and also in Internet Black Tigers attack on Sri Lanka in 1997[3]. Cyber Terrorism not only include cyber-attacks but also sending of thread messages, defacing of websites, disrupting internet communication for government services as well as civil amenities. Cyber terrorism has emerged as a new phenomenon in India, in past in Ahmedabad, Delhi, Jaipur and Bangalore serial blasts in 2008, considerable evidences of cyber terrorism was found[4]. Also 2010 Varanasi blasts traces of cyber terrorism were found[5]. This chapter focuses on how elements of cyber terrorism were used to conduct the attacks of 26/11 in Mumbai in 2008.

Attacks of 26/11 on link with Cyber terrorism

[1]Syed Umarhatab 'Cybercrime and Digital disorder'(2011) <https://www.researchgate.net/publication/228192670_Information_Technology_Act_and_Cyber_Terrorism_A_Critical_Review> accessed on 10February 2020

[2] ibid

[3] Debarati Halder 'Information Technology Act and Cyber Terrorism: A Critical Analysis' (2012) <http://www.mit.gov.in/sites/upload_files/dit/files/RNUS_CyberLaw_15411.pdf > accessed on 12 April 2020

[4] Bureau, Ministry of Home Affairs, Government of India, New Delhi, India

[5] ibid

Most of the terrorist incidents in India involve Muslim jihadists like Indian Mujahideen[6]. Extreme usage of Cyber communication could be established in these attacks starting from spreading of terror messages, targeting state heads and claiming responsibilities for the attacks. Cyber terrorism ensures that present day devices drawing out that psychological militant isn't just fixated on my EIDs and AK 47 but also utilisation of workstations, tablets and personal computers[7]. Cyber terrorism is a critical condition on two grounds, first being, there is no knowledge or awareness about cyber terrorism to general public. They are not aware of cybercrimes, threats or basic computer knowledge. Second, they are more dangerous in nature because it is difficult to establish connection between attack and the cyber security[8].

The main aim of cyber terrorists today is to cripple critical infrastructure of a country by cyber-attacks to further the causes they espouse for as a terrorist group. Cyber terrorism includes two main types of activities, viz., cybercrime and misuse of Information Technology and therefore it would not be wrong to assume that cyber terrorism is a new time of Cybercrime. There has been a analysis of legal issues involved in cyber terrorism in India post 26/11 Mumbai attacks. 2008 attacks created some devastating results in India and minute analysis would show that cyber communication between territories and usage of Cyber Technology acquainted with the target population and the place created the same[9].

In *Ajmal Amir Kasab vs State of Maharashtra*[10], it was held that the attacks was planned meticulously with Google Earth. The use of cellular phone networks for command and control of the movements of Indian commandos were controlled, the use of social media to track and thwart the efforts of Indian government were used by the terrorists. The same was monitored by the people who coordinated these attacks sitting in Pakistan and other parts of the world quite easily. Terrorists manage to convert audio signals to data before transmission. Considering the current situation of infrastructure and capabilities, it became very difficult for Indian security forces to intercept the signals or to match expertise demonstrated by terrorist which bore hallmarks of professional team in Computer technology. Therefore it was simply established that Computer Network operations (CNO) were used by terrorist as a tactic in their operations[11].

Elements of Cyber Terrorism in attacks of 26/11

---

[6] National Crime Records 'Crime in India: 2011-Compendium' (2012)

[7] Talan Singh 'Cyber Law and Information Technology' (2011)

[8] Yogesh Barua and Denzyl P.Dayal 'Cyber Crimes' New Delhi: Dominant Publishers and Distributors (2001)

[9] Cyber Terrorism: The Fifth Domain <http://www.indiablooms.com/MedleyDetailsPage/medleyDetails040612a.php> accessed on 15 March 2020

[10] Criminal Appeal Nos.1899-1900 Of 2011

[11] Mihir Agrawal, and H.R. Rao., ' Information control and terrorism: Tracking the Mumbai terrorist attack through Cyber Security' (2011) Economic and Political Weekly 251

Judgement of Ajmal *Amir Kasab vs State of Maharashtra,* established the elements of cyber terrorism with Mumbai attacks of 26/11[12]. Computer viruses and worms are most popular weapon used in cyber terrorism. While analysing the attacks cyber terrorism was also referred as 'computer terrorism'[13]. Attack on computer infrastructure of the country can be classified into three categories:

