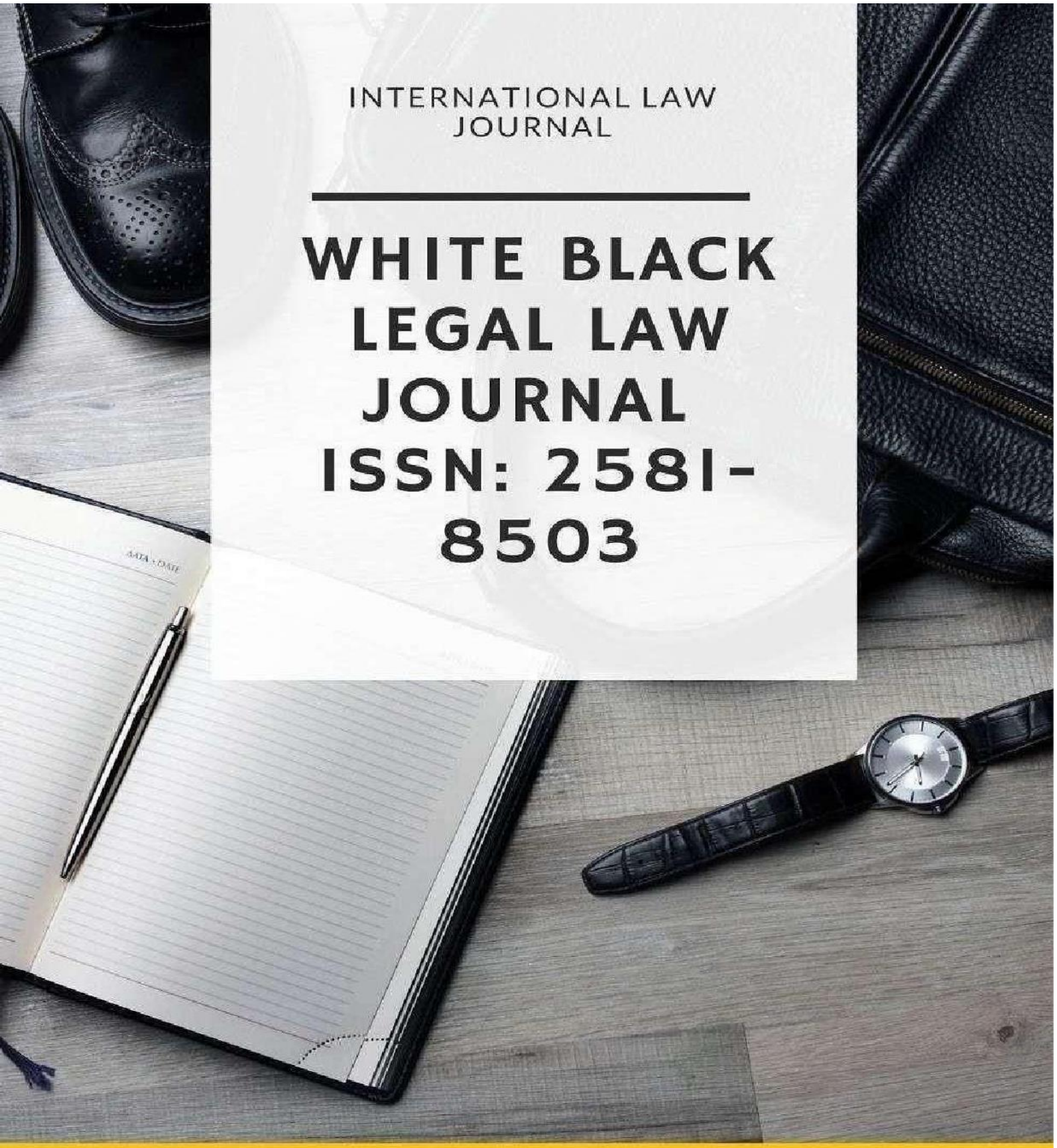

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

www.whiteblacklegal.co.in
Volume 3 Issue 7 | June 2026 ISSN: 2581-8503

CYBER TERRORISM IN INDIA: AN ANALYSIS OF LEGAL FRAMEWORK AND ITS EFFECTIVENESS

AUTHORED BY - PARAKH JAIN
Monad University, Hapur, Uttar Pradesh

Abstract

Cyber terrorism has emerged as a serious threat to national security in the digital age. India's growing dependence on digital technologies, online banking, e-governance, and communication networks has increased the risk of cyber-attacks on government institutions, financial systems, and critical infrastructure. Cyber terrorism involves the use of computers and the internet to create fear, disrupt services, or threaten the security and sovereignty of a nation.

To combat such threats, India has introduced laws such as the Information Technology Act, 2000, especially Section 66F, which deals with cyber terrorism. Other laws like the Unlawful Activities (Prevention) Act, 1967 (UAPA) and agencies such as CERT-In also help in preventing and investigating cyber-related offences.

However, despite these measures, India still faces challenges such as cross-border cyber-attacks, lack of technical expertise, weak enforcement, and rapidly changing technology. Therefore, stronger laws, better cyber infrastructure, and improved international cooperation are necessary to effectively tackle cyber terrorism in India.

Introduction

Cyber terrorism refers to the use of computers, networks, or digital systems to cause fear, disrupt essential services, or threaten national security for political or ideological purposes. With the rapid growth of internet usage and digital services, India faces increasing cyber threats from hackers, terrorist organizations, and foreign actors.

Cyber terrorism can include attacks on government websites, financial institutions, power grids, and communication systems. Therefore, a strong legal framework is necessary to protect national security and maintain cyber stability.

Legal Framework in India

Information Technology Act, 2000:

The Information Technology Act, 2000 is the primary law dealing with cyber offences in India.

Section 66F – Cyber Terrorism:

- Section 66F defines cyber terrorism as unauthorized access to computer resources with the intention of threatening India's sovereignty, security, or integrity. Punishment may extend to life imprisonment.

The section covers:

- Attacks on critical infrastructure
- Hacking of sensitive government data
- Disruption of essential services

Unlawful Activities (Prevention) Act, 1967 (UAPA):

- The UAPA is India's anti-terror law. It applies when cyber activities are connected with terrorist organizations, online radicalization, or terror financing.

Institutional Mechanisms:

India has established several agencies to tackle cyber threats:

- **CERT-In –** Responds to cyber security incidents
- **National Cyber Coordination Centre (NCCC) –** Monitors cyber threats
- **National Investigation Agency (NIA) –** Investigates terrorism-related cyber offences

Effectiveness of the Legal Framework

India's legal framework has helped recognize cyber terrorism as a serious offence and establish important cyber security institutions. However, the effectiveness of these laws is limited due to inadequate infrastructure, lack of coordination among agencies, and rapidly evolving cyber threats.

Conclusion

Cyber terrorism poses a serious threat to India's national security and digital economy. Although India has introduced important laws such as the Information Technology Act, 2000 and established agencies like CERT-In, challenges remain in enforcement and technological preparedness. Strengthening legal provisions, improving cyber infrastructure, and enhancing international cooperation are essential for effectively combating cyber terrorism in India.

References

- Information Technology Act, 2000
- Unlawful Activities (Prevention) Act, 1967
- National Investigation Agency Act, 2008
- Government of India cyber security reports
- Research articles on cyber laws and cyber terrorism in India