

CYBER TERRORISM AND ITS SOCIETAL IMPACT: AN EMPIRICAL STUDY

Chitra Shukla¹

ABSTRACT

Cyber terrorism has emerged as a significant threat to national security, critical infrastructure and societal stability in the digital age. This research examines the perception and impact of cyber terrorism on society with a particular focus on India. Using a mixed-research method design, the study combines quantitative survey analysis of public perception before and after awareness intervention with qualitative insights from legal and cyber security experts. The findings reveal that cyber terrorism creates severe economic, psychological and infrastructural consequences, while public awareness significantly influences threat perception. The study further identifies legal gaps, institutional weaknesses and lack of international cooperation as major challenges in combating cyber terrorism. Based on empirical evidence, the research proposes policy and legal reforms aimed at strengthening national resilience, improving public trust and developing comprehensive counter-cyber terrorism strategies.

INTRODUCTION

Cyber terrorism is the use of the internet to conduct violent acts that result in, or threaten, in order to achieve political or ideological gains through threat or intimidation. The term cyber terrorism was coined by Bary C. Collin in the late 1990s.² Cyber terrorism has developed at a large scale and involves various software, hardware, viruses, and phishing to emerge new forms of cyber terrorism.³ Cyber terrorism can also be defined as using computers, networks and the internet to cause destruction and harm. For instance, experienced cyber terrorists by hacking causes massive damages to government systems.⁴ Cyber terrorism is a major concern at

¹ PhD Research Scholar, Department of Law, Sri Padmavati Mahila Visvavidyalayam, Tirupati ² Bary C. Collin, The Future of Cyber Terrorism: Where the Physical and Virtual World Converge, 11th Annual International Symposium on Criminal Justice Issues, (1997), p. 15-18.

³ Dawoody, Alexander R. Eradicating Terrorism from the Middle East Policy and Administrative Approaches, Vol. 17 Springer International Publishing Switzerland, p. 201-206.

⁴ Liqueur, Walter; C., Smith; Spector, Michael, Cyber Terrorism, Facts on File (2002), p. 52-53. 51

international level and so various investigating agencies are trying to find effective legal measures to eradicate the cyber terrorism. In India nearly 80% of companies suffer from cyber-attacks due to which cyber security is a major concern of our nation. The punishment for cyber terrorism is life imprisonment in India.⁵

The roots of cyber terrorism can be traced in the early 1990s, when the rapid growth in internet use and the debate on the emerging information society sparked several studies on the potential risk faced by the highly networked, high tech dependent United States. After the 9/11 attacks, the terrorist organization Al Qaeda has used cyber technology as a major weapon. Cyber-attacks like ransomware, malware, phishing and hacking are an important weapon of cyber terrorists. Data encryption and other cyber security measures are adopted to protect the data from cyber terrorism. Cyber terrorism is felt as a major challenge at global level.⁶ The major reason for the increase in cyber terrorism is that it is cheaper in comparison with other traditional terrorist methods. As there are no physical barriers in cyberspace so cyber terrorism is more easy for modern terrorist organizations. The next reason is the number of targets are more enormous in which from government to private anyone's network can be easily targeted. There is less investment and more profits in cyber terrorism so it is the prime choice of terror activities. The last reason is it has more potential in comparison with other traditional terrorist methods as a result cyber terrorism is increasing along with the growth in technologies.

This research mainly aims to bring out major causes of increase in cyber terrorism and find effective measures that can be adopted to completely eradicate cyber terrorism. For this research a number of books and articles on cyber terrorism have been studied. To understand from which type of cyber-attack they face more challenges and how that impacts them a small survey has been conducted by me in which a questionnaire has been sent to the professionals of different sectors. This survey has been crucial in understanding which cyber-attack is a major instrument of these modern terrorists. At last an analysis was done on how cyber security can be ensured with the help of emerging artificial intelligence technology. This research in my opinion is very important to understand different concepts of cyber terrorism in depth and also the methods of ensuring cyber security in this digital world.

⁵Information Technology Act, 2000 s. 66F.

