EVOLVING PATTERNS OF TERRORISM IN INDIA: A MULTI-DIMENSIONAL THREAT

Dr. Subhi Subhani, Department of Law, University of Jammu

ABSTRACT

Terrorism is a menace to peace and order in society, which finds its genesis in the regional, ethnic, and linguistic conflicts. It is that gruesome act against humanity that any ideology, reason, or grievance cannot justify. The paradigm shift of the traditional methods of terrorism to the emergence of evolving threats such as cyber terrorism, online radicalisation, lone wolf attacks, 3D technology, Deepfakes technology, and drone warfare, etc, is a concern which needs to be addressed. However, the balance between civil liberties and national interests should be maintained so that neither is compromised for the sake of the other.

Keywords: Terrorism, cyberterrorism, lone wolf attacks, Civil liberties, and National Interests.

Introduction

Terrorism is a persistent threat to world peace and security. It is not only a war against the state and its political institutions but against humanity. Terrorism is a recognised global threat from the regional, ethnic, and linguistic conflicts worldwide. It aims to destabilise the political structure and institutions vis-à-vis the subversion of the state. It is the most inhumane act against humanity and cannot be rationalised by any ideology, grievance, or reason.

The term terrorism was first used to describe the *Reign of Terror*, a period of the French Revolution where the citizens identified or suspected of being the enemies of the Revolution were subjected to the harshest measures. Initially, the term was used as a means by the state to enforce political control; however, with time, the term became synonymous with non-state actors or groups that use violent and terrorist activities such as killings, bombings, and assassinations against innocent individuals and non-combatants to instil their fear and presence. The term "*Terrorism*" does not have a universal definition. However, the United Nations defined it in its Resolution[1] on *Measures to Eliminate International Terrorism, 1994,* as an act that intends to provoke fear in a public or group of persons for political motives. It further stated that such acts are unjustified, whatever may be the reasons invoked to justify them. The Oxford English Dictionary defines "terrorism" as a violent action that aims to achieve political aims and compel the government to act or abstain from doing an act.[2]

The world has witnessed gruesome terror attacks in the past, where many innocents have been killed and injured. The *Global Terrorism Index* (GTI), produced by the Institute for Economics and Peace (IEP), states that in 2023, there was a 22% rise in deaths from terrorism worldwide compared to 2017, although these numbers are still lower than those in 2015.[3] For instance, almost 2000 people died in terrorist attacks in Burkina Faso from a total of 258 incidents. According to the GTI 2025, there has been a shifting pattern of terrorist activities beyond geographical borders. The Report states that ISIS and its affiliates remain the deadliest terrorist organisation in the year 2024, responsible for the deaths of 1805 people across 22 countries.[4] Antisemitic and Islamophobic hate crimes were on the rise, especially after the Israel-Palestine war, with the Federal Bureau of Investigation (FBI) recording incidents rising by 270 per cent

[1] United Nations, *Resolution on Measures to Eliminate International Terrorism*, GA/Res/49/60 (Dec 9, 1994)
[2] Catherine Soanes, *Oxford English Dictionary* 575 (Oxford University Press, 9th edn., 2025)
[3] Institute for Economics and Peace, "Report on Global Terrorism Index," (June 2024).
[4] *Ibid.*

in just two months. The Sahel, one of Africa's most vulnerable regions, has suffered hugely from terrorism and related activities. The extremists and the armed groups have an operational footprint in areas like Niger and Burkina Faso.[5] Weak political structures, corruption, lack of means and equipment, poverty, unemployment, poor civil-military relations, etc, contribute to the growth of terrorism and extremism in the region of Sahel. Syria, after the Sahel, is again the worst hit by terrorism. As per the *Report of the Syrian Network for Human Rights* (SNHR), in 2024, a total of 230,000 civilians have been killed by ISIS since 2011.[6] Like these, many countries are severely hit by terrorism and extremism around the world.

