Content is available at: CRDEEP Journals
Journal homepage: http://www.crdeepjournal.org/category/journals/ijssah/

International Journal of Social Sciences Arts and Humanities
(ISSN: 2321-4147) (Scientific Journal Impact Factor: 6.002)
A Peer Reviewed UGC Approved Quarterly Journal

Research Paper

An Analysis of Some high-profile terrorist attacks in India during 2008 and what Legislative and Institutional Developments were taken by the Indian Government after the 26/11 Mumbai attack (A case of Cyberterrorism)

Aditya Kumar[1*] and Dr. Anand K. Singh[2]
[1]-Research Scholar, Dept. of Defence and Strategic Studies, Hindu College Moradabad U.P. India
[2]-Professor and Incharge, Dept. of Defence and Strategic Studies, Hindu College Moradabad U.P. India (Affiliated to MJP Rohilkhand University, Bareilly, India)

ARTICLE DETAILS

Corresponding Author:
Aditya Kumar

Key words:
Cyberattack, cyberterrorism, digital technologies, legal reforms, India

ABSTRACT

Before 2008, India did not experience any high-profile case of cyberterrorism, but there were several cyber-related threats and incidents that raised concerns about cybersecurity and the potential for cyberterrorism in the country. Though cyberterrorism was still in its nascent stages in 2008, CRPF Camp attack, Jaipur Blasts, Bangalore Blast, Ahmedabad Blasts, Delhi Serial Bomb Blasts, Mumbai attacks highlighted the potential for digital technologies to be leveraged in the service of terrorism. The main objective of this study is to understand and analyse the terrorist attack in India during 2008 and why 26/11 Mumbai attack is taken as a first case of cyberterrorism in India. To analyse the high-profile attacks in India data were collected through primary and secondary sources. The year 2008 was marked by six high-profile terrorist attacks in India, with the 26/11 Mumbai attacks being the most devastating and widely remembered. After Mumbai attacks, the Indian government, recognized the potential for a cyberterrorism attack on defence and energy infrastructure, started focusing on enhancing the protection of critical national assets.26/11 terrorist attack (Mumbai, 2008) was a major wake-up call for the Indian government to highlight the importance of cybersecurity and the need to address cyber threats (Cyberterrorism). The 2008 terrorist attacks, especially the 26/11 Mumbai attacks, were a watershed moment in India's fight against terrorism and its response to emerging threats like cyberterrorism. The Indian government undertook a series of legislative (Section 66F), institutional (CERT-In,), and security reforms to address the vulnerabilities exposed during the attacks. While significant progress has been made in the areas of counter-terrorism, cybersecurity, and national security, the evolving nature of global terrorism continues to present new challenges for India and the international community.

1. Introduction

After 9/11 in US, International organizations like the United Nations and developed countries were already developing frameworks to address cyberterrorism as a growing threat to national security. Though no direct cyberterrorism attacks occurred in India before 2008, there was a clear understanding that cyber tools could be used in combination with traditional forms of terrorism to cause significant disruption. The year 2008 was notable for the beginning of more serious recognition of the vulnerabilities of critical national infrastructure, government systems, and sensitive information in cyberspace. In 2008, Indian government websites were frequently targeted by hackers. Many of these attacks were carried out by groups or

*Author can be contacted at: *Research Scholar, Dept. of Defence and Strategic Studies, Hindu College Moradabad U.P. India*
Received: *25-01-2025*; Sent for Review on: *28-01- 2024*; Draft sent to Author for corrections: *05-02-2025*; Accepted on*: 19-02-2025*; Online Available from *28-02-2025*
DOI: *10.13140/RG.2.2.20979.44326*
IJSSAH: *-9909/*