⁶Paul T. Augustine, Computer Crime, Crescent Publishing Corporation, (2007), p. 272

METHODS OF CYBER TERRORISM

Hacking is the first method in which the hackers have unauthorised access to computer systems or networks. It poses a threat to various sensitive information. Next method includes theft of sensitive electronic information of victims through physical or virtual medium by tampering with them. Many times the computers of target are flooded with more requests than it can handle which is also known as denial of service attacks. It is also a method used in cyber terrorism. Many times terrorist groups steal data from the network itself due to which data exfiltration occurs. Due to this method most people are affected every day. Sometimes a particular website is made unavailable to the public which is also known as defacing websites due to this public cannot access the websites. The terrorist organizations also hack the communication platforms to intercept or stop the communication. Interception of communication majorly affects the people. Sometimes accounts of financial institutions are hacked to complete a particular terror activity. In the Salami attacks which are normally done on financial institutions in which alteration of very small things that remain unnoticed is done like in the Ziegler case wherein a logic bomb was introduced in the bank's system which deducted 10 cents from every account and deposited in a particular account has been committed.⁷

Other times virus attacks are done. Viruses are programs that attach themselves to a computer or file and then circulate themselves to other files and other computers on a network. They can alter or delete the data. For example - love bug virus which has affected 5% of computers globally.⁸ There are different types of viruses in which file infector virus is the most traditional form of virus which hides within the code of another program. Whereas boot sector viruses reside in the part of the disk that is read into memory and executed when the target's computer first boots up. Script viruses are based on common scripting languages, which are macro-like pseudo-programming languages typically used on websites and in some computer applications. These viruses are written into JavaScript, ActiveX and Java applets that run when the target visits a web page or opens a Word or Excel application. Nowadays e-mail Trojans are spread as innocent-looking attachments to e-mail messages; when the target opens his e-mail the virus attached to his mail is automatically launched.⁹

⁷ Clark, Franklin & Ken Diliberto, *Investigating Computer Crime*, Boca Raton: CRC Press (1996), p. 88. ⁸ Francis & Dorothy Berber, *Computer Crime*, New York: Leicester Books, (1987), p. 66. ⁹ Smith, George; *The Virus Creation Label: A Journey into the Underground*, American Eagle Publication (1994) p. 76.

The worm is also used as a kind of weapon by modern cyber terrorists. Worm is a program that exists in system memory, making it harder to identify than conventional file-hosted worms. These worms can cause havoc in future. There are also risks from cookies as it enables a website to remember the user's details and keep track of that user's visit to that website. Cyber terrorists hack the web servers which make the websites unavailable. Rootkits give the cyber attackers complete control over the target's operating system.

Malware is a malicious computer software that can damage a computer system and assist cyber terrorists to damage the system of their target. There are many types of malware which creates different types of cyber threats. The mobile malware is used for doing cyber-attacks on the target's mobile phone by stealing his various sensitive information. Malware is used for stealing crucial data from computer systems and permanently damaging the system. The botnet malware adds infected systems to the botnet which are used by attackers for criminal activities. Crypto miners mine the cryptocurrency using the target's computer. The target even being innocent is being falsely accused of cyber-attacks. The sensitive information of the target's computer is generally stolen by using info stealers. Banking Trojans are used to steal various financial and credential information from the websites of banks.¹⁰ Ransomware is a kind of malware by which financial institutions are forced to pay huge amounts of money to unlock files or data systems. Most countries are affected by ransomware. Phishing is also the most common way of cyber terrorism in which terrorist groups manipulate their targets by sending mails and get access to the sensitive information of the government and other crucial sectors.

INSTANCES OF CYBER TERRORISM IN INDIA AND ITS IMPACTS

India is prone to different cyber terror attacks. Recently during Operation Sindoor when there was a military crisis in India, numerous cyber-attacks have been seen in Indian cyberspace. This has led to a wide range of fear among people towards their data security. Apart from this there were other cyber terror attacks such as SPARSH data breach, Tamil Nadu's Financial Recognition data breach etc. in 2023, Hathaway ISP data breach AIIMS Ransomware attack, BharatPay hacked, Swachhta Platform hacked, RailYatri data breach, CloudSEK data breach etc. in 2022, Government Website Attacks in 2012 and in 2001 Mumbai Stock Exchange Attack.¹¹

¹⁰ Paul T. Augustine, Computer Crime, Crescent Publishing Corporation, (2007) 86-90.

