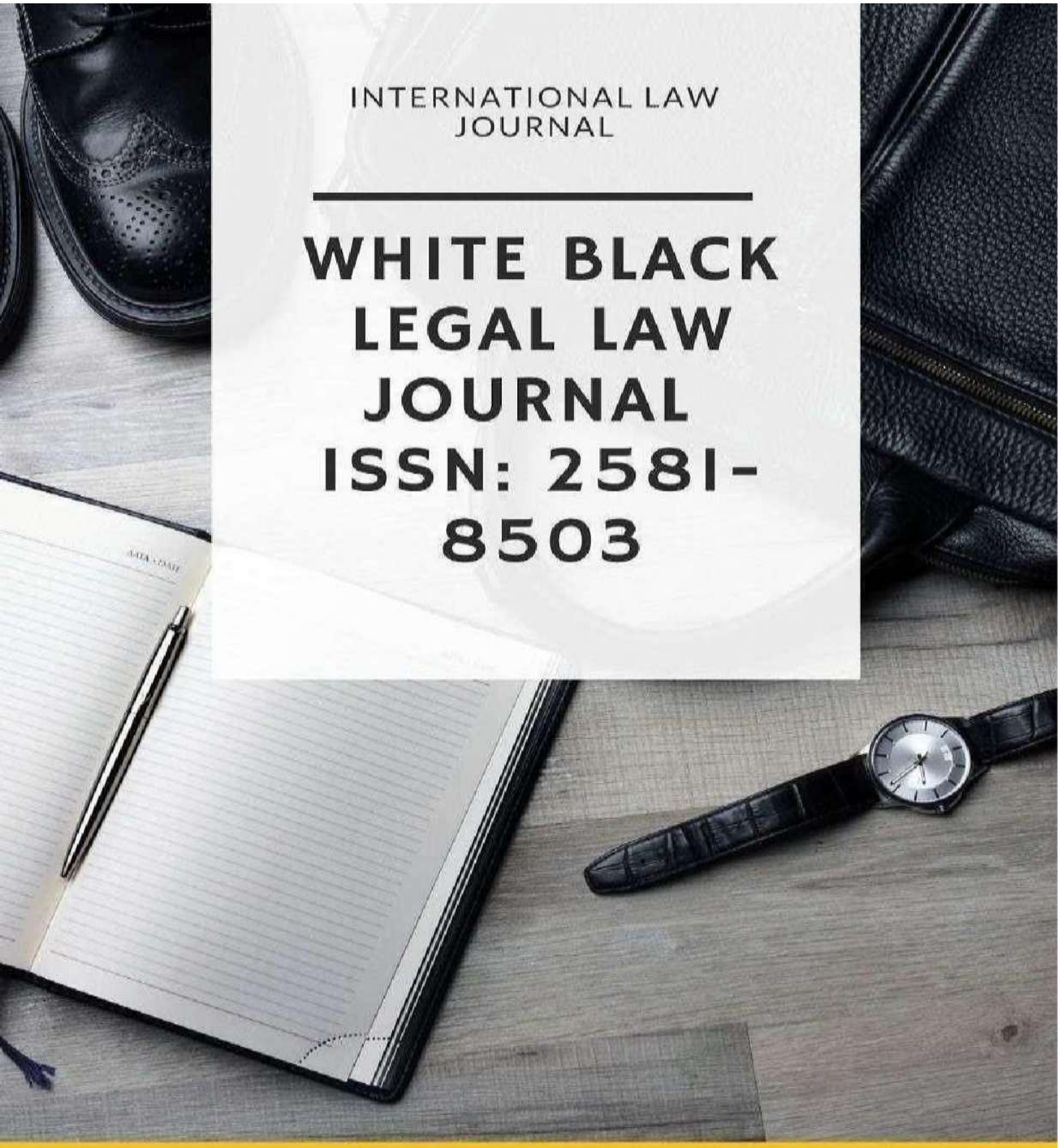

INTERNATIONAL LAW JOURNAL

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

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB, LLM degrees from Banaras Hindu University & PHD from university of Kota. He has succesfully completed UGC sponsored M.R.P for the work in the Ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; PH.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St. Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,
Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing PH.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, PH.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, PH.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on CR.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); PH.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal provide dedicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