individuals with ideological motives. Some hackers defaced government websites or gained access to sensitive data, though these actions were generally considered to be politically motivated rather than purely terrorist in nature. Although no direct cyberterrorism attacks were widely reported before 26/11 in 2008, there were growing concerns that neighboring terrorist groups could use the internet to disseminate propaganda, recruit operatives, or even organize attacks on India's critical infrastructure or spreading anti-national propaganda. Another area of concern in India during 2008 was the increasing cyberattacks on financial institutions. Cybercriminals were targeting banks, ATMs, and online financial systems for fraud. Although these were typically motivated by financial gain, the growing use of the internet for such purposes raised alarms that terrorist organizations might also use the same tactics to disrupt the financial infrastructure or steal information. The information technology is a double-edged sword, which can be used for destructive as well as constructive work. The 26/11 attacks led to more discussions on the Potential use of social media and communication networks to spread terror among people. Agrawal, and Rao (2011) and LaRaia and Walker (2009) had corroborated the usage of cyber technology to extremist use to present the scenario of cyberterrorism which engulfed India as well as the whole world. Both Oh et al. (2011) and La Raia and Walker (2009) have also elaborated how satellite phones, GPS and various websites were widely used for fulfilling the mission of the extremists. On the contrary, the term cyber terrorism has been broadly used by the media especially to identify the usage of cyber space and /or cyber technology to aid the terrorist activities, gain information about the target place and population, recruit operatives, motivation and disseminate propaganda.etc. In the year 2008, 2565 security incidents were reported by CERT-in, in which phishing (23.54%), network scanning (10.33%), Virus/malicious code (15.9%), spam (11.89%), denial of service (2.10%) and others (3.66%). Maximum cases (32.55%) were from websites compromise and malware attacks (Fig.1).

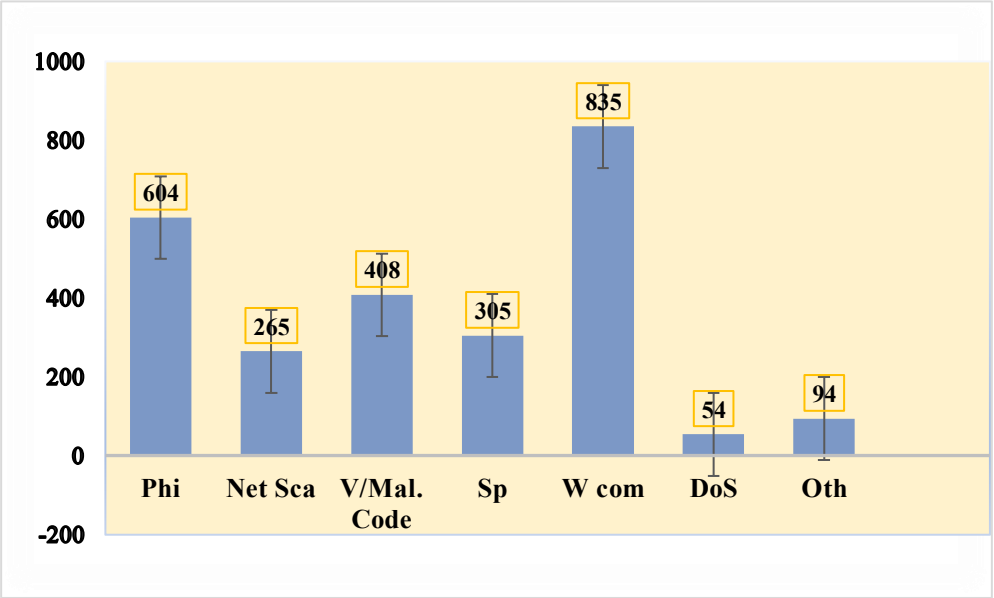

Fig.1. Security incident statistics in India in 2008 (*Source:* CERT-in)
(Phi=phishing, Net Sca=network scanning, V/Mal code=Virus/malicious code, Sp=spam, W com=websites compromise/malware attacks, DoS=denial of service, Oth= others.)

