White Collar Terrorism in India: Legal Gaps

Dr. V Sandra
Assistant Professor
Providence Women's College,
Autonomous Calicut, Kerala
Email:ssskrishna100@gmail.com

Abstract

This paper examines the emerging discourse on white-collar terrorism in India. The primary aim of the paper is to highlight the legal and regulatory gaps in India that help professionals with radical mentality who indirectly or directly facilitate extremist activities using their professional advantages and privileges. Relating to theories of criminology, white- collar crime and contemporary terrorism studies, this paper explores how professionals with radical ideologies misuse their potential, skills, institutional access, professional identity and expertise for financing, logistical coordination, digital communication and ideological mobilisation for radical and extremist activities. The paper argues that existing anti-terrorist laws in India are primarily designed to punish direct participation in terrorist activities and therefore, those indirectly help terrorism while appearing to perform their normal professional duties escape from the legal proceedings. The paper advocates for making clearer statutory definitions of professional liability, enhancing inter-agency coordination, implementing stronger digital and financial oversight, and promoting a preventive, system-oriented compliance culture that can effectively counter the emerging dynamics of white-collar terrorism in India.

Keywords

White-collar terrorism, white-collar crime, criminality, India, professional crime.

Reference to this paper should be made as follows:
Received: 08-03-26
Approved: 22-03-26

Dr. V Sandra

White Collar Terrorism in India: Legal Gaps

RJPP Oct.25-Mar.26,
Vol. XXIV, No. I,
Article No. 05
Pg. 050-061

Similarity Check - 07%

Online available at:
https://anubooks.com/journal-volume/rjpp-mar-2026-vol-xxiv-no1--270

https://doi.org/10.31995/rjpp.2026.v24i01.005

Introduction

White collar terrorism, which refers to any form of violent extremism or radical activity planned and executed by a person or group of persons who belong to a respectable profession in the course of a radical act, is a relatively new coinage in academia (Newman & Anderson, 1988). The key characteristic of this radical activity includes the involvement of educated and skilled professionals with intellectual and technical expertise in the designing of sophisticated attacks to spread a specific ideology, ensuring their escape from any chance of detection of their involvement (Michel, 2026). The major professional groups often considered white-collar in this setting include medical practitioners, lawyers, engineers and academicians (Mahajan & Sharma, 2019). The term 'white collar terrorism' did not originate from a single definition, but it evolved through the convergence of deliberations on organised and non- spectacular crimes. The term originated from Edwin Sutherland's (1993) coinage, "white collar crime," which he presented in his seminal work *White Collar Criminality*. In this book, Sutherland used this term to describe the act of crime by elite, respectable actors who perform serious social harms through their occupational roles.

While countries across the world have their own policies to describe and prevent any form of terrorist acts, they generally do not classify terrorism based on the profession or educational status of those involved in terrorism related act. However, after incidents such as the Ahmedabad Serial Blasts (2008) and Bangalore Serial Blasts (2008), Indian news media started highlighting the involvement of engineering students and IT professionals from the urban middle-class background in the radicalisation. These terrorist attacks involved not only militant operatives but also the participation of educated and technically skilled individuals who contributed to the planning, logistics and communication aspects of the attack. The coordinated planting of bombs within a short period of time demonstrated technical precision, including the use of improvised explosive devices assembled with LPG cylinders, ammonium nitrate, detonators, batteries and timed circuits. Investigations revealed the use of stolen vehicles transported across states, the strategic placement of explosives in hospitals and public transport systems, and the circulation of a pre-attack email sent minutes before the blasts claiming responsibility in the name of Indian Mujahideen (Gosh, 2022). The email, traced to an IP address in Navi Mumbai, reflected technological sophistication and digital knowledge. Several accused were linked to organised networks such as Students Islamic Movement of India (SIMI) and Harkat-ul-Jihad-al-Islami, with investigations indicating structured planning meetings, training camps, logistical coordination and cross-border linkages. The execution required skills in bomb assembly, digital communication, transportation

management and operational secrecy. These all suggest the involvement of individuals with technical education and organisational capability rather than spontaneous actors (Teesha, 2025). It also reflects how professional or white-collar competencies, particularly in engineering, information technology and communication, can be utilised to conduct terrorist operations.