1. Through physical attack computer infrastructure was damaged by conventional method of attacks like bombing fire stone pelting etc. This results in damaging of personal and public property in large scale. Through these conventional methods Information Technology structures is highly compromised. In Mumbai attacks it was seen that through firing and gunshots computer technology split the difference[14]. The internet connections and telecommunication signals were cut off.
2. Synthetic attack is a second type of category where computer the structure is damaged by introducing a delay or a system which makes the system unpredictable and modifying the logic of the system[15]. This could be done by putting computer virus into the system or use of trojens[16], it affects android devices specifically bye attacking the routers on their wireless networks. This was compromised by India security system and were hacked by the terrorist's organisations. The Indian cyber security was compromised terrorist was successful to get unauthorised access through hacking and other Technologies like packet sniffing, Tempest attack, password cracking and buffer outflow[17]. This shows that the terrorist had intention not only to attack the people in the country but also intelligence security.
3. 3. The last type of category is semantic attack, it is the most dangerous type of computer terrorism as it exploits this system during entering and exiting the system without users knowledge to induce errors. India is shifting gears for entering into the facets of e-governance. This category was not symbolically present in the attacks but also all together cannot be neglected. The militants used web based live to track and obstruct the endeavours of indian public and security forces.

The digital correspondent showed by militants in during the 26/11 attack, stirred the Government of India to find a way to reinforce the digital security. Indian ministry of Home Affairs in their annual report of 2010 discharge a definite nexus between computerized innovation and abuse of same by fanatics, satellite

---

[12] ibid

[13] Mithila Nehla Hani and Rajan Awasthy, 'Critical Analysis of Cyber Terrorism with special reference to Attacks of 26/11' (2018) International Journal of Pure and Applied Mathematics 1165

[14] ibid

[15] M. Cereijo, 'Cyberterrorism and Cyberwar' (2006) <http://www.lanuevacuba.com/archivo/manuel-cereijo-110.htm> accessed on 26 February 2020

[16] Switcher Trojan, it infects users' devices to attack the routers on their wireless networks. Cybercriminals could redirect traffic on the Wi-Fi-connected devices and use it to commit various crimes

[17] ibid

telephones, GPS and different websites to satisfy the mission[18]. Report also showcase is that culprits accessed the personal computers assets available in Taj Hotel and Oberoi Hotel. The intention behind this was to download the guest list and can access the visitors record particularly coming from United States of America and London and to track list of people present in the hotel at that point of time[19]. By getting infiltrating into the PCs of these hotels, the terrorists tried to debilitate solidarity, respectability, struck fear and to harm and devastate propert.

Handling and admissibility of Digital Evidences

Digital evidence is material processed or distributed in a digital form that can be counted on by the court. This can be stored on a hard disk, a cell phone, and other items. Online evidence is generally related to cybercrime or e-crime, such as underage pornography or payment transaction fraud.[20]

Collection and Handling of digital evidences

Digital evidence is sensitive and frail, and the poor management of this evidence can modify it. Due to its high variability and fragility, procedures need to be followed to ensure that data is not changed during its handling (i.e. during entry, processing, packaging, transfer and storage). Such guidelines detail the steps to be taken when treating digital evidence. The initial handling of digital evidence includes four phases: recognition, compilation, storage and preservation. [21] The Intelligence agencies of India collaborated with that of UK and US to analyse the cyber impact of the attack and collect evidences. The role of Zarrar Shah, a computer expert and the tech-chief of Lashkar-e-Taiba was found eminent in this aspect. In the reports, they wrote how Google Earth was used to get route for target cities. They collected an internet phone from him which he used to disguise his location by routing calls to New Jersey. They also found 'virtual numbers' and DID numbers with country code of Austria and of United States. Intelligence agencies in UK, US and India tracked co-operators and deployed high-tech surveillances tools in advance of Mumbai attacks. In the charge sheet submitted, Satellite phones and GPS sets which consists of coordinates of the city in about 12 pages were filed as annexures. The collection of various Transcripts which was also produced in the court was collected from Lashkar's control room in Pakistan along with some telephonic intercepts[22].