The main objective of this study is to understand and analyse the terrorist attack in India during 2008 and why 26/11 Mumbai attack is taken as a first case of cyberterrorism in India.

2. .Methodology

The following methodology outlines the approach taken to analyse the high-profile terrorist attacks in India in 2008, particularly focusing on the 26/11 Mumbai attacks, and the subsequent legislative and institutional developments undertaken by the Indian government.

2.1 Primary Sources: Government annual reports, official documents, and public statements from the National Investigation Agency (NIA), Police reports and investigation findings related to each of the attacks. Media coverage from Indian and international news.

2.2 Secondary Sources: Academic journals, various articles published in websites and books focused on terrorism studies, national security, and cyberterrorism.

2.3 Case Study Approach: The study uses a case study approach to analyse each high-profile attack in 2008, with particular emphasis on CRPF camp attack in Rampur, Jaipur Blasts, Bangalore Blast, Ahmadabad Blasts, Delhi Serial Bomb Blasts, Mumbai attacks. The 26/11 (Mumbai attacks) are treated as the central focus due to their scale, impact, and subsequent legislative and institutional responses.

2.4 Cyberterrorism Analysis: A special emphasis is placed on the role of cyberterrorism in the Mumbai attacks, where attackers used mobile phones, the internet, and encrypted communications for coordination. This section explores the use of cyber tools by terrorist organizations like Lashkar-e-Taiba/ Indian Mujahideen to carry out and communicate during the attack. Post-attack developments in cybersecurity legislation such as Section 66F of the IT Act 2008, which criminalized cyberterrorism.

3. Results

3.1 Some noteworthy terrorist attacks in India during 2008

In 2008, India faced a series of high-profile terrorist attacks that involved both physical violence and digital aspects, raising concerns about the potential for cyberterrorism. Table-1 and Fig.2 are showing detailed description of terrorist attacks and their possible relation to digital or cyber elements and casualties in terrorist attacks in 2008 in India.

Table-1. Noteworthy terrorist attacks in India during 2008 and their cyber dimension

Date	incidents	Perpetrators	Category	Cyber Dimension
01/01/2008	Terror attack on CRPF camp in Rampur, U. P.	Lashkar-e-Taiba	Act of terror	No information about the use of mobile phones or internet
13/05/2008	9 bomb blasts along 6 areas in Jaipur	Indian Mujahideen (Accountable), Harkat-ul-Jihad-al-Islami (suspected)	Act of terror	use of mobile phones for communication & sent warning emails for bomb blasts
25/07/2008	8 low intensity bomb blasts in Bangalore	Lashkar-e-Toiba, SIMI	Act of terror	use of internet for planning, coordination, and execution, no direct evidence of hacking or cyberattacks
26/07/2008	17 serial bomb blasts in Ahmadabad	Indian Mujahideen, Harkat-ul-Jihad-al-Islami	Act of terror	internet communication to coordinate the blasts ,email to send out bomb warnings to the media
13/09/2008	5 bomb blasts in Delhi markets	Indian Mujahideen	Act of terror	no direct evidence linking the blasts to cyberattacks, use of mobile phones for communication
26/11/2008	12 shooting and bombing attacks lasting four days in Mumbai	Lashkar-e-Taiba	classified as cyberterrorism	use of mobile phones, satellite phones & the internet (VOIP), evidence of hacking and attack against the digital Infrastructure& physical violence