ANALYTICAL STUDY OF INITIATIVES OF GOVERNMENT TO ALLEVIATE CYBER TERRORISM

AUTHORED BY - DR. NEETI PANDEY & DR. CHETNA SHARMA

Abstract

The development of technology has made human life dependent upon it. With human life being touched by technology, criminal acts against computers have been rising ominously. And this crime did not limit itself to a single country, but it has even stretched the criminal fraternity on the international plane with instances of cyber war, cyber terror. The Internet had been created for the common people for their convenience, but nowadays, all terrorist organizations and other criminal-minded people of terrorist organizations use technology for the benefit of their country and their organization. They succeed in their evil intents by hacking the technology of other countries. The incidences of cyber-terrorism include Uri Attack, Pulwama Attack, and 26/11 Mumbai attacks. India ranks 14th worldwide among the countries affected by cyberterrorism, which also includes digital terrorism. The research studies the essential legal principles, including the implications of statutory provisions, government initiatives to regulate and reduce cybercrimes concerning nuclear safety and interstate relations. Through this paper, the author has endeavored to examine government attempts in instituted anti-terrorist organizations. The paper is thereby oriented toward, among other things, proposing future strategies, demonstrating enforcement issues, and bringing about a stronger call to seriously consider ways of combatting cyberterrorism, improving channels for international cooperation, and integrating state-of-the-art technologies like artificial intelligence to solve enforcement issues encountered in pursuing such crimes.

Key words: Cyber terrorism, Information Technology Act, Section 66F, Indian cybersecurity initiatives, digital infrastructure.

Introduction

Since the event of 9/11 in America, it has become the standard modus operandi to avail computer-oriented mercenaries cyber assistants to fulfill their extremist objectives. The Kosovo conflict instigated the first recorded cyber terror events in 2001, which included hackers defacing multiple NATO websites and installing denial of service against them in support of anti-NATO activities. Black Tigers undertook the internet operation against the Sri Lankan embassy in 1997, involving 800 emails carrying contradicting extremist messages to disrupt communication. Al-Qaeda-style 9/11 cyberattacks against the US government, therefore, involved sending threat messages, defacing numerous websites, disrupting internet communication of government and civil amenities, and building sympathy among hackers to join the militant forum in jihad.[1]

Since 9/11, using cyber-assistance has become a thing for militants to seek their extremist objectives. In this early part of cyberterrorism, the Kosovar conflict in 2001 sparked the defacement of several NATO Web sites and DoS-ing activities from the hackers supporting anti-NATO moves; in another instance, the attacks of Black Tiger militants against the Sri Lankan Embassy involved sending 800 emails containing extremist messages to disrupt communication. Typical 9/11-like cyber-attacks have been carried out by Al-Qaeda against the USA government, wherein threat messages are conveyed to the destruction of many websites, interruption of internet communication for governmental and civil amenities, and raising an empathetic feeling among hackers willing to endorse the militant forum in its jihad.

Cyberterrorism has lately become a novel phenomenon in India. Evidence of cyberterrorism was found in plenty during the investigation into the 2008 serial blasts in Ahmedabad, Delhi, Jaipur, and Bangalore; similarly, the 2010 blast in the holy city of Varanasi and the 2008 attack on Mumbai's Taj hotel, nowadays better known as 26/11, had evidence of cyberterrorism. The Jaish Mohammad suicide bomber used virtual SIMs in the Pulwama attack in Jammu and Kashmir on 14th February 2019.

[1] Shiv Raman, Nidhi Sharma, "Cyber Terrorism in India: A Physical Reality or Virtual Myth", 5 *IJLHB* 102 (2019).