On 26 November 2008, the terrorist attack in Mumbai was in communication with Pakistan on a full-time VOIP mobile, as well as all the computer systems in Taj Hotel, Leopal Cafe, Shivaji Maharaj Terminus, Obroi Trident, Cama Hospital, Nariman House were infiltrated, they had exposure to all the hotel and other

---

[18] Col SS Raghav, 'Cyber Security in India's Counter Terrorism Strategy' (2010) <ids.nic.in> accessed on 10 march 2020

[19] *Mohd. Ajmal Amir Kasab v. State of Maharashtra*, (2012) 9 SCC 1

[20] Digital Evidence and Forensics, <https://nij.ojp.gov/digital-evidence-and-forensics> accessed on 3rd April,2020)

[21] Handling of digital evidence, < https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html> accessed on 3rd April,2020

[22] Glance James, 'Attacks of 2008, Piles of Spy' The New York Times (2014)

location info. They had the entire itinerary of the Taj Hotel sign in time, room number, etc. Basically, they were targeting a foreign visitor from the U.S. and England and elsewhere. Since they had exposure to all the cafe's records, the hospital had a clear list of people they wanted to tar the doors. The blast lasted four days and terrorist were connected to Pakistani hacker all the time. 26/11 was among the significant events in our nation that prompted the government to think about the data security and cyberattack which might arise in a nation like India, and what measures the state might take through with these Attack Reports indicate that the perpetrators used Google Earth to prepare their operations and decipher the architecture of their locations – two hotels, a railway station., and a Jewish centre in the Indian capital, Mumbai.[23]

After discovering forensic evidences in the case of *Md. Ajmal Md. Amir Kasab @Abu vs State of Maharashtra*[24] during investigation these evidences were send to FBI to properly handle the evidences and make them admissible in the court as described during the trial

"341. The Thuraya satellite phone and the GARMIN GPS recovered from MV Kuber, along with four other GPS devices recovered from the other sites of terrorist violence, were sent for forensic examination to the United States Federal Bureau of Investigation (FBI)[52] where the data stored in the GPS devices were analysed by Daniel Jackson (PW-152) who was working in the FBI as Electronic Engineer/Forensic Examiner. He had vast experience in his field of specialty, particularly mobile phones, GPS devices, I-pods, etc., and he stated before the court that before examining the devices sent by the Mumbai Police, he had examined over a thousand electronic devices in the Bureau's laboratory."[25]

In the Mumbai attack it was important for the forensic evidences to be handled in proper way so as to bring proper justice to the case and Indian investigatory system not being adequate enough at that time to handle such a delicate evidence it was important to handle these evidences to experts because Finally, the analysis of the incident for the investigation process uses limited information to make inferences about the case on the basis of available facts and proof investigation. For the above context, it is crucial for cyber-crime analysts and digital forensics experts to consider these shortcomings and resist bias perceptions of the findings of such analyzes, such as those arising from confirmation bias, where persons try and endorse findings that favor their work hypothesis and reject results that disagree with their research assumption.[26]

Admissibility of forensic Evidences

Such legal and technological standards must be fulfilled in order to ensure the constitutionality of digital evidence before a court. So far as the prior is

---

[23]Carvell, A. (2008, 11 December), *Indian lawyer has Google Earth in his sights*, < http://www.geek.com/articles/news/indian-lawyer-has-google-earth-in-his-sights-20081211/> accessed on 3rd April,2020

[24] AIR 2012 SC 3565

[25]Ibid 19

[26] Ibid 2

concerned, the court discusses the legal approval for the execution of searches and seizures of communication and information technologies and associated data and the validity, accuracy, credibility and accuracy of digital evidence. In regard to the above, the Court thoroughly discusses the digital forensics techniques and methods used to collect, store and evaluate forensic evidence; the virtual laboratories in which analyses are carried out; the reports of digital forensics experts; and the professional and academic credentials of digital forensics experts and forensic experts. [27]Cyber Forensics in order to admit an evidence needs to go through process of developing and documenting, followed by assessment of potential evidence. Preserving the integrity of the potential evidence is must and finally examination of data within appropriate databases.