Though the involvement of professionals has been part of the terrorist activities for a long time, the term white-collar terrorism, particularly to address the professionals, became more popular in the media discourse after the ISIS Kerala and Karnataka Module Case (2016-2023), which recognised the joining or supporting of professional and technically educated youths from Kerala and Karnataka in the Islamic State (ISIS) (Piyush, 2025). The latest Delhi Red Fort terror attack in November 2025, which involved the suicide bomber Dr. Dr Umar Mohammad, a medical practitioner by profession, further motivated the media and the investigators to use the term white-collar terrorism. The investigators described this attack as a "white collar terror ecosystem", a network of educated professionals, predominantly doctors, who allegedly used their social legitimacy and professional positions to build infrastructure for terrorist activities whilst maintaining links with handlers across the border (Sentinels, 2025). In this context, the Indian media used the phrase to emphasise online radicalisation and technological sophistication for terrorist acts (Jain, 2023). Abhinav Pandya (2025) argues that while the 'white-collar terrorism' is presented as a fancy jargon in the mainstream media, prime-time shows and YouTube podcasts, it is not as new as it is presented now. However, the term remains as a media construct and not yet recognised as a legal or academic term in terrorism studies. It is in this context that this paper attempts to understand the possibilities of the term white-collar terrorism. This exploration will offer valuable insights into the complex dynamics of *white-collar* terrorism and can inform future research and policy efforts to prevent and detect similar cases (Rashidian & Archie, 2025).

Literature Review

Recent scholarship has increasingly recognised the involvement of white-collar professionalism, employing their characteristics like occupational status, technical expertise, organisational authority and social legitimacy for terrorism related acts in complex and indirect ways. The traditional, white-collar crime was conceptualised as non-violent economic offending committed by individuals in positions of trust. However, contemporary research demonstrates that professional roles, corporate structures, and financial systems may also facilitate or sustain terrorist activities. A study conducted by Gottschalk and Hamerton (2025) using "convenience theory" argued that organisational opportunity, weak oversight and the erosion of

trust enable white-collar offending. Their study suggested that professional environments can create structural convenience through access to financial systems, regulatory loopholes, and institutional protection, which may indirectly support illicit financial flows, including those linked to extremist networks. Expanding this framework, Kamaei et al. (2025) highlight how increased professional integration into economic sectors broadens access to white-collar crime opportunities, including cyber-enabled financial crimes that may overlap with terrorism financing mechanisms. A study conducted by Shichor (2017), applying white- collar crime frameworks to terrorism, explored the theoretical overlap between white-collar crime and terrorism. Shichor argued that factors such as "lure of gain," weak external oversight, and internal rationalisations, originally used to explain corporate misconduct, can also illuminate pathways into extremist activity like terrorism. This suggests that professional expertise and institutional access can be mobilised for ideological as well as financial objectives. Similarly, Grieco (2023) underscores the operational convergence between corporate crime and terrorist financing, particularly through money laundering, shell entities, and financial manipulation. A study conducted by Pacini et al. (2019) also supports this argument, demonstrating how shell corporations, often established or facilitated by accountants, lawyers, and financial consultants, can obscure beneficial ownership and enable both white-collar fraud and terrorism financing. Teichmann (2019) reveals how compliance systems in financial institutions are frequently circumvented by professionals with insider knowledge, highlighting the role of expertise in sustaining illicit financial networks.

From a broader structural perspective, Holmes (2024) argues that organised crime, white- collar crime, and terrorism increasingly overlap within legitimate economic spaces, particularly through globalisation and technological advancement. This convergence blurs the boundary between lawful enterprise and political violence. Levi (2022) similarly notes that while organised crime is neither a necessary nor sufficient condition for terrorism, financial crimes, including white-collar offences, can sustain large terrorist networks over time, especially where ideological groups require substantial funding. Empirical studies also illustrate the institutional dimension of this nexus. Hagan (2024) documents how international banking misconduct intersected with terrorism-related compensation mechanisms, exposing how corporate financial systems can become entangled in global violence and political responses. LaFree (2022) observes that both white-collar offenders and terrorists often perceive themselves as non-criminal actors, reinforcing the importance of professional identity and moral neutralisation in understanding participation in both domains.