Within the context of India, the country has witnessed some deadly terror attacks in the past, where people have been killed and many injured. It continues to fight insurgency, terrorism, and secessionist activities in the Union territory of Jammu and Kashmir bordering Pakistan, the states of Jharkhand and Chhattisgarh (also called the Red Corridor), and the northeastern states bordering Myanmar, Nepal, and China. As per the Report of the *South Asian Terrorism Portal* for the year 2025, there have been 24395 deaths in India since the year 2000 due to terrorism and insurgency.[7] The influx of foreign terrorists and the money for the execution of terrorist activities in India is through porous borders, arms and weapons smuggling, and drug trafficking.

Naxalism is the most significant internal security challenge that India faces.[8] The principles of Mao Zedong influence this movement. The people involved in it are called Naxalites, and the region that they dominate in India is called "*The Red Corridor.*"[9] Initially, they waged an armed struggle against corrupt bureaucrats, capitalists, and landlords. However, their cause has changed over time and now involves violence, killings, and subversion of the established order of the state. According to the Report by the Ministry of Home Affairs, there were 17,679 Left Wing Extremist incidents in states like Chhattisgarh and Jharkhand from 2004 to 2014, resulting in 6,984 casualties.[10] From 2014 to 2023, there have been 7649 LWE incidents and

[5] Stephen Buchanan and Sibusiso Nkomo, "Violent Extremism in Africa, Citizens perspectives from the Sahel epicentre and periphery,"74 *AFR Barometer,* (2021).
[6] Anna Fleck, The Syrian Civil War, *available at*: https://www.statista.com/chart/33663/documented-civilian-deaths-in-syrian-war-since-2011/ (Last visited on April 20, 2025).
[7] South Asia Terrorism Portal, Datasheet India, *available at:* https://www.satp.org/datasheet-terrorist-attack/fatalities/india (Last visited on May 10, 2025).
[8] Neeraj Adhikari, " The Naxalites and the Maoist Movement in India: Birth, Demise, and Reincarnation," 3 *Information Technology*" (2007).
[9] Jayadev Dash, "Human Rights Violation in Red Corridor of India" 8(10) *IJCRT*, 3601- 3607 (2020).
[10] Press Information, Bureau, Ministry of Home Affairs, Naxalites Incidents 2023, *available at: https://www.pib.gov.in/PressReleasePage.aspx?PRID=1942471#:~:text=During%20the%20period%20from%2*

2020 fatalities.[11] This data illustrates the impact of terrorism on society and the nation as a whole. However, there is a decline in the activities of Naxalites and Maoists, as according to the South East Asian Terrorism Portal (SATP) Report 2024, Special Forces have arrested 401 Naxalites as against 395 in the year 2022.[12] As per the SATP, since March 2000, a total of 16,780 Naxalites have surrendered.

India's leadership is committed to eliminating terrorism from its soil. It has a zero-tolerance policy against any movement that aims to subvert the state and endangers its sovereignty and integrity. India, including its military system, has always given a befitting response to acts that compromise its sovereignty and integrity; for instance, the latest was "*Operation Sindhoor*" in response to the brutal terrorist attack on the tourists visiting Pahalgam in the union territory of Jammu and Kashmir on the 22nd of April 2025. The Indian military forces conducted this operation against the terrorists in the neighbouring country. This response testifies that India will not succumb to terrorism at any cost and will fight tooth and nail. The present leadership has unequivocally stated that terrorism and talks cannot go hand in hand with Pakistan or any state that harbours terrorism on its soil.

India's struggle for independence was taken seriously by the world after the 9/11 terrorist attack on the Twin Towers in the United States of America.[13] The United Nations, soon after this brutal attack, brought Resolution No. 1373, where the nation-states were urged to enact laws in their statute books to control and combat terrorism worldwide. Apart from these attacks, the world has seen many deadly attacks like the United Kingdom Liverpool bombings in 2021, the 2010 Iraq bombings, the ISI attacks in Syria, the 2015 Paris attacks, the 2016 Brussels attacks, the terrorist attacks in India, and worldwide. Such attacks reflect that the objective is to create terror in the minds of people, compel the respective states to do or abstain from doing anything, and subvert the established political structure of the states.

Literature Review

The researcher has studied various statutes, reports, books, journals, and newspapers relevant

02004%20to%202014%20there,incidents%20and%202%2C020%20deaths.%20Year-wise%20details%20are%20annexed (Last visited on April 25, 2025).