Changes in Indian Evidence Laws For Admission of Cyber Evidences

The law relating to admissibility of evidence in India is dealt under Indian Evidence Act, 1872. Prior to the enactment of the Information Technology Act, 2000, electronic evidence obtained by all ways, namely cyber forensics, was regarded as a record and supplementary proof of these digital "documents" was generated by means of printed reproductions or transcripts, the validity of which has been confirmed by the qualified signatory. The signatory must recognize his signatures in trial and be subject to cross-examination. All of this was achieved in compliance with the requirements set out in provisions 63 and 65 of the Evidence Act.[28]

The IT Act modified Section 59 of the Evidence Act, 1872 in order to exempt electronic information from the probative power of oral testimony in the same way as it excluded papers. It is the re-application to digital archives of the documentary hearing law. However, instead of sending digital records to the secondary evidence test-which, for documents, is found in Sections 63 and 65, it introduced into the Evidence Act two new evidence rules for electronic records: Section 65A and Section 65B. The purpose of the legislature is to enact new laws which derive from the technological design of the evidence, especially since the evidence in electronic form cannot be generated in the court of law by reason of the size of the computer/server, which resides in the machine language and therefore needs the interpreter to read the same.[29]

In the case of Mumbai Attack the evidences although were declared admissible to the court after being examined and handled by FBI Experts were not particularly used during the trial due to presence of any other primary evidences as well as eye witnesses.

“103. In regard to the CST episode, like all other parts of the case, the prosecution has gathered a very large amount of evidence: ocular, forensic and of other kinds, e.g., CCTV recordings.[4] They have documented practically every action and

[27] Ibid 2

[28] Aneesh V Pillai, ‘Admissibility Of Digital Evidences: An Overview Of The Legislative And Judicial Perspectives’ 2016 (2) Elen. L R

[29] Vivek Dubey, ‘Admissibility of electronic evidence: an Indian perspective’ (2017)Forensic Research & Criminology International Journal 4(12)

movement of the two killers from the point when Abu Ismail threw the first hand grenade[5] at the passengers on the platform till they went out of CST through the foot-overbridge on the side of platform no.1 of the local lines (and thereafter….). On the basis of the ocular evidence alone (not taking into account for the moment the other evidences) the prosecution has presented before the court a vivid and photographic (figuratively and actually) account of the CST events. Here we propose to examine in slightly greater detail four witnesses whose evidence, in one way or another, has some special features, and then to take an overview of some more witnesses to construct a broad picture of the massacre at CST."[30]

Aftermath of Mumbai attack 26/11: Amendment in IT Act, 2000

In India, cyber terrorism has emerged as a modern phenomenon. The 2008 recurring blast investigation in cities such as Ahmedabad, Delhi, Jaipur, and Bangalore found significant traces of cyber terrorism including the 2008 attack on the Mumbai Taj Hotel, now known as 26/11. All of these reported incidents suggest two core elements of cyber terrorism, namely, the collection of intelligence and the dissemination of terror through electronic communications to threaten national security and stability.[31]

Following the incident on 26/11, the Indian parliament adopted a series of new provisions to the Information Technology Act 2000, which includes broad provisions to counter cyber terrorism. Section 66F of the law addresses cyber security in the broadest context.[32]

Sec. 66(f) of the said Act reads as to the following effect- "Whoever:- (A) With the 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) By 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 to damage to or destruction of property or disrupts or knowing that it is like to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or (B) Knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons for the security of the state or foreign relations, or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the state, friendly relations with foreign states, public order, decency or morality,

[30] Ibid

[32] <https://www.hyderabadpolice.gov.in/acts/ITAct2000-2008(amendment).pdf> (accessed on 4th April,2020)

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."[33]

In addition, this law sets out the sanctions to be enforced on cyber-terrorism offenders. Section 66F(1)B), which describes "cyberterrorism" is far too broad, and requires unauthorized access to data on a computer that assumes that such data can be used to inflict harm to or ethical or defamation. Although there is no internationally agreed concept of cyber terrorism, it is difficult to conceive of defamation as a terrorist attack.[34] In order to improve the legislation on cyber terrorism, the Indian Government subsequently introduced a set of rules in 2011, which aim to strengthen loose links.[35]

After 2008 attack legislation also made changes in the rules and regulations to be followed by the internet cafes which was included in the definition of intermediary[36] due to their huge involvement in the planning and supervision of the attack by the terrorist group. The alteration of the clause on intermediary liability (Sec.79) though a step in the progressive direction, which aims to make only the specific violators of the law responsible for the crimes committed, is still not broad enough. The exclusion is expected to be broad in scope in order to promote creativity and to enable corporate and public content sharing programs, including through peer-to-peer technology.