Research objective

1. What specific legal measures have been implemented by the Indian government under the Information Technology Act, 2000 to counter cyber terrorism?
2. How effective are India's cybersecurity initiatives such as CERT-In, Cyber Swachhta Kendra, and Cyber Surakshit Bharat in mitigating cyber terrorism threats?
3. What challenges do law enforcement agencies face in investigating and prosecuting cyber terrorism cases in India?
4. How does cyber terrorism affect national infrastructure, and what are the gaps in legal and technical preparedness to address such threats?
5. What role does social media play in the spread of cyber terrorism, and how is it being regulated under existing laws?

Limitations

The research in question will solely focus on computer crime as viewed with Indian Laws, conducting investigations into Indian remedial mechanisms as well as the Indian government's efforts to curb this worldwide problem.

Understanding Cyber Terrorism

This analysis will concentrate merely on cyber terrorism legislation in India and how the Indian government is fighting against this international menace.

Due to huge disagreements as to the extent to which violence can be legitimately used for political ends, an uncontested definition of terrorism could never agree upon. The term still remains unclear and undefined and is yet to acquire a largely accepted definition, either in law or academia. "Terrorism," therefore, becomes subject to the idiosyncratic definitions of states and remains malleable under any given state will. Thus, this leaves an agitated fact as to the very clashes among scholars and lawyers on the meaning of "cyberterrorism," for which the term was first proposed by Barry Collin in 1997.[2]

The offences that constitute terrorism are enumerated by the United States Federal Bureau of Investigation (FBI) as: "The unlawful use of force or violence committed by groups of two or

[2] Chapter II: Cyber Crime and Its Classification, *available at:* https://www.bbau.ac.in/dept/Law/TM/1.pdf (Visited on May 11, 2025).

more persons against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."

Indian law, Section 66F of the information technology act, 2000 defined a cyberterrorism terrorist with the intent of compromising a country's sovereignty, unity, integrity, or security. The internet's use has shown that both individuals and organizations use cyberspace as a medium to terrorize citizens of nations and endanger governments of countries. The law also states under Sec. 66F that anyone who commits or conspires to commit cyberterrorism shall be liable to a maximum punishment of life imprisonment.[3]

Indian Law related to prevention of cyber terrorism

Section 66(F) attempts to dissuade persons and organizations from participating in acts that either undermine public order or threaten national security by clearly listing these activities as crimes of cyberterrorism. The clause prescribes severe punishments for acts of cyberterrorism, such as life imprisonment. This has signified the increasing awareness of the threat posed by cyberattacks and the need for strong legal means to counter this violation. However, it raises the question of how should security and freedom be balanced in the digital age.

The year 2008 saw certain amendments being brought into the IT Act, along with provisions for cyberterrorism. The original legislation went through major changes, bringing in new definitions, offences, and penalties under the ambit of the Information Technology (Amendment) Act, 2008, to fit the ever-changing cyber scenario.[4]

The year 2008 saw certain amendments being brought into the IT Act, along with provisions for cyberterrorism. The original legislation went through major changes, bringing in new definitions, offences, and penalties under the ambit of the Information Technology (Amendment) Act, 2008, to fit the ever-changing cyber scenario.[5]

Section 66(F) of the Information Technology Act is considered vaguely strong, causing

[3] Muhammad Deri Putra, "New Media and Terrorism: Role of the Social Media to Countering Cyber Terrorism and Cyber Extremism for Effective Response", *available at:* https://ssrn.com/abstract=2754370 (Visited on May 11, 2025).
[4] D. Broeders, F. Cristiano, et.al., "Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy", 46 *Stud. Confl. Terror.* 2426 (2021).
[5] Sudhakar Rolan, "An Analysis of Law Relating to Cyber Terrorism in International Perspective", 2 *IJLRA* 13 (2023).

concern about its ramifications for democracy and the rule of law. It primarily addresses cyberterrorism, which is defined as any act committed with the intention of creating terror in the minds of people or actually causing terror to threaten India's unity, integrity, security, or sovereignty by interfering with critical services or infrastructure. The wide scope of this definition has raised concerns about its potential for abuse and violation of fundamental rights. Critics assume that because of the vague wording of Section 66(F), it could be used to suppress dissent and free speech. Whereby, democratic values are at stake.