[11] *Ibid.*

[12] Institute of Conflict Management, *South Asian Terrorism Portal*, *available at*: https://satp.org/terrorism-assessment/india-jammukashmir-jammukashmir (Last visited on April 20, 2025).

[13] P.M. Kamath, "Terrorism in India: Impact on National Security" Vol 25(9) *Strategic Analysis,* 1081- 1087 (2008)

to the research. The researcher found that extensive scholarly work on terrorism and its evolving nature is conducted through sociological, strategic, and political perspectives. However, there is a lack of research in the area of contemporary threats like digital radicalisation, Lone wolf attacks, Artificial Intelligence, and drone warfare in India.

Evolution of Terrorism and Its Dimensions in India

Terrorism strikes at the rule of law, democracy, and human rights. Its objective is to shake the foundations of the state and jeopardise its peace and stability. It is not a recent phenomenon in India, but it has its historical roots in the partition of India into two states, namely India and Pakistan. The violence and bloodshed of the partition have left a scar between the people and communities. The early secessionist calls from the Indian Union, especially from the southern part of India, on a linguistic basis, soon after partition, laid the foundation of terrorism and secessionism in India.[14] In response to these secessionist calls, the Parliament of India enacted the Constitution (Sixteenth Amendment) Act, 1963, into the statute books. The amendment brought certain changes, and the most important was the insertion of the words "sovereignty and integrity" of India after the words "in the interests of" under Article 19(2) of the Constitution of India. Thus, this insertion meant that the right to free speech and expression, as given under Article 19(1)(a) of the Constitution of India to citizens of India, would be restricted on the grounds of the sovereignty and integrity of India. India, that is, Bharat, is a Union of States, which means no state has the freedom to secede from the Indian Union.[15] However, the Parliament of India can form a state out of a state, unite two states, or merge any territory with a part of a state.[16] It can further alter the areas, boundaries, or names of the state.[17] Thus, one can say that India is an indestructible Union of destructible states.[18]

Within the context of India, terrorism has posed a significant security challenge since independence. Besides, many terrorist attacks, the Indian Parliament Attack of 2001, the Mumbai Terror attacks in 2008, the Uri attack in 2016, the Pulwama attack in 2019, and the recent attack on the tourists in Pahalgam in 2025, were major blows to the security and sovereignty of India. As the legislative enactments are concerned, the Parliament of India have

[14] Dr Anand Kumar& Aditya Kumar, "A Study of Terrorism and its impact in India," 10(2) *IJRAR*, 983-986 (2023).
[15] Prof. Narender Kumar, *Constitutional Law of India*, 36 (Allahabad Law Agency, 7th edn., 2008).
[16] The Constitution of India, 1950 art.3(a).
[17] *Id..,* art. 3(b) to (e).
[18] Prof. Narender Kumar, *Constitutional Law of India*, 36 (Allahabad Law Agency, 7th edn., 2008).

enacted various laws, such as the Preventive Detention Act,[19] 1950; the Unlawful Activities (Prevention) Act,[20] 1967; the Maintenance of Internal Security Act,[21] 1971; the Terrorist and Disruptive Activities (Prevention) Act,[22] 1987; the Prevention of Terrorism Act,[23] 2002, and the National Security Act,[24] 1980, to control and combat terrorism in India. Some of these laws have been repealed owing to their excessive use against individuals and encroaching upon the people's civil liberties. The laws still on the statute books are the Unlawful Activities (Prevention) Act[25] of 1967 and the National Security Act[26] of 1980. These laws have been effective in combating the problem of terrorism in India. The stringent measures in these Acts deter individuals from taking up arms, thus protecting the sovereignty and security of India. The concerns remain that there should be a balanced approach between upholding the civil liberties of individuals and the national interests, as both are important to the state.

The emergence of terrorism in the Union territory of Jammu and Kashmir in the early 1980s, backed by Pakistan's state-sponsored terrorism, has stretched for more than five decades and has witnessed the loss of lives in thousands and hundreds. Along with it, the rise of terrorism in Punjab in the late 90s and the emergence of Naxalism and Maoist insurgency in the states of Chhattisgarh and Bihar have contributed to the growth of terrorism in India.[27] The presence of sleeper cells, overground workers, local support, indoctrination, and the use of the internet for digital radicalisation and cyber-attacks has made the issue more complex.