The literature indicates that white-collar professionalism does not inherently produce terrorism; rather, it creates structural opportunities, technical capacities, and institutional shields that may facilitate terrorism financing, logistical support, or ideological mobilisation. The convergence emerges particularly in areas such as money laundering, corruption, shell entities, cyber-finance, and regulatory capture. Contemporary scholarship thus calls for an integrated criminological framework that situates terrorism within broader analyses of economic crime, organisational trust, and professional misconduct.

Modus Operandi of White-Collar Terrorism

The modus operandi of white-collar terrorism is marked by the strategic misuse of professional legitimacy, institutional access, and technological sophistication to conceal extremist activities. Individuals in respected professions exploit their status to justify frequent travel, procure regulated materials, access laboratories, and move goods with minimal suspicion (*White collar terrorism*, 2025). Academic institutions and professional spaces such as university labs, faculty residences, and medical hostels may be misused as safe zones for meetings, storage, and operational planning. Communication and coordination typically occur through encrypted digital platforms, including secure messaging applications, encrypted VoIP calls, and virtual private servers, alongside social media channels used for radicalisation and recruitment. Recruitment often takes place within trusted professional networks, targeting students, junior colleagues, and associates for logistical or support roles. Financial transactions are layered through crowdfunding, NGO-style fronts, digital wallets, cryptocurrencies, and informal hawala channels to obscure funding trails. In some cases, cross-border coordination and emerging technologies such as drones are employed for transferring arms, components, or funds, reflecting a high degree of operational planning and adaptability (Piyush, 2025).

White-Collar Terrorism in the Indian Context

The intervention of the professionals in terrorist activities takes place through various means such as financing, legal compliance, technological assistance and formation of organisations for the spread of specific ideologies (Farber & Yehezkel, 2024). The involvement of professionals amplifies the reach and sustainability of terrorist networks. Unlike foot soldiers, professionals provide technical legitimacy, financial sophistication, and institutional cover. Their actions may not be violent, but they enable violence by ensuring that funds move undetected, documentation appears legitimate, and digital communications remain secure.

Terrorism Financing

One of the most significant areas of professional involvement in terrorism

is financing. Terrorist groups require funds for recruitment, weapons procurement, training, propaganda, and logistics (Limodio, 2022). In India, investigations have shown that formal banking systems, shell companies, and charitable fronts have occasionally been misused to channel illicit funds. Chartered accountants and financial consultants play a critical role in setting up corporate entities, managing accounts, and navigating regulatory frameworks. When these professionals manipulate documentation, create layered transactions, or fail to report suspicious activity, they can indirectly support terrorist financing.

Legal and Administrative Complicity

Lawyers and bureaucrats may also become entangled in white-collar facilitation of terrorism. While legal representation is a constitutional right, complicity arises when legal expertise is used to deliberately shield illicit financial flows or obstruct investigations. Similarly, corruption within administrative systems, such as the issuance of fraudulent identity documents, licenses or land registrations, can provide logistical support to extremist networks. India's experience demonstrates how bureaucratic inefficiency or misuse of statutory authority can weaken counter-terrorism efforts. When regulatory bodies lack independence or are influenced by political or economic interests, oversight mechanisms fail. Such institutional vulnerabilities create opportunities for professionals within the system to misuse their authority for personal gain or ideological alignment.

Technology Experts and Digital Platforms

The rise of digital technology has expanded the role of professionals in terrorism-related activities. While the integration of digital technologies such as the internet, Internet of Things and social media platforms has created a communication revolution, these advancements have also given rise to several cyber threats that can lead to terrorism and extremism (Montasari, 2024). Those IT specialists, cybersecurity experts and digital marketers who are motivated by certain ideologies that are a threat to national integrity and co-existence utilise their skills to design encrypted communication channels, manage online propaganda and facilitate anonymous financial transactions. Though digital payment platforms and cryptocurrencies have posed new regulatory challenges in the recent past, professionals with advanced technical knowledge and radical thoughts may exploit these systems to mask funding sources and evade detection. The 2008 Mumbai attacks illustrated the sophisticated logistical planning behind major terrorist operations (Collins, 2025). Although the attackers themselves were not white- collar professionals, investigations revealed extensive financial coordination and international transfers (D'Souza, 2026). Such operations often depend on

intermediaries who understand banking systems, international trade channels, and digital communication infrastructure.