Being a draconian provision, Section 66(F) of the Information Technology Act has generated objections as to how its application can affect democratic values and the rule of law. The section is concerned with acts of cyberterrorism, which are defined as any acts carried out with the intention of threatening the unity, integrity, security, or sovereignty of India, or with the raising of alarms among the public by way of interference with any vital service or essential infrastructure. The wide import of this definition has, therefore, raised apprehensions of possible misuse to the detriment of basic rights. Critics claim that the vague language of Section 66(F) can be used against dissent and free speech, thereby jeopardizing democratic values. [6]
A cyberterrorist in India is sentenced to death. In truth, Section 66(F) does not prescribe for the death penalty; however, the courts end up invoking the death penalty possibly with other provisions to punish cyberterrorism that results in deaths. The killing of the death penalty vis-a-vis cyberterrorism is a highly contested issue; some feel that the death penalty must operate as a deterrent to very grave offenses, whereas others feel that it is an exceptionally inhuman form of punishment that infringes on fundamental human rights. This debate on death penalties for cyberterrorism marks a few of the moral and legal issues when we try to apply traditional principles of criminal jurisprudence to the virtual world.`[7]

The IT Act's flaws and challenges

The 2015 R. V. S. Mani v. Union of India case related to the question of whether cyberattacks from foreign entities could be considered a compromise of national security and integrity of Indian government websites and databases. The court stressed that stringent action and the exercise of Section 66F of the IT Act are imperative to effectively tackle cyberterrorism. The

[6] Nibedita Mohanta, "Combatting Cyberterrorism via Spatial Insights", available at: https://geospatialworld.net/prime/special-features/combatting-cyberterrorism-via-spatial-data-insights/ (Visited on May 11, 2025).
[7] Iftikhar S., "Cyberterrorism as a Global Threat: A Review on Repercussions and Countermeasures", 10 *PeerJ Comp. Sci.* 72 (2024).

State v. Imran (2014) was a case in which the defendant sought to breach government databases to seek private information and compromise national security as part of the conspiracy of cyberterrorism. Apart from convicting the accused under the relevant sections and reiterating the gravity of cyberterrorism and its threat to national security, the court also applied Section 66F of the IT Act for cyberterrorism and Sections 121 and 124A of the IPC for waging war and sedition.[8]

Various fundamentalist organizations and individuals have been contravening the law despite the existence of the IT Act. With cybercrime and cyberterrorism posing greater problems to India in recent times, all the while including the IT Act, 2000 and its amendments, would be a disgrace. Fundamentalist individuals and organizations have somehow managed to circumvent the law and have exploited vulnerabilities in the cyber-theft-to-helpful-online-circumstances sphere. There could be many reasons ranging from the common man's ignorance about cyberthreats to police having a very limited capacity to investigate and prosecute cybercrimes to the skyrocketing technological development hurdles that are in the way of the law from keeping pace with emerging threats.

While technological threats continue to menace the Indian legal system, the Indian IT Act is considered inadequate. Those who speak ill of the 2000 IT Act say that it neither covers all cyberthreats existing in India. Some considerations have been made that criticize the Act for being too specific and limited, while others have condemned it for being too broad and vague. It has also been criticized for not disposing of several threats properly, namely cross-border jurisdiction, data protection, and privacy. Fast-paced technological advancement only aggravates the crisis that the Indian legal system faces, for creating newer varieties of cybercrimes and cyberterrorism.

The prosecution of cybercrimes, the evolving technology, causing legislations to always be behind the newly occurring threats. Moreover, none of the countries can effectively prosecute such cases by itself due to the global nature of cybercrime and cyberterrorism.[9]

[8] Astha Sharma, Aradhya Gupta, et.al., "Emerging Cybercrimes: Measures and Challenges in Cyberspace", available at: https://nhrc.nic.in/sites/default/files/Group%201_FEB%202022.pdf (Visited on May 11, 2025).
[9] Cyber Security Breach at National Informatics Centre, Malware Attack Traced to Bengaluru, *ETGovernment*, September 19, 2020.