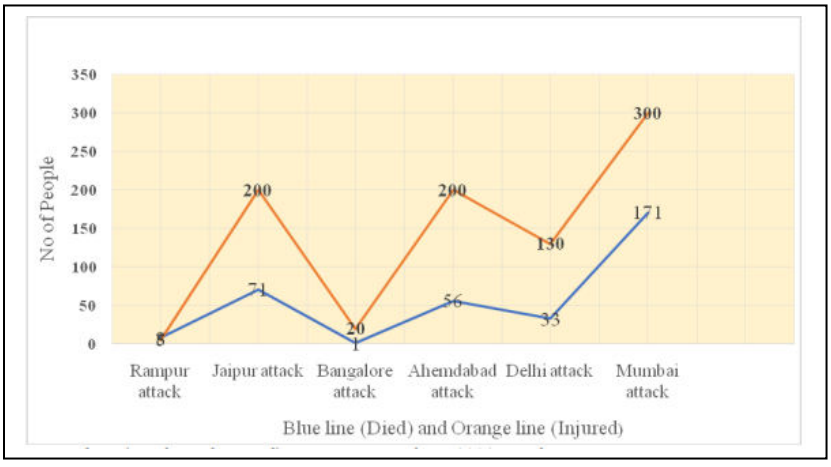

Fig.2 .Showing casualties (Deaths and injured) in terrorist attacks in 2008 in India

3.2 Mumbai Attacks (26-29 November, 2008): The 26/11 Mumbai attacks were one of the most horrific and high-profile terrorist events in India. On November 26, 2008, ten gunmen, associated with the Pakistani-based militant group Lashkar-e-

Taiba, launched a series of attacks across Mumbai, including on the Taj Mahal Palace Hotel, Leopold Café, and Chhatrapati Shivaji Maharaj Terminus. The attacks lasted for more than 60 hours, leading to over 171 deaths and hundreds (300) of injuries (Fig.3). The Mumbai attacks showed an unprecedented combination of detailed planning and organization, multiplicity of targets andindiscriminate killing on a large scale in a major city.

Fig.3. Mumbai attacks (a case of cyberterrorism)

3.3 Cyber Dimension: Though the attacks were physically violent, the role of technology was significant. The terrorists used satellite phones and the internet (VOIP) to communicate with their handlers (Lashkar-e-Taiba) in Pakistan during the attacks. They tracked the movements of Indian forces using social media, and Google Earth. The gunmen were reportedly in contact with their commanders via Skype and other internet-based tools, allowing them to receive real-time instructions during the siege. Cyberterrorism was not the main feature of the attacks, but the reliance on cyber communication for coordination raised alarms about the vulnerability of communication networks. It showed that terrorists could use the internet to coordinate complex operations.

3.4 Impact: The 26/11 attacks marked a major shift in how terror organizations could leverage cyberspace for operational purposes. This led to greater awareness about cyber capabilities being used for physical violence and terrorism. Indian security agencies started paying more attention to the digital infrastructure and the possibility of cyberterrorism being part of a broader strategy by terrorist groups, either to launch attacks or disrupt operations. These concerns led to an increased focus on cybersecurity.

3.5 Status: A case was registered under IPC, Unlawful Activities (Prevention) Act and the Explosive Substances Act. Mumbai Police was the first to register a case of *Cyberterrorism* under section 66F of IT Act. Out of ten terrorists, 9 were killed throughout the attacks and the only terrorist who was caught alive, was executed in 2012. While cyberterrorism was not a direct feature of these 2008 attacks, except Mumbai attacks, the growing role of technology in planning and executing terrorist acts was increasingly evident- mobile phones and satellite phones were often used for direct coordination between terrorist groups and their handlers. Terrorist groups were increasingly using emails for threatening warnings and other communication. This digital footprint became a significant tool for intelligence agencies to track and trace terrorists. Online tools like Skype, encrypted messaging services, and even social media were increasingly being used by terrorists for secure communication, making it harder to intercept messages.

4. Legislative and institutional developments in India

In 2008, India took significant steps to bolster its legal and institutional frameworks to address the rising threats of cybercrimes and cyberterrorism--

Information Technology Act (Amendments in 2008): The Information Technology Act, 2000 (IT Act), which had initially focused on e-commerce and digital transactions, was amended in 2008 to address growing concerns related to cybercrimes and cyberterrorism. Some important provisions introduced included:

Section 66F: This section specifically addressed cyberterrorism, making it a punishable offense under the law. The section criminalized attacks on critical infrastructure, hacking into government systems, or using cyberspace to cause harm to the

sovereignty and integrity of India. Example-The Mumbai police have registered a case of cyber terrorism, under Section 66F of amendment IT Act in 2008 for the first time in India.