¹¹ Top 25 Biggest Cyber Attacks in India: Major Data Breaches & Cybercrime available at

According to the key findings of India Cyber Threat Report as published on December 5, 2024 there were 369.01 million distinct Malware detection which shows increase in the landscape of cyber threats in India.¹²

These instances have impacted India's critical infrastructure which includes railways, banks, financial markets, most reliable Government websites, companies and power grids. They create a threat among the public over misuse of crucial data which can pose a threat even to national security. The vast range of frauds that were done by cyber-attacks causes financial losses which creates economic crises. Even there can be disruption of essential services such as power which affect many people. Apart from monetary and disruption of service losses there has been widespread threat among people which subsequently affects their trust in Government and its organisations.

In response to all these cyber terror attacks Government has established specialised agencies like National Cyber Coordination Centre (NCCC) and Indian Cyber Coordination Centre (I4C) along with implementing a national Cyber Crisis Management Plan (CCMP) and promoting public awareness through initiatives like the Cyber Swachhta Kendra. NCCC implemented by the Indian Computer Emergency Response Team (CERT-In) serves as the control room to scan cyberspace in the country and detect cyber security threats.¹³

Even though there are multiple rules and regulations providing strict legal and policy frameworks for controlling cyber terrorism but still these attacks are very common and as a result they have become a threat to human peace. Cyber technologies are growing day by day and with the emergence of AI technologies there is a threat of adoption of other techniques for committing cyber-crimes. Today there is a need for such an Act which can potentially catch the culprits of cyber terror attacks as many times due to cross border crime they escape and it becomes very difficult for law enforcement authorities to identify and arrest these criminals.

RESEARCH PROBLEM

¹² As reported by India Cyber Threat Report 2025 published by Data Security Council of India available at

The global reliance on interconnected Critical National Infrastructure has made societies acutely vulnerable to cyber terrorism. Existing counter terrorism and cyber security strategies primarily focus on technical defense and immediate response neglecting a deep understanding of the long-term impacts of cyber terrorist attacks. This lack of understanding hinders the development of holistic national strategies, effective international protocols against cyber terrorism and providing effective financial support to the victims.

There have been numerous researches focusing on technical vulnerabilities of systems and roles of legal and policy frameworks to control the growth of cyber terrorism. Lack of integrated models that systematically quantify and compare different impacts of cyber terrorist attacks on national infrastructure. The main research question is how does the impact of a cyber-terrorist attack impact on critical national infrastructure in comparison to traditional terror attacks on the same sector? This research is significant as it explores the subsequent policy that can be brought for developing the security system of our country from the multiple impacts of cyber terrorism.

RESEARCH OBJECTIVES

There are two primary objectives of this research among which the first one includes to develop a legal framework which provides comprehensive solutions to impacts of cyber terrorist attacks on critical national infrastructure. The next objective includes comparatively analysing the impact of cyber terror attacks on different sectors. There are four secondary objectives of this research, among which firstly our aim is to empirically analyse the public trust in Government and its authorities. As cyber terrorism mostly causes psychological distress among the victims. So the next secondary objective is to analyse the level of psychological distress and behavioural changes caused by cyber terror attacks. In most of the cases it is seen that rigorous legal frameworks are enacted immediately after the successful terror attacks. So this research further aims to analyse the political impact of the cyber terror attacks. The last objective of this research is to formulate evidence based policy recommendations for enhancing national resilience, public communication and psychological recovery strategies for controlling the threat of cyber terrorism.

HYPOTHESES OF RESEARCH

Based on the research problem and objectives, following hypotheses were formulated: 56

SUBODH NEXUS VOLUME V ISSUE I, JUNE 26' ISSN No: 3048-5371

H1: Awareness intervention significantly increases public perception of cyber terrorism as a threat to national security and societal stability.

H2: Cyber terrorism significantly affects public trust, psychological security and perceptions of data privacy and financial safety.

H3: Cyber terrorism poses a greater and more pervasive impact on critical national infrastructure compared to traditional forms of terrorism.

H4: Perceived inadequacy in legal and institutional frameworks significantly contributes to the persistence of cyber terrorism.