The government's challenges in national security

Cyberterrorism's Effect on National Infrastructure

Prosecute cybercrimes, and the speed at which technology is developing, makes legislation lag behind new threats. Being an entirely new realm for interstate cooperation and the many powers against it, cybercrime and cyberterrorism-on a worldwide scale-defy any single nation from adequately responding to these threats alone.

Your dependency on information and communication technology (ICT) demands strategy in technological inclusion decision-making. As governments, businesses, and individuals continue to rely on ICTs, the national framework becomes more prone to cyberattack. Digital systems are required by essential services such as communication, transportation, water, and power, and any interference with their functioning may cause serious consequences. Hence one way for cyberterrorism to occur is through the disruption of critical infrastructure, hence causing chaos and economic damage. For that strategic value in ICTs, governments must consider technology in their national security planning and develop safeguards to protect vital infrastructure from cyberattacks.

A power grid cyberattack is a real possibility and grave danger. Because interruptions to the electricity supply can create a domino effect on other essential services and industries, the power grid is a rather vulnerable target for cyberterrorists. Should a successful cyberattack be able to paralyze the blackout of a power grid, the communication, transportation, and healthcare services would cease to operate, thereby affecting public safety and undermining national security while exposing the country to untold economic losses. It has to be multi-pronged in nature for protection of the power grid from cyberattacks, involving enhancement of cyber security defenses, improved monitoring and detection abilities, and incident responses planning.

Surveillance capabilities to Prevent Terrorists from Using Technology in the Future

Cyberterrorism can give rise to vast financial, military, and human casualties. By hacking corporations for intellectual property theft and financial defaults, these cyberattacks can inflict fatal damages on the economy. They have the power to intrude into military systems and compromise confidential information or hamper military operations. Sometimes cyberattacks can even cause loss of lives, especially if they target critical infrastructures such as

transportation or the healthcare system. The ominous possibility of considerable financial, military, and human losses calls out for the toughest cyber security measures and efficient global cooperation against cyberterrorism.

Electronic information goes through interception, being observed by government agencies, or by any form of reluctantly forced decryption procedure. In the interests of State Security, sovereignty, or integrity, the Government of India may, if so required or practicable, intercept or monitor any electronic information under Section 69 of the IT Act, or may decrypt it. This power is subject to two safeguards: firstly, the issuance of a written order by a competent authority, and secondly, adherence to procedural requirements. Yet, the wider reach of this power with non-transparent application has raised concerns over misuse and violation of privacy rights.[10]

Investigating Cyberterrorism Cases Presents Difficulties

Interception, monitoring, and decryption are the standard practices performed upon electronic information by government agencies. In interests of welfare of the people, sovereignty, or integrity, the government may, with Section 69 of the IT Act, intercept, monitor, or decrypt any electronic information, if deemed necessary or practicable to do so. This power is subject to two safeguards: the issuance of a written order by a competent authority and observance of the procedural safeguards. However, the very wide ambit of this power coupled with the opacity of procedures has caused concerns about its misuse and resulting infringement upon privacy.

Very rarely do cases get handled by technical specialists. Lack of technical competence on the side of the law enforcement agencies is amongst the major barriers toward investigations into cases of cyber-terrorism. Investigations of cybercrimes require particular skills in digital forensics, networks, or computer systems. Inadequately equipped to investigate cybercrimes efficiently are some police agents and investigators, hence making it difficult to search for and prosecute cyber terrorists. To retrofit this, law enforcement bodies ought to invest in training and development.

[10] S. Haataja, "The 2007 Cyber Attacks Against Estonia and International Law on the Use of Force: An Informational Approach", 9 *LIT* 159 (2017).