Section 69A of the IT Act conjointly empowers the Central government or any of its authorized 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.

Section 70(3) sanctions punishment up to 10 years with fine in case a person secures or attempts to secure access to a protected system.

Section 70A of the Act, the central government, has designated National Critical Information Infrastructure Protection Centre (NCIIPC) as the National Nodal Agency in respect of CII protection.

Section 70B of the Act, provides for the constitution of CERT-In, which had gained prominence in responding to cyber incidents, providing a focal point for coordinating responses to cybercrimes, hacking, and potential threats related to cyberterrorism. CERT-In's role became more critical as India began to realize the strategic importance of cybersecurity.

National Cyber Security Policy (NCP): Although the National Cyber Security Policy came later in 2013, the 2008 amendments to the IT Act were one of the key precursors to India's long-term cybersecurity strategy. As part of efforts to improve cybersecurity, India started focusing on enhancing its cyber defense capabilities and training specialized cybersecurity professionals.

NIA The Parliament also amended the National Investigation Agency (NIA) Act in 2019, empowering the NIA to investigate and prosecute acts of cyberterrorism.

DCA Under the Ministry of defence, Defense Cyber Agency (DCA)has also established to deal with matters of cyberwarfare and cybersecurity.

NCCC The Government of India took a major leap with the establishment of the National Cyber Coordination Centre (NCCC). It deals with cyber threats and cyber-terrorism. All CERTs and ISACs would subsequently be linked with NCCC to provide a speedy and seamless flow of cyber threat information across the board for all stakeholders.

IC4 The Indian Cyber Crime Coordination Centre (IC4) is also launched under the Ministry of Home Affairs (MHA) to combat cybercrime and cyberterrorism. Adequate protections are implemented in the form of Cyber Audits, Physical Checks, and Policy Guidelines to guarantee the Armed Forces of the nation are strong in cyberspace. Mock drills and exercises in cyber security are conducted regularly. To reduce the susceptibility of internet traffic to cyber-attacks, efforts are taken to guarantee that traffic originating and ending within India is routed within India's geographical borders. The mechanisms will be developed in collaboration with the relevant government ministries, Internet Service Providers (ISPs), and NIXI.

Botnet Cleaning and Malware Analysis Centre: Cyber Swachhta Kendrahas been established to identify dangerous programs and provide free tools to remove them. Moreover, technology and threat Intelligence play major roles to counter terrorism and cyberterrorism. The multi-agency centre (MAC) atthe national level, set up after the Kargil intrusion, along with subsidiary MACs (SMACs) at state levels, have been strengthened and reorganized to enable them to function on 24×7 basis. Around 28 agencies are part of the MAC and every organisation involved in counter-terrorism is a member of this mechanism. This is yet another important element of national initiative.

International Cooperation: Following the 26/11 attacks, India intensified its cooperation with countries like the United States, United Kingdom, and Pakistan in combating terrorism.

5. Conclusion

Cyber terrorism presents a particularly unique dilemma for the Indian government and military as these attackers often work outside of their respective governments, and act separately as a result. In other words, it can be more difficult to determine the origins of cyber terrorism attacks. Terrorist groups can act with greater anonymity when they are not working in coordination with a state government, yet they can also be funded and organized to do a specific country's bidding. Regardless of why they attack, these groups present a legitimate threat to Indian cyber security interests. The 26/11 attacks marked a major shift in how terror organizations could leverage cyberspace for operational purposes. This event caused many government agencies to review their security practices and procedures. It also has raised awareness of other avenues that terrorists might pursue to achieve their goals, including cyber terrorism.