First, the obligation to eliminate material upon acquisition of "real information" is far too heavy a responsibility on intermediaries. Such a condition allows the intermediary to take action instead of the proper authorities (which often is the judiciary). The intermediary is not in a capacity to determine whether or not the Gauguin painting of Tahitian women is indecent, because this involves judicial interpretation of the mind. Furthermore, this provision is vitiated by the values of natural justice and freedom of speech, as it enables the interaction and news media to be suffocated without giving it or the party having any due hearing into it. It has also been established by our courts that a limitation which does not give the persons concerned the right to be heard is procedurally unfair. [37]

The agent violates the security of the act if (a) the transmission is initiated; (b) the receiver of the transmission is chosen; and (c) the information is chosen or changed. Although the first two must be listed as real "intermediaries," the third criterion is a little too loosely worded. For example, an intermediary may instantly insert commercials into all transmissions, but the alteration doesn't go to the core of the transmission, or in any way makes it liable for the transmission. Likewise,

---

[33] Ibid

[34] <https://cis-india.org/internet-governance/publications/it-act/short-note-on-amendment-act-2008> (accessed on 4th April,2020)

[35] Halder, Debarati. (2011). Information Technology Act and Cyber Terrorism: A Critical Review. SSRN Electronic Journal. 10.2139/ssrn.1964261.

[36] Ibid

[37] *Virendra v. State of Punjab*, AIR 1957 SC 896.

the intermediary would have a code of ethics and can govern communications with respect to specific language (which is easy to judge), but may not be able to make decisions about the fair usage of copyrighted content. Therefore, this kind of "collection" does not make the intermediary accountable, because the infringement of copyright can well be contrary to the terms and conditions of use of the intermediary.[38]

In addition to these rules and regulations concerning cafes, they were also addressed in the streets introduced in 2011. The Act enables the government to recommend requirements for intermediaries, namely cyber cafes. If the cybercafé does not conform with the regulations, it would be responsible for any infringement by the consumer. According to the law, all cyber cafes must register with the registry agency authorized by the law. The laws allow cyber cafes to retain identification records, contact information and websites viewed for a minimum duration of one year. They monitored a Lashkar control room in Pakistan where the terror chiefs directed their men, hunkered down in the Taj and Oberoi hotels. The Indian government did not respond to several requests for official comment, but a former Indian intelligence official acknowledged that Indian spies had tracked Mr.Shah's laptop communications. It is unclear what data the Indians gleaned from their monitoring.

On request, cyber cafes are expected to reveal records to inspecting officers. The regulations also set down criteria for seating and laid-out. Cyber cafés shall feature a board that is clearly visible to users, prevent them from browsing pornography sites and from accessing information prohibited under the statute.[39] The Act describes cybercafé as a location where Access to the internet is provided to the consumer in the regular course of business. This means that companies such as restaurants, airports and coffee shops offering access to Wi-Fi facilities may be viewed as cyber cafes. Under this case, the regulations relating to seating, notice boards and the management of registers can be tedious for all institutions to comply with them.[40]

While the Information Technology Act, 2000 itself is an extensive piece of law, it has had some underlying limitations. But now the latest amendment act now in place, numerous threats and problems in the real cyber world will be resolved. The updated act is a positive move to address loopholes in the former act in India, such as the implementation of legal recognition of electronic signatures, data protection responsibilities and procedures, provisions to counter evolving cyber security threats such as cyber terrorism, identity theft, spam, video voyeurism, Internet pornography and other crimes. It laid the foundation for the removal of certain unacceptable wordings in certain parts of the IT Act.