Very few law officers have technical training. One of the biggest hurdles in investigating and prosecuting cybercrimes efficiently is the lack of technically trained officers in law enforcement agencies. Cybercrime investigations require full knowledge of networking protocols, digital forensic tools, and computer technology. Complex cases of cyberterrorism are difficult to investigate, as it is nearly impossible to keep up with the evolution in techniques with fewer number of officers possessing such expertise. Law enforcement agencies need to hire and retain technically qualified personnel to enrich India's cyber security capabilities.[11]

Cybersecurity Procedures to Safeguard User Information

Furthermore, there is a lacuna. Another major hurdle is the regular jurisdictional issue. Jurisdiction issues also emerge when considering cyberterrorism cases. In the case of cybercrimes, with victims and perpetrators coming from several jurisdictions, deciding which court has jurisdiction over such a case could become an exhausting issue. However, in some cases, cybercriminals will get away from prosecution because of this problem sometimes caused by vague regulations. To redress this issue, clear jurisdictional norms shall be laid down, and utmost international cooperation shall be promoted.

Dealing with Data Security and Online Fraud

As online commerce is becoming more and more popular, the risks tied to fraud and matters of security and trust have also become severe walls. In fact, online fraud and data security breaches have grown by leaps and bounds with our increasing reliance on online commerce, stifling exponential growth of the sector. With increased awareness about the risks of online fraud and data theft, customers might tend to lose faith in e-commerce. These considerations need to be checked in the creation of a safe and convincing online environment. [12]

With the growing dependence on e-commerce, fraud risks and security and trust problems have become major hindrances. However, the rise in online fraud and data breaches have proven to be a worldwide hurdle to the flourishing of this sector due to our growing reliance on online commerce. Even the increasing concerns about online fraud and data theft may hamper customers' trust in e-commerce. In order to create a safe and reliable atmosphere, such issues need to be addressed.[13]

[11] Michael Kenney, "Cyber-Terrorism in a Post-Stuxnet World", 59 *Orbis* 111 (2015).
[12] Don Melvin and Greg Botelho, "Cyberattack Disables 11 French TV Channels, Takes Over Social Media Sites", *CNN*, April 9, 2015.
[13] Debarati Halder, "Information Technology Act and Cyber Terrorism: A Critical Review", *available at:* https://doi.org/10.2139/ssrn.1964261 (Visited on May 11, 2025).

Social Media's Contribution to Cyberterrorism

Social networking sites came with unprecedented privileges and unprecedented drawbacks; unlike anything the laws had ever had to deal with. These social media platforms have given rise to online harassment, cyberbullying, fake news, etc. These cannot be addressed through legal changes alone but in conjunction with technological advancements and user education.

The social media regulation and crimes peculiar to the social media platforms have been highlighted as one of the set of problems that social networking sites present to the untouched set of laws. Online harassment, cyberbullying, and the spread of misinformation have flourished on these sites. These issues can be addressed by legal reforms, technological remedies, and user education.[14]

Social Media as a Tool for Terrorist Propaganda and Recruitment

Technology facilitates the manufacture, dissemination, and recruitment for extremist propaganda and cyber-attacks, thus calling for stronger legal counter-measures, stressing great importance to the role of technology in facilitating terrorist activities and the response to countermeasures. Terrorist organizations use social media for propaganda, recruitment, and coordination of attacks. Hence, activities should be countered using a combination with social media monitoring, disruption of terrorist groups, and the countering of extremist narratives.

Upgraded technological advances allow for heightened propaganda, recruitment, and cyber-attacks by extremist organizations and hence need a better legal infrastructure; at the same time, they shed light on the role technology plays in facilitating terrorist activities and therefore accentuate the need to counter-terrorism efforts. Terrorist groups use social media to propagate information, recruit new members, and launch attacks. This situation has to be confronted with monitoring social media content, dismantling terrorist networks, and countering extremist narratives.[15]

Indian Government Cybersecurity Initiatives

Upgraded technological advances allow for heightened propaganda, recruitment, and cyber-attacks by extremist organizations and hence need a better legal infrastructure; at the same time, they shed light on the role technology plays in facilitating terrorist activities and therefore accentuate the need to counter-terrorism efforts. Terrorist groups use social media to propagate