Corporate Structures and Front Organisations

Corporate entities and non-governmental organisations (NGOs) can sometimes serve as fronts for extremist financing. Terrorist organisations seek the resources to further their cause, which makes non-profit organisations vulnerable to abuse by terrorists or terrorist networks (Financial Action Task Force, 2025). Professionals are central to registering, auditing and managing these organisations. When oversight mechanisms fail, such entities may be used to collect donations under charitable pretexts while diverting funds to extremist causes. India's compliance with global standards set by the Financial Action Task Force (FATF) has required stricter scrutiny of nonprofit organisations and financial intermediaries. It highlights the international dimension of professional accountability. The broader state–corporate nexus also deserves attention. Corruption, scandals and financial fraud cases have exposed systemic weaknesses in oversight and compliance (Sahoo, 2022). These vulnerabilities demonstrate how professionals in positions of trust can bypass internal controls. The same structural loopholes could be exploited for terrorism financing if not rigorously monitored.

Legal Gaps

White-collar terrorism is considered more dangerous because it is significantly harder to detect, as professionals carry trusted identities and rarely attract suspicion (Davar, 2025). Their access to chemicals, laboratory facilities, and technical expertise increases the potential lethality of attacks, while their careers often enable seamless movement across states, facilitating the creation of large, multi-state networks. Their capacity to plan high-intensity, multi-target attacks with the support of large quantities of explosives exposes their level of operational sophistication that can result in catastrophic consequences. When dignified professionals, such as doctors or academics, are radicalised, they use their social authority to recruit and legitimise extremist narratives. These developments have serious national security implications for countries like India. It highlights the need for stronger screening mechanisms in academic institutions, enhanced monitoring of chemical access and cybersecurity systems. It also demands dedicated counter-radicalisation programs in professional and technical colleges. Moreover, improved multi-agency coordination among law enforcement and intelligence bodies, and closer monitoring of cross-border digital radicalisation networks can also detect the intervention of professionals in radical activities.

Though India has a strong counter-terrorism framework, some legal gaps persist in addressing white-collar terrorism, particularly when professionals indirectly exploit their institutional structures to support and execute violent acts. The primary anti-terror legislation in India, the Unlawful Activities (Prevention) Act (UAPA), and its later amendments focuses largely on membership, support and direct participation in terrorist organisations, including the arrest of individuals as terrorists. The Act does not specifically address the involvement and role of professionals who facilitate terrorism indirectly through financial, technical, or administrative expertise. As a result, proving intentional complicity by white-collar actors remains legally complex, particularly when their involvement is masked within legitimate occupational functions. Similarly, the Prevention of Money Laundering Act (PMLA) criminalises money laundering linked to scheduled offences, including terrorism (Kaura, 2017). However, enforcement challenges arise in demonstrating the knowledge requirement of professionals such as accountants, auditors and compliance officers. Many cases collapse due to difficulties in proving that the accused knowingly assisted in laundering funds connected to extremist activities rather than merely performing routine professional services. The absence of clear statutory standards defining "wilful blindness" or professional negligence in terrorism financing cases creates ambiguity in prosecution.

Another major gap lies in the regulatory fragmentation of agencies such as the Enforcement Directorate (ED), National Investigation Agency (NIA), Reserve Bank of India (RBI), and Financial Intelligence Unit (FIU-IND). Since they share overlapping responsibilities in monitoring financial irregularities, there exist coordination deficits and bureaucratic compartmentalisations that can delay intelligence sharing and reduce accountability. Professionals with radical mentalities may make use of these institutional loopholes to move funds across sectors without triggering immediate suspicion.