This can be anticipated that the glaring discrepancy will also be supplemented with time when and when there may be more problems for the judiciary. Essentially, it cannot assume that this amendment is an end in itself, but it is a

[38] Ibid 15
[39] Rule 3 (1) and (5) <https://cis-india.org/internet-governance/resources/intermediary-guidelines-rules> accessed on 5th April,2020
[40] Rule 3 (7)

start, as the IT Act may need amendments when and when technology progresses more and more. Since it is obvious that the aspect of technology is rising both vertically and, thus, further changes may be made to make it completely evident.[41]

Sugesstion and Conclusion

By thorough analysis of Mumbai terrorist attacks of 26/11, it was observed that the attacks were form of Cyber terrorism as it was done to convey particular destructive message to the government, sending of threatening emails, defacing of government websites, hacking and cracking of crucial government systems. 'Protected systems' were compromised and civil amenities were disrupted. Digital information systems computer networks which not only affected governing system but also the population of a target area was affected to create a panic or situation of threat.

Computer and digital communication networks were main tools of extremists in this case. Also, Supreme Court judgement on Mumbai Attacks case, in para number 57 specifies about use of Google Earth, tampering with telecommunication networks and digital networking shows that the Attack was done by was done by Hi-Tech offenders. Although electronic eavesdropping often yields valuable data, even tantalizing clues can be missed if the technology is not closely monitored, the intelligence gleaned from it is not linked with other information, or analysis does not sift incriminating activity from the ocean of digital data as traced by Inteligence agencies of US, UK and India during investigation of attacks.

The report successfully establishes that cyber terrorism has been broadly used to conduct the attack, by identifying the usage of cyberspace and technology to get information about the target place and population, recruitment and motivation of the terrorist and also to find out the details about the guests in Hotel Taj and Oberoi.

Indian government websites are at stake risk. There are several reports on hacking and effacement of websites which includes 2010 case of defacement of government website by Pakistani hacker. It will not be the case data vandalising, which manages confidential correspondences but was sort of a warning that still are cyber security laws are inappropriate. During the first half of 2011, 117 Government websites had been the defaced which also includes some important websites of National Investigation Agencies (NIA). This is alarming for Indian intelligence agencies to take some appropriate steps in order to safeguard confidential information and to safeguard people. Such types of attacks actually fulfil the qualities of Cyber-attacks against government.

It has been a harsh reality that advancement in technology had been subsumed in society in very negative aspects. Understanding of cyberspace and cyber

[41]Asawat, Vikas, 'Information Technology (Amendment) Act, 2008: A New Vision through a New Change' <https://ssrn.com/abstract=1680152> accessed on 4th April,2020

criminals is very important, technical hardware and computer code should be provided to fight such crimes. In order to control crime within the virtual world facilities should be established in varied components. Indian agencies working after cyber security should also keep a close vigil on the developments in the IT sector of our potential adversaries. This includes continuous cyber education and learning which must be included in a legal arena. Technology field is very dynamic as it becomes obsolete during very short of time. Law cannot afford to be static; it must be modified in accordance with the dynamical times. Cyber-attacks in India post 2005 demands rigorous changes in the cyber laws of India.

References

Aneesh V Pillai, Admissibility Of Digital Evidences: An Overview Of The Legislative And Judicial Perspectives, 2016 (2) Elen. L R

Anikar M. Haseloff, Cybercafes and their Potential as Community Development Tools in India <http://ci-journal.net/index.php/ciej/article/view/226/181> accessed on 5th April,2020

Asawat, Vikas, Information Technology (Amendment) Act, 2008: A New Vision through a New Change, <https://ssrn.com/abstract=1680152> accessed on 4th April,2020

Carvell, A. (2008, 11 December), Indian lawyer has Google Earth in his sights, < http://www.geek.com/articles/news/indian-lawyer-has-google-earth-in-his-sights-20081211/> accessed on 3rd April,2020

Carvell, A. (2008, 11 December). Indian lawyer has Google Earth in his sights., <http://www.geek.com/articles/news/indian-lawyer-has-google-earth-in-his-sights-20081211/> accessed on 6th April,2020

Cereijo Cuba The threat II: Cyberterrorism and Cyberwar <http://www.lanuevacuba. com/archivo/manuel-cereijo-110.html> accessed on 12 February 2020

Chaudhary Shubham 'Cyber Terrorism: World Wide Weaponisation' 2019 3(2) International Journal of Law and Legal Jurisprudence and Studies 227