References:

1. Agrawal, O. M., & Rao, H. R. (2011) Information control and terrorism: Tracking the Mumbai terrorist attack through twitter. Information Systems Frontiers, Special Issue on Terrorism Informatics, 13(1): 33-43.
2. Bhandarwar, A.H., Bakhshi, G.D., Tayade, M.B., Borisa, A.D., Thadeshwar, N.R. & Gandhi, S.S. (2012). Surgical response to the 2008 Mumbai terror attack, British Journal of Surgery, 99(3): 368–372.
3. Bruce, Riedel (2008). Mumbai Terrorist Attacks: A Challenge for India and the World. The Brookings Institute.
4. CERT-in Annual Report,2008, http//www.cert-in.org.in,15may2009
5. Chuipka, A. (2017). The Strategies of Cyberterrorism: Is Cyberterrorism an effective means to Achieving the Goals of Terrorists? https://ruor.uottawa.ca/bitstream/ 10393/35695/1
6. Cyber terrorism and the reality of threat, www.aspistrategist.org.au
7. Cyber terrorism: The Fifth Domain, www.indiabloom.com
8. Cyberterrorism How Real Is the Threat? https://www.usip.org
9. Duggal, P. (May 30, 2011). Cyberterrorism Some legal perspectives. http://neurope.eu/cybersecurity2011/?p=47
10. Ghosh, S. (2009). Mumbai Terror Attacks: An Analysis. Institute of Peace and Conflict Studies,1-9, www.jstor.com/stable/resrep09336
11. Govt Approves Setting up of Defence Cyber Agency, The Times of India, 17 Nov. 2019,http://timesofindia.indiatimes.com/articleshow/72264836.cms?
12. Heickerö, R. (2014). Cyber Terrorism: Electronic Jihad. Strateg. Anal.,38 (4):554–565.
13. Information Technology Act, 2000 (Act 21 of 2000), Chapter III, Section 66F
14. LaRaia, W., & Walker, M. C. (2009). The Siege in Mumbai: A Conventional Terrorist Attack Aided by Modern Technology. In M. R. Haberfeld., & A.V. Hassell. (Eds.), A New Understanding of Terrorism (pp.309-340). New York: Springer.
15. Ministry of Communication and Information Technology, 'National Cyber Security Policy2013'p.5, pdf.
16. Mumbai Terrorist Attacks: A Challenge for India and the World," The Brookings Institute, December 03, 2008.
17. Nagpal, R. (2002). Cyber Terrorism in The Context of Globalization, in II World Congress on Informatics andLaw,1–23.
18. Nagpal, Rohus (2008). Introduction to Indian Cyber Law. Asian School of Cyber Laws, Pune, India
19. Naughton, J. (2016). The evolution of internet from military experiment to general purpose technology. J of Cyber Policy, doi.org/ m10.1080/23738871.2016.1157619
20. Oh, O., Agrawal, M., & Rao, H. R. (2011) Information control and terrorism: Tracking the Mumbai terrorist attack. Information Systems Frontiers, "Special Issue on Terrorism Informatics", 13(1):33-43.
21. Sauter, M. (2015). Terrorism in Cyberspace: The Next Generation. Journal of Communication. https://doi.org/10.1111/jcom.12193
22. Saxena, A. (August 4 2011). 117 Indian Government Websites Defaced till July. MEDIANAMA.http://www.medianama.com/2011/08/223-indiangovernment-websites-hacked/
23. Sonawane, D.V., Garg, B.K., Chandanwale, A., Mathesul, AA., Shinde, O.R. & Singh, S. (2020)., 26/11 Mumbai terrorist attack revisited: Lessons learnt and novel disaster model for future. Journal of Disaster Risk Studies,12(1): 915-919.
24. Stohl, M. (2006). Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriotgames? Crime, law Soc. Chang.,46(4):223–238.
25. Weimann, G. (2004). Cyberterrorism – how real is the threat. United States Institute of Peace, Special report. www.usip.org/sites/default/files/sr119.pdf