The digital spheres also have certain limitations; the existing information technology and cybersecurity laws struggle to keep pace with encrypted communication, cryptocurrency transactions and other cross-border crowdfunding platforms. Though there are regulatory efforts, technological experts with extremist intentions can manipulate decentralised systems that fall outside traditional banking oversight. The existing law has loopholes that skilled professionals can exploit. In addition, India lacks a clear statutory framework imposing enhanced due diligence obligations on certain high-risk professional categories, such as lawyers, chartered accountants, and company secretaries, when dealing with politically exposed persons or suspicious financial structures. While reporting requirements exist under AML/

CFT norms, enforcement against professional enablers remains inconsistent. Professional regulatory bodies also tend to treat misconduct as ethical violations rather than national security concerns, which limits deterrence.

As the existing terrorism preventive mechanisms focus primarily on detection and punishment rather than structural reform, it does not stop the involvement of the radicals. At the same time, the weak whistleblower protection, limited transparency in corporate ownership records, and delays in judicial proceedings reduce the deterrent effect of existing laws. As there are no strong mechanisms to ensure professional accountability, white-collar actors may continue to operate in grey areas between legality and complicity.

Conclusion

This paper highlighted how white-collar terrorism in India and elsewhere indirectly enables extremist activities through financial manipulation, technological expertise and institutional access. Although India has a strong legal framework, gaps in professional liability, regulatory coordination and technological oversight continue to create vulnerabilities. Addressing this challenge requires clearer statutory definitions, stronger inter-agency cooperation, enhanced monitoring of digital and financial systems, and greater ethical accountability within professional communities. A preventive, system-oriented approach, rather than a purely punitive one, is essential to protect institutional integrity and effectively counter the evolving dynamics of terrorism.

References

1. Browning, S. L., Butler, L. C., & Jonson, C. L. (2024). *Gender and crime: Contemporary theoretical perspectives*. Routledge.
2. Collins, L. (2025, November 26). Urban warfare project case study #16: Mumbai terrorist attacks - modern war institute. *Modern War Institute* -. https://mwi.westpoint.edu/urban-warfare-project-case-study-16-mumbai-terrorist- attacks/
3. Davar, K. (2025, December 5). *Confronting white-collar terrorism in India*. Orfonline.org; Observer Research Foundation. https://www.orfonline.org/expert-speak/confronting- white-collar-terrorism-in-india
4. D'Souza, S. M. (2026, February 11). *Mumbai terrorist attacks of 2008*. *Encyclopaedia Britannica.*
5. Farber, S., & Yehezkel, S. A. (2024). Financial extremism: The dark side of crowdfunding and terrorism. *Terrorism and Political Violence*, 1–20. https://doi.org/10.1080/09546553.2024.2362665

6. Financial Action Task Force. (2025, July 8). *Comprehensive update on terrorist financing risks*. FATF.
7. Ghosh, S. (2022, February 11). Explained: The Ahmedabad blasts of 2008, recalled. *The Indian Express*. https://indianexpress.com/article/explained/ahmedabad-serial-blasts- case-of-2008-recalled-7767130/
8. Gottschalk, P., & Hamerton, C. (2025). *Economic crime and conceptions of trust: Offender convenience by organisational opportunity*. Springer International Publishing.
9. Grieco, E. (2023). White-collar crime and terrorism. In *Countering Terrorist and Criminal Financing* (pp. 127–138). CRC Press.
10. Hagan, J. (2023). Banking on genocide: The racial disparities and patriotic politics of a massive international corruption case. *Journal of White Collar and Corporate Crime*. https://doi.org/10.1177/2631309x231205182
11. Holmes, L. (2024). *Rethinking organised crime*. Edward Elgar Publishing.
12. Jain, B. (2023, July 20). *Major terror bid foiled as NIA busts Kerala-based ISIS module*. The Times of India. https://timesofindia.indiatimes.com/india/major-terror-bid-foiled-as- nia-busts-kerala-based-isis-module/articleshow/101994421.cms
13. Jayasekara, S. D., Perera, K. L. W., & Ajward, R. (2024). Structural deterrents of combating white-collar money laundering in emerging economies: evidence from Sri Lanka. *Journal of Money Laundering Control*, *27*(4), 630–646. https://doi.org/10.1108/jmlc-05-2023-0097
14. Kamaei, M., Gottschalk, P., & Dearden, T. E. (2025). *The gender gap in white-collar crime: A multi-country study of women offenders in economic crime*. Apple Academic Press.
15. Kaura, V. (2017). India's Counter-Terrorism Policy against Jihadist Terror: Challenges and Prospects. *Connections*, *16*(4), 51–67. https://www.jstor.org/stable/26867926
16. LaFree, G. (2022). In the shadow of 9/11: How the study of political extremism has reshaped criminology. *Criminology; an Interdisciplinary Journal*, *60*(1), 5–26. https://doi.org/10.1111/1745-9125.12299
17. Levi, M. (2022). The organised crime-terrorism nexus and its funding. In *The Nexus Between Organised Crime and Terrorism* (pp. 125–145). Edward Elgar Publishing.
18. Limodio, N. (2022). Terrorism financing, recruitment, and attacks.