Cyber space played key role in 26/11 Mumbai attack: US commander <https://economictimes.indiatimes.com/news/politics-and-nation/cyber-space-played-key-role-in-26/11-mumbai-attack-us-commander/articleshow/13164308.cms> accessed on 30 January 2020

Denning, D. E. 'Terror's Web: How the Internet is transforming Terrorism' 2006 Handbook of Internet Crimes 194

Dhaval D. Desai and Parjanya Bhatt, "Securing India's Cities: Remembering 26/11, Learning its Lessons", ORF Special Report No. 92, July 2019, Observer Research Foundation. <https://www.orfonline.org/research/securing-indias-cities-remembering-2611-learning-its-lessons-53066/> accessed on 5th April,2020

Digital Evidence and Forensics, <https://nij.ojp.gov/digital-evidence-and-forensics> accessed on 3rd April,2020

Dogrul Murat 'Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism' 2011 International Conference on Cyber Conflict 29

Economic Times Report dated 26 November 2019 'Eleven Years since Mumbai Terrorist Attacks' <www.economictimes.indiatimes.com/> accessed on 10 April 2020

Elias Neocleous & Co LLC, Admissibility of digital evidence in court, <https://www.lexology.com/library/detail.aspx?g=29828d6d-8396-4070-9424-05ac2e0ecfae> accessed on 6th April,2020

F Cassim 'Addressing the spectre of cyber terrorism: a comparative perspective' 2012 15(2) PER 381

FBI hands over crucial evidence to Mumbai police. Retrieved , <http://www.dailytimes.com.pk/default.asp?page-2009%5C02%5C22%5Cstory_22-2-2009_pg7_8> accessed on 6th April,2020

Gulati, Rishi, The 26/11 Mumbai Terrorist Attacks: Assessing Pakistan's Responsibility in International Law (July 12, 2011). Indian Journal of International Law, vol. 51, no. 3 (2011), pp.321-363. <https://ssrn.com/abstract=2046864> accessed on 6th April,2020

Halder, Debarati. (2011). Information Technology Act and Cyber Terrorism: A Critical Review. SSRN Electronic Journal. 10.2139/ssrn.1964261, <https://cis-india.org/internet-governance/resources/intermediary-guidelines-rules> accessed on 5th April,2020

Handling of digital evidence, < https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html> accessed on 3rd April,2020

Harsh V. Pant and Maya Mirchandani, Eds., "26/11: A Decade After", ORF Special Report No. 77, December 2018, Observer Research Foundation., <https://www.orfonline.org/wp-content/uploads/2018/12/ORF_Special_Report_77.pdf> accessed on 5th April,2020

India Faces Serious Threads from Cyber Terrorism, says expert <https://www.firstpost.com/business/biztech/india-faces-serious-threat-from-cyber-terrorism-warns-expert-1869729.html> accessed on 21 January 2020

India sends 11th Mumbai attacks dossier to Pakistan, <http://www.dailytimes.com.pk/default.asp?page=2010%5C06%5C19%5Cstory_19-6-2010_pg1_3> accessed on 6th April,2020

Information Technology (Amendment) Act, 2008, <https://www.bcasonline.org/Referencer201516/Other%20Laws/information_technology_act_000.html> accessed on 7th April,2020 International Journal of Recent Technology and Engineering 159

Matiha Nehala and Awasthi Rajan 'A Critical Study on Cyber Terrorism with Reference with 26/11 Mumbai Attack' 2018 119(17) International Journal of Pure and Applied Mathematics 1617

Md. Ajmal Md. Amir Kasab @Abu vs State of Maharashtra, <https://indiankanoon.org/doc/193792759/> accessed on 4th April,2020

NDTV Correspondent (2010). Hacked by 'Pakistan cyber army', CBI website still not restored < http://www.ndtv.com/article/india/hacked-by-pakistan-cyber-army-cbi-website-still-not-restored-70568> accessed on 25 March 2020

Oh, O., Agrawal, M. & Rao, H.R. Information control and terrorism: Tracking the Mumbai terrorist attack through twitter. Inf Syst Front 13, 33–43 (2011). <https://doi.org/10.1007/s10796-010-9275-8> accessed on 5th April,2020