Shift from traditional to Contemporary methods

Over the years, terrorism has evolved from employing traditional methods to utilising more sophisticated techniques. There is a shift from organised crime to Hybrid warfare, which developing countries face in today's highly competitive world. Killings and bombings targeting individuals and sites of economic and geopolitical significance do persist, but are

[19] The Preventive Detention Act, 1950 (Act 4 of 1950).
[20] The Unlawful Activities (Prevention) Act, 1967 (Act 37 of 1967).
[21] The Maintenance of Internal Security Act, 1971 (Act 026 of 1971).
[22] The Terrorist Disruptive Activities (Prevention) Act, 1987 (Act 28 of 1987)
[23] The Prevention of Terrorism Act, 2002 (Act 15 of 2002)
[24] The National Security Act, 1980 (Act 65 of 1980)
[25] *Supra* note 21.
[26] *Supra* note 25.
[27] Nilambar Saraka, "History of terrorism in India: An Analysis," 2(2) *International Journal of Applied Research,* 157-161(2016).

now exacerbated by the utilisation of Weapons of Mass Destruction, chemical and biological agents, cyber warfare, drone warfare, and drug trafficking.

Hybrid warfare: A threat that exploits the fault lines between the state and its people, thus creating a dilemma of who, what, and how he is attacking.[28] It integrates contemporary methods, such as technological advancements in equipment, artificial intelligence, and digital environments, with cyber warfare, alongside traditional methods like organized crime and attacks on military establishments.[29] The strategy of using fake currency, the inclusion of counterfeit goods in the market, and adverse propaganda in the international market are the new means employed by the terrorists to weaken the economy of the targeted country. The smuggling and circulation of Fake Indian currency notes has been made a terrorist act under the Unlawful Activities(Prevention) Act of 1967.[30] The 2008 National Investigating Agency Act[31] established the National Investigating Agency (hereinafter as NIA) in 2008. It established a *Terror Funding and Fake Currency Cell* (TFFC) to address the issue of counterfeit currency circulation in the country. A total of 92,17,80,480 fake currencies were confiscated in India in the year 2020.[32] The Ministry of Home Affairs has also constituted the *Fake Currency Notes Coordination Group* (FCORD) to share intelligence information between security agencies and control the problem of fake currency notes in India.[33]

Cyberterrorism: The emergence of digital platforms and technology has altered the landscape of terrorism in India and worldwide. Cyberterrorism was the term coined for the first time by Barry Collin in 1980 as an abuse of digital technology, or a network used to support or facilitate a terrorist objective or campaign.[34] The unlawful attacks against computers and networks or secured cyberspace to coerce the government to do or not to do an act. Cyber terrorists use the internet in contemporary times for psychological warfare, in which they target vulnerable

[28] Brig. Narender Kumar (Retd), "Hybrid Warfare Division, An Urgent Operational Requirement for India" 8 *USI*, 74-82 (2020).
[29] Manish Raj Singh, "India and the Hybrid Threat: The Changing Dimensions of the Conflict," 9 *International Journal of Scientific and Innovative Research Studies*, 27-32, (2021).
[30] The Unlawful Activities (Prevention) Act, 1967, (Act 37 of 1967) s.40.
[31] The National Investigating Agency Act, 2008 (Act 34 of 2008).
[32] IANS, "Fake Currency worth Rs 137 cr seized in 3 years, most are Rs 2000 notes," *The Indiatimes*, (Dec 19, 2002).
[33] Ministry of Home Affairs, Steps taken to stop terror funding, *available at https://www.pib.gov.in/PressReleasePage.aspx?PRID=1578107* (Last visited on April 21, 2025).
[34] Aditya Kumar & Dr Anand K. Singh, " Cyberterrorism in India: A Novel Facet in the Warfare Domain," 10(12) *JETIR* (2023).