Econometrica: Journal of the Econometric Society, *90*(4), 1711–1742. https://doi.org/10.3982/ecta18530

19. Mahajan, R., & Sharma, S. (2019). A case study on white-collar crimes in different professions. *International Journal of Emerging Technologies and Innovative Research, 6*(5), 658–662. http://www.jetir.org/papers/JETIR1905D93.pdf
20. Michel, C. (2026). Blame attribution for white-collar crime in France and the US: Comparative profiles of public attitudes. *Journal of White Collar and Corporate Crime*, *2631309X261424893*. https://doi.org/10.1177/2631309x261424893
21. Montasari, R. (2024). The impact of technology on radicalisation to violent extremism and terrorism in the contemporary security landscape. In *Advanced Sciences and Technologies for Security Applications* (pp. 109–133). Springer International Publishing.
22. Newman, D. J., Anderson, P. R. (1988). *Introduction to Criminal Justice.* Random House.
23. Pacini, C., Hopwood, W., Young, G., & Crain, J. (2019). The role of shell entities in fraud and other financial crimes. *Managerial Auditing Journal*. https://doi.org/10.1108/MAJ-01-2018-1768.
24. Pandya, A. (2025, December 20). *How 'white-collar terrorism' is not a new phenomenon*. Usanas Foundation. https://usanasfoundation.com/how-white-collar-terrorism-is-not-a- new-phenomenon
25. Piyush. (2025, November 14). *White-collar terrorism: Meaning, recent cases, modus operandi, and national security impact*. StudyIQ. https://www.studyiq.com/articles/white-collar-terrorism/
26. Rashidian, C., & Archie, K. (2025). A multi-theoretical approach to understanding the Tom Girardi embezzlement scheme: Integrating convenience theory, game theory, and social network theory. *Proceedings of the Annual Hawaii International Conference on System Sciences*.
27. Sahoo, N. (2022). Corruption and national security: Insights from the Indian experience. In *India Studies in Business and Economics* (pp. 235–247). Springer Nature Singapore.
28. Sentinels, I. (2025, November 11). *Delhi Red Fort terror attack: Doctor identified as suspected bomber*. India Sentinels. https://www.indiasentinels.com/internal- security/nia/delhi-red-fort-terror-attack-doctor-identified-as-suspected-bomber-7099

29. Shichor, D. (2017). Adopting a white-collar crime theoretical framework for the analysis of terrorism: An explorational undertaking. *Journal of Contemporary Criminal Justice*, *33*(3), 254–272. https://doi.org/10.1177/1043986217699314 Sutherland, E. H. (1993). *White Collar Criminality*. Irvington.
30. Teesha, C. (2025). Ahmedabad serial bomb blast case. *Indian Journal of Legal Review, 5*(1), 1091–1106. Institute of Legal Education. https://iledu.in
31. Teichmann, F. M. (2019). Recent trends in money laundering and terrorism financing. *Journal of Financial Regulation and Compliance*. https://doi.org/10.1108/JFRC-03- 2018-0042
32. *White collar terrorism*. (2025, November 12). INSIGHTS IAS - Simplifying UPSC IAS Exam Preparation. https://www.insightsonindia.com/2025/11/12/white- collar-terrorism