H5: Awareness and information dissemination significantly influence public demand for immediate policy and legal interventions to combat cyber terrorism.

RESEARCH METHODOLOGY

Considering the depth of concept mixed research methodology has been adopted to analyse the impacts of cyber terrorism on society. Both qualitative and quantitative analysis has been done in this research. In quantitative analysis impact related questions have been asked with respondents. Here cyber terror attacks such as malware, hacking and other methods adopted by terror groups for committing cyber terrorism have been taken into consideration while framing questions. For quantitative analysis stratified random sampling techniques have been used. The test is conducted in two phases. In the first phase without providing any detail on cyber terrorism their views have been gathered on Likert scale questionnaires. In the second phase, brief details about cyber terrorism have been provided through PowerPoint presentations. The presentation includes details of cyber terrorism, its impacts and existing policy and legal framework adopted for combatting cyber terrorism specifically in India. After this intervention again the same questionnaire is provided.

For data interpretation descriptive analysis has been used to explain each Likert scale item and people's responses for individual statements. Then mean and standard deviation for the composite scores for both the pre- and post- intervention data. By using the mean central tendency for a

composite Likert Scale score is measured. After that, inferential statistics have been used for hypothesis testing. Paired-samples t-test have been used to compare mean score of

pre-intervention and post-intervention data for the same group. Significance value is taken as 0.05.

For qualitative analysis semi-structural interviews have been done with legal and cyber experts who play a key role in providing security, government authorities responsible for framing policies and mainly with aim to identify structural and legal challenges that exist in India and which reforms can be brought to control cyber terrorism in India. For this, a sample size of 20-30 people have been interviewed. The thematic analysis has been done for the responses gathered through qualitative analysis.

DATA INTERPRETATION AND ANALYSIS

The entire research has been done in multiple phases. To assess the impact of awareness intervention on public perception of cyber terrorism, a paired-samples (dependent) t-test was employed. In the pre and post intervention survey the same 500 respondents have participated. Responses were recorded on a 5-point Likert Scale with coding as 1 = Strongly Disagree, 2= Disagree, 3 = Neutral, 4 = Agree and 5 = Strongly Agree. Composite mean scores were calculated for each statement before and after the PPT intervention on “Cyber Terrorism and Its Impacts.” The level of significance for statistics was set at $p < 0.05$.

Pre-Intervention Survey Data of respondents

Statements	SD (%)	D (%)	N (%)	A (%)	SA (%)
Cyber terrorism is a significant threat to national security.	14.8	28.2	19.2	15.6	22.2
Cyber terrorism poses a long-term threat to a country's stability.	15.6	28	18	15.8	22.6
Cyber terrorism creates a threat to personal safety.	16.8	24.2	17.6	12.8	22.8
Cyber terrorism affects the data privacy of people.	19.2	24.6	17.4	16.6	22.2
Cyber Terrorism can influence election results.	17.4	26.8	4.6	16.4	34.8

Cyber terrorism disrupts critical infrastructure of a country. 17.8 22 6.8 16.8 36.6 Personal data protection is affected due to cyber terrorism. 18.8 22.8 10.4 12.6 35.4

Public finance is at higher risk due to cyber terrorism.	19.6	23.6	6.8	16.6	33.4
Lack of proper implementation of laws increases cyber terrorism.	16.6	24	9.6	17.2	32.6
Immediate steps are highly needed to combat cyber terrorism.	13	25.2	7.2	19.6	35

The post-intervention results indicate a statistically significant increase in perceiver severity across all dimensions. Below table shows post-intervention survey results.

Post-Intervention Survey Data of Respondents

Statements	SD (%)	D (%)	N (%)	A (%)	SA (%)
Cyber terrorism is a significant threat to national security.	10.6	5.8	8.4	18.8	56.4
Cyber terrorism poses a long-term threat to a country's stability.	12	7.6	14	21.6	44.8
Cyber terrorism creates a threat to personal safety.	10.8	8	8.6	20.6	52
Cyber terrorism affects the data privacy of people.	10.2	9.2	14.4	27.2	39
Cyber Terrorism can influence election results.	8	10.8	12.4	24.6	44.2
Cyber terrorism disrupts critical infrastructure of a country.	