people for recruitment into their groups, spread propaganda, and justify their violent acts.[35] They also engage in interactive content with their target audience, sharing their narrative to influence, radicalize, and present a humanizing picture alongside violent crimes. These measures taken by terrorists do have an influence on vulnerable people, which contributes to the growth of terrorism. For instance, the ISIS group used encrypted apps such as WhatsApp and Telegram to coordinate attacks on Paris in 2015 and Brussels Bombings in the year 2016.[36] A Sukhoi Su-30 crashed in May 2017 on the India-China border, and later the Indian Air Force revealed that a cyber attack caused the crash while the plane was airborne.[37] 'Bharat Biotech' and 'Serum Institute of India' information systems were hacked by the Stone Panda(a Chinese-based organisation).[38]

The Maharashtra Cyber Cell, in its Report titled "Echoes of Pahalgam," has stated that there is a sharp rise in cyber attacks focusing on India, with nearly 10 lakh attempted breaches so far since the Pahalgam attack on the 22nd of April 2025 in the Union Territory of Jammu and Kashmir.[39] The departments such as defence, education, banking, and communication are the most vulnerable. According to the Report, these attackers target vulnerable resources on websites, such as software, plugins, and misconfigured settings, to gain access. Once they get access, they can misuse the website by uploading inappropriate content or defacing it. These attackers send numerous requests to a system, thereby congesting and rendering it non-functional.[40] Ransomware attacks encrypt a person's data and do not release it unless a ransom is paid. These attacks have led to substantial financial losses. For instance, in 2023, cyber attackers attacked the servers of AIIMS Delhi, disrupting health services. The sensitive data of the patients was compromised, and it shook the healthcare industry of India.[41] The billing data of 26 lakh customers of Uttar Haryana Bijli Vitran Nigam (UHBVN) was compromised in a ransomware attack, and the attackers demanded Rs 1 crore in cryptocurrency.[42] The *Computer*

[35] Chinasa Susan,(*et al*), "The Evolution of Terrorism in the Digital Age: Investigating the adaptation of terrorist groups to Cyber technologies for recruitment, propaganda and cyber-attacks, 24(3) *Asian Journal of Economics, Business and Accounting*, 298-306 (2024).
[36] *Ibid*.
[37] *Supra* note 34.
[38] Reuters, "Chinese hackers target Indian vaccine makers SII, Bharat Biotech, says security firm," *The Economic Times,* (2021).
[39] Faizan Khan, "Hackers strike hard: Over one million cyber attacks on India since Pahalgam terror attack," *The Midday*, (May 2, 2025).
[40] *Ibid.*
[41] Cyber Security Centre of Excellence*,* 7 Biggest Ransomware attacks in India, *available at: https://ccoe.dsci.in/blog/7-biggest-ransomware-attacks-in-india* (Last visited on May 20, 2025).
[42] Hackers steal 26 lakh Haryana power consumer's data, demand Rs 1 crore ransom, *The Statesman* (March 28, 2018).

Emergency Response Team (CERT) has developed a Cyber Crisis Management Plan to address cyber attacks.[43]

3D Technology: The use of 3D technology by extremists and terrorists for the making of guns in the West is also a matter of concern. The case of Stephen Balliet, a 27-year-old German citizen, use of homemade weapons and the posting of his 3D design and manifesto online. In this antisemitic attack, he killed two people and streamed it live on the internet.[44] Though the terrorists in India have not used the technology, the time is not far when it will be put to use.

Lone Wolf attacks: These are carried out by individuals who are inspired by extremist ideologies and online radicalisation and take the initiative. They are not associated with any terrorist groups, nor do they receive any formal training, nor do not have direct ties with terrorist organisations, which makes their attacks difficult to predict and counter. These lone wolf attacks are not a new phenomenon; the era between 1878 to 1934 was marked by anarchist terrorism, where most of the actors were lone wolves as they rejected organised leadership.[45] The first lone wolf attack was the assassination of U.S. President McKinley in 1901. What distinguishes contemporary lone wolf attacks is that current perpetrators are more driven by internet radicalisation, particularly via social media platforms, which provide them the means to execute violent acts. Easy access to violent propaganda online, mental health issues among the youth, and vulnerability are the contributing factors of growing lone wolf attacks in the world, especially in the West. The data shows that between the years 2000 to 2009, there were 3.7 mass shooting events per year; however, the number rose to 5.8 and from 2020 to 2024, it was 5.6 per year.[46] The latest was this year in Sweden, where ten people were killed in a mass shooting.[47] Lone wolf attacks are less common in India, but considering the awareness that travels faster than the speed of light in contemporary times, it is a matter of national security concern, as the attackers are not anticipated and are often of a young age, thus increasing the chances of successful detection and launch.