Pankaj Choudhary Upasna Singh, Ranking Terrorist Nodes of 26/11 Mumbai Attack using Analytical Hierarchy Process with Social Network Analysis <https://www.albany.edu/iasymposium/proceedings/2016/12_Choudhary_Singh_ASIA2016.pdf> accessed on 7th April,2020

Ponnusamy Suhannia ‘An International Study on the Risk of Cyber Terrorism’ 2019 7(5)

Prem Mahadevan, A Decade on from the 2008 Mumbai Attack: Reviewing the question of state-sponsorship, <https://icct.nl/publication/a-decade-on-from-the-2008-mumbai-attack-reviewing-the-question-of-state-sponsorship/> accessed on 8th April,2020

Raghavan, S. Digital forensic research: current state of the art. CSIT 1, 91–114 (2013), <https://doi.org/10.1007/s40012-012-0008-7> accessed on 8th April,2020

RATH, SAROJ KUMAR. "26/11 Mumbai Attacks: INDIA IS HAMSTRUNG." World Affairs: The Journal of International Issues14, no. 4 (2010): 36-71. Accessed April 17, 2020., <www.jstor.org/stable/48504857> accessed on 5th April,2020

Reich, Pauline C. "Case Study: India - Terrorism and Terrorist Use of the Internet/Technology." , Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization, ed. Pauline C. Reich and Eduardo Gelbstein, 377-408 (2012),

RITA MANCHANDA, Media-Mediated Public Discourse on 'Terrorism' and Suspect Communities, Economic and Political Weekly, Vol. 45, No. 15 (APRIL 10-16, 2010), pp. 43-50, <https://www.jstor.org/stable/25664331> accessed on 6th April,2020

Rules & Regulations Review, The Information Technology Rules, 2011, <https://www.prsindia.org/uploads/media/IT%20Rules/IT%20Rules%20and%20Regulations%20Brief%202011.pdf> accessed on 7th April,2020

Saxena, A. (August 4 2011). 117 ‘Indian Government Websites Defaced Till July. MEDIANAMA’ <http://www.medianama.com/2011/08/223-indian-government-websites-hacked/> accessed on 15 March 2020

Schjolberg, S. Terrorism in Cyberspace - Myth or reality? <http://www.cybercrimelaw.net/documents/Cyberterrorism.pdf> accessed on 15 January 2020

Shah, Nishant (2007) 'Subject to technology: internet pornography, cyber-terrorism and the Indian state ', Inter-Asia Cultural Studies, 8:3, 349 – 366, <http://dx.doi.org/10.1080/14649370701393725> accessed on 6th April,2020

Shashi Shukla, Emerging New Trends Of Terrorism : Challenges Before The United Nations, The Indian Journal of Political Science, Vol. 67, No. 1 (JAN. - MAR., 2006), pp. 165-176 <https://www.jstor.org/stable/41856202> accessed on 5th April,2020

Shukla Shashi ‘Emerging New Trends Of Terrorism : Challenges Before The United Nations’ 2006 67(1) The Indian Journal Of Political Science 165

Shweta, Tauseef Ahmad, Relevancy and Admissibility Of Digital Evidence: A Comparative Study International Journal of Law Management & Humanities Page , Volume 2, Issue 1 ISSN: 2581-5369

Soni Lavin Valecha, Sonika Bhardwaj, Admissibility of Electronic Evidence under the Indian Evidence Act, 1872, International Journal of Management and Humanities (IJMH) ISSN: 2394-0913, Volume-4 Issue-7, March 2020

Sriram Raghavan, Digital forensic research: current state of the art, < https://link.springer.com/article/10.1007/s40012-012-0008-7> accessed on 3rd April,2020

Tejas Karia, Akhil Anand and Bahaar Dhawan, The Supreme Court of India re-defines admissibility of electronic evidence in India, Digital Evidence and Electronic Signature Law Review, 12 (2015)

The Information Technology (Amendment) Act, 2008, <https://internetdemocracy.in/laws/the-information-technology-amendment-act-2008/> accessed on 7th April,2020

Vatis Michael 'The Next Battlefield: The Reality of Virtual Threats' 2006 28(3) Harvard International Review 56

Vivek Dubey, Admissibility of electronic evidence: an Indian perspective, Forensic Research & Criminology International Journal, Volume 4 Issue 2 – 2017