[14] Tanvi Mehta, "Indian Police Arrest Minor for Hoax Bomb Threats on Flights", *Reuters*, October 17, 2024.
[15] Indian WhatsApp Lynchings, available at: https://en.wikipedia.org/wiki/Indian_WhatsApp_lynchings (Visited on May 11, 2025).

information, recruit new members, and launch attacks. This situation has to be confronted with monitoring social media content, dismantling terrorist networks, and countering extremist narratives.[16]

CERT-In, the Indian Computer Emergency Response Team

Cybercrime has been on a rise in the recent years in India, affecting all individuals and organizations via a variety of cyberattacks. To counter cybersecurity problems in the country, the Indian government has put forth numerous initiatives and laws.[17]

Cyber Surakshit Bharat

CERT-In is important while dealing with cybersecurity incidents and organizing the response efforts. In the cyberspace of India, the agency functions as a focal point for incident response, vulnerability management, and oversight of security.[18]

Cyber Swachhta Kendra

The campaign was carried forward to create awareness amongst the countrymen about cybersecurity issues in India and the recent cybercrimes. The Cyber Surakshit Bharat campaign was launched by the Ministry of Electronics and Information Technology and the NeGD under the vision of "Digital India."[19]

National Cybersecurity Policy

The campaign was carried forward to create awareness amongst the countrymen about cybersecurity issues in India and the recent cybercrimes. The Cyber Surakshit Bharat campaign was launched by the Ministry of Electronics and Information Technology and the NeGD under the vision of "Digital India." [20]

[16] Press Trust of India, "Potential for Spread of Terror from Social Media Higher Than Ever: Centre", *NDTV*, December 13, 2022.

[17] Sampath Kumar Venkatachary, Jagdish Prasad, et.al., "Cybersecurity and Cyber-Terrorism Challenges to Energy-Related Infrastructures – Cybersecurity Frameworks and Economics – Comprehensive Review", 45 *Int'l J. Crit. Infrastruct. Prot.* 100677 (2024).

[18] PTI, "NIA Files Chargesheet Against 8 Terrorists in ISIS-Kerala Module Case", *The Economic Times*, January 28, 2022.

[19] HT Correspondent, "Kashmir State Investigation Agency Produces Chargesheet in Cyber-Terror Case", Hindustan Times, December 24, 2024.

[20] Digital Arrests: Understanding Their Legal Framework, Technology, and Case Studies in India, available at: https://www.indiancybersquad.org/post/digital-arrests-understanding-their-legal-framework-technology-and-case-studies-in-india (Visited on May 11, 2025).

Conclusion

Implementing the National Cyber Security Policy for eliminating cyberthreats remains one of the most crucial steps taken by the government of India. It tries to protect data and other lots of infrastructure while at the same time creating an accepted framework for a secure cyber environment. As an important stone in digital growth of India, the Telangana government contributed significantly to setting up a center of excellence at Hyderabad. We have been working to back the Data Privacy & Protection Bill and in the development of the National Cybersecurity Policy 2020. To maintain their vision of a safe, secure, and credible cyberspace, the government together with the Data Security Council of India (DSCI) has partnered with our center of excellence in Hyderabad.[21]

Suggestion

1. Promote research and development in cutting-edge technologies like artificial intelligence, quantum cryptography, and machine learning to stay ahead of cyberterrorist capabilities and secure critical digital assets.
2. Strengthen bilateral and multilateral treaties to facilitate international cooperation in tracking, investigating, and prosecuting cyberterrorism across borders.
3. Establish fast-track courts and streamline judicial procedures for cybercrime cases to enhance deterrence and ensure timely justice.
4. Set up dedicated cybercrime helpline numbers at the district level to assist victims promptly and enhance public awareness.
5. Increase the accessibility and presence of cyber law enforcement by institutionalizing cyber thanas at the sub-divisional level for better outreach and faster response.
6. Regularly train and upskill officials responsible for cybersecurity enforcement to ensure they are proficient in handling complex and evolving cyber threats.

[21] Prevention of Cyber Crimes, *available at:* https://pib.gov.in/PressReleasePage.aspx?PRID=1845321 (Visited on May 11, 2025).