---

[43] Priyanka Gandhi and Sonal Pahwa, " All India Institute of Medical Sciences(AIIMS) Delhi: Cyberattack puts digitalisation under scanner," 2(2) *IMIB journal of Innovation and Management* (2024).
[44] Julia Kupper*, Decoding Terrorism: An Interdisciplinary Approach to a Lone-Actor Case* (Cambridge University Press, 2024)
[45] Institute for Economics and Peace, "Lone Wolf and Youth Terrorism," *available at: https://www.economicsandpeace.org/wp-content/uploads/2025/03/Lone-Wolf-and-Youth-Terrorism.pdf* (Last visited on March 13, 2025).
[46] *Ibid*
[47] *Ibid*

Deepfakes: This technology utilizes Generative Adversarial Networks (GANs) algorithms to produce highly realistic fake content that emulates real individuals while incorporating alterations.[48] The technique can spread misinformation and disinformation, thus contributing to the problem of law and order. Due to the advent of technology, the lines between fact and fiction are getting blurred by the day. The most recent example, according to the *Indian Express*, is when doctored, unverified visuals and videos were circulating on social media when India gave a befitting reply to Pakistan in response to the terror attack on the civilians in the Union Territory of Jammu and Kashmir.[49] The Deepfakes technology was used deliberately to instill fear and panic among the people. Dedicated teams are appointed to make and disseminate this content through social media influencers, platforms, and apps. It is a form of parallel warfare where people are caught between misinformation and factual information. This misinformation spreads at the click of the mouse, but reality takes time to reach, and by the time the damage is done. Fear escalates, and public opinion and narratives are formed, which are hard to break. Terrorists and extremists can exploit this deepfake technology to spread false narratives. These can result in escalating social unrest, forming political opinions and thus contributing to the law and order situation. The deepfakes technology results in the *Liar's Dividend phenomenon,* where genuine and reliable facts are dismissed as fake. It erodes the credibility of the factual information and creates an environment of disinformation and apprehension.[50] According to the Report by the Home Secretary, the number of deepfake videos has increased by 550%, resulting in around 95,820 incidents in 2023, making India the sixth country affected by this emerging threat. Another technology used to spread misinformation is voice cloning technology. It is used to replicate someone's voice accurately. This technology can lead to financial fraud and scams, thus contributing to economic instability and consumer mistrust.

Agroterrorism: Agroterrorism refers to the intentional dissemination of hazardous substances, including pathogenic bacteria, fungi, parasites, and pests, to infect plants, animals, crops, or humans, resulting in disease, poisoning, and death.[51] It is an attempt to infect animals and people, thus causing considerable economic harm and food insecurity. It has become a

[48] Ankita Sultania, "Deepfakes in India: Legal challenges and regulatory imperatives," 3(3) *Journal of Legal Research and Juridical Sciences*, 648-655 (2022).
[49] Aishwarya Khosla, "Warfares at the night, Deepfakes at the day: The anatomy of the rumour in modern era conflicts," *Indian Express*, May 29, 2025.
[50] *Id*
[51] Sunita Chandel, "Agroterrorism: An Upcoming threat to agriculture and Food Security" 02 *Agri Articles* 319-324 (2022).

national threat as a result of globalisation. This kind of terrorism is on similar lines to biological warfare and chemical warfare.[52]

The proliferation of digital platforms, along with the aforementioned modern dangers to national security posed by vested interests, presents a problem that India must confront.

threats to national security by vested interests are a challenge that India needs to address.

Counter Terrorism Measures: The Legal and Institutional Framework In India

The Parliament of India has enacted special laws to address the issue of terrorism in India. The statutes, such as the Unlawful Activities (Prevention) Act,[53] of 1967 and the National Security Act,[54]of 1980, the National Investigating Agency Act,[55] of 2008, the Information Technology Act,[56] 2000 has provisions to control terrorism and online radicalisation; However, in the light of emerging threats like 3D Technology, the Lone wolf attacks, Deepfakes, Voice Cloning, agro-terrorism, it is imperative to broaden the horizon of these statutes or bring the new laws on statute books.

The UAPA, 1967, and the NSA, 1980, empower the government to take decisive steps against terrorism and related matters. The term terrorist act is defined as any act that intends to threaten the unity, security, sovereignty, economic security, monetary security and integrity of India with the use of bombs, dynamites, etc to instill fear or terror amongst the people or kidnaps, abducts any person or persons so to compel the government to do or abstain from doing an act commits the terrorist act.[57] The statutes provide stringent penalties for individuals and organisations engaged in terrorism. The person who commits the terrorist act shall be given an imprisonment of five years, which may extend for life or the death penalty.[58] The definition is incorporated in the Bharatiya Nyaya Sanhita,[59] 2023 (hereinafter referred to as BNS). The BNS, 2023, also provides for a punishment of seven years or life imprisonment to anyone who, by words, actions, visible representations, or electronic communications, attempts to incite

[52] *Ibid*.
[53] *Supra* note 31.
[54] *Supra* note 32.
[55] The National Investigating Agency Act, 2008 (Act 34 of 2008).
[56] The Information Technology Act, 2000 (Act 21 of 2000).
[57] *Supra* note 31 at s.15.
[58] *Id* at s.16.
[59] The Bharatiya Nyaya Sanhita Act, 2023 (Act 45 of 2023).

secession, armed rebellion, or subversive activities, or endangers the sovereignty, unity, and integrity of India.[60] The NSA, 1980, is a preventive detention law that detains an individual whose activities are anticipated as prejudicial to the sovereignty and integrity of India.[61] This Act is not punitive in nature, but rather preventive. These statutes grant law enforcement agencies the power to swiftly deal with perpetrators of terrorism, aiming to jeopardise the sovereignty and integrity of India. However, the concerns lie in the excessive use of the law and its subsequent encroachment upon the civil liberties of Individuals.

The NIA has been instrumental in apprehending the terrorists, the Overground workers (OGWs), and their sleeper cells in India. The agency works directly under the Central government and investigates and prosecutes offences concerning terrorism and other related activities. The agency is proactive and responds swiftly to domestic or transnational threats emerging from terrorism. It has also been empowered to arrest, search, and seize persons and their property for the purpose of effective investigation.[62] It has played a key role in apprehending the terrorists involved in many gruesome terrorist attacks in India, such as the Malegaon blasts in 2008, the Pathankot attack in 2016, and the Pulwama attack in 2019. The arrests were made based on available oral, digital, forensic, and electronic evidence.

To counter digital terrorism, the IT Act of 2000 penalizes whoever threatens the unity, security, or sovereignty of India by denying access to any person authorized to access a computer, or tries to exceed authorized access, or introduces a contaminant into the computer, with imprisonment for life.[63] To enhance cybersecurity and prevent the spread of computer contaminants, the central government shall authorise any agency to monitor and collect traffic data, resources, or information generated in any computer resource. The intermediary shall provide all access to the agency duly appointed by the Central government. If the intermediary intentionally or knowingly fails to provide access to the latter, they will be punished for a term that may extend to three years and a fine.[64] The intermediary, if it conspires, or abets the commission of an unlawful act, or fails to remove the content which is unlawful in nature, shall not be exempted from the liability so imposed by the IT Act 2000.[65]

[60] *Ibid* at s.152.
[61] *Supra* note 32 at s.3.
[62] *Ibid.*
[63] The Information Technology Act, 2000 (Act 21 of 2000) s.66F.
[64] *Id* at s. 69A.
[65] *Id* at s.79(3).

To counter Deepfakes technology in India, the legal framework is yet to be made; however, the IT Rules 2021[66] puts a duty upon the intermediaries, including a social media intermediary, to have due diligence and not publish, display or modify any information that impersonates another person, or threatens the unity and integrity, security and sovereignty of India.[67] Furthermore, whoever impersonates another person for the purpose of cheating shall be punished for a term that may extend up to three years and also liable to a fine.

The legal framework to deal with the issues of terrorism and its changing dimensions with time is not enough, considering the emergence of new threats over time. Expanding the existing legal framework and incorporating new provisions dealing with these emerging threats is crucial. The existing provisions do not adequately address the threats, and the problem lies in effectively executing the laws already on the statute books.

Civil Liberties vis-à-vis National Interests: A Balanced Approach

The judiciary is the guardian and the protector of the Constitution. It plays a pivotal role in upholding the civil liberties of the people vis-à-vis national interests. The judiciary protects the rights of the people from the arbitrary action of the state. It does give primacy to national interests over fundamental rights when it is utmost required; however, the restrictions on the rights must test the principles of proportionality, necessity, and proximity to the object sought to be achieved. The laws enacted by the Parliament of India to combat terrorism in India should be used with caution and care. They must not include those that were never meant to be included by the legislature.[68] The scope of a terrorist act should be such that it goes beyond the realm of ordinary laws and must not arise from any normal law and order problem.[69] The court in *Brij Bhushan* v. *State of Delhi*[70] observed that the principles of proportionality, necessity, and proximity keep the state actions regulated, thus avoiding arbitrary encroachment upon the fundamental rights of the people. The court in *Natasha Narwal's case*[71] observed that the callous application of the UAPA on the individuals undermines the objective of the law. The intent of the parliament while enacting the law was to use it with great care and caution, and only when there is a real threat to the existence of the state. The court in *NIA* v. *Ahmed Zahoor*

[66] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
[67] *Ibid* at 3 (vi) (vii).
[68] *Niranjan Singh Punjabi* v. *Jitendra Bhimraj Bhijjaye,* (1990) 4 SCC 76.
[69] *Hitendra Vishnu Thakur* v. *State of Maharashtra,* AIR 1994 SC 2623.
[70] 1950 SCR 605.
[71] *Natasha Narwal* v. *State of Delhi NCT,* AIRONLINE 2021 DEL 832.

Shah Watali[72] observed that arbitrary power by the state against the individuals when there is no prima facie case involved loses the objective that the legislature intended to achieve while framing the law. Hence, it is incumbent upon the state to exercise its power in a constitutional and not arbitrary way.

However, the judiciary has also taken notice of the misinformation that is spread with the click of a mouse. The internet can connect the globe in an instant, but it can also serve as a mechanism for disseminating misinformation and propaganda, thereby inciting discontent and public disorder. The apex court in *Anuradha Bhasin* v. *Union of India*[73] observed that the state must keep a watch upon the digital realm, used by the terrorists for radicalising the youth and creating fear psychosis. The internet is nowadays used more for spreading misinformation, disinformation, and misleading propaganda that can create public unrest. The High Court of Delhi in *Md. Heydaitullah* v. *National Investigation Agency*[74] while dismissing the bail application of the plaintiff, observed that the nature of online radicalisation is lucrative and motivates people to join terrorist groups. The digital activities of the plaintiff demonstrate active participation and the propagation of extremist thoughts, rather than mere advocacy.

Thus, the judiciary has taken note of the emerging contemporary threats of terrorism that India faces, in addition to the traditional ones. The only concerns remain that the laws so framed for combating terrorism and its emerging threats in contemporary times should not be excessively used. The judiciary in India strikes a balance between civil liberties and national interests, as both are important to the state.

Conclusion

Terrorism intends to destabilise the established order of the state by challenging its sovereignty, integrity. It is a complex and evolving threat that transcends borders, ideologies, and technologies. The terrorist acts range from traditional methods such as bombings, hijackings, explosions, to more modern ones like lone wolf attacks, cyber terrorism, online radicalisation, 3D technology, chemical weapons, etc. Alongside the traditional security measures employed by the state, it is time to strengthen the intelligence capabilities, address the root causes of terrorism, and implement technological solutions in response to the dynamic nature of

[72] (2019) 5 SCC 1.
[73] AIR 2020 SC 1308.
[74] CR.L.A. 871/2023.

terrorism. The implementation of laws enacted to address terrorism should strike a balance between national interests and individual civil liberties. Judicial oversight of the laws should be maintained so that neither the civil liberties are compromised for the national interests nor vice versa. One cannot be prioritised against another, but to maintain an equilibrium between the two that promotes progress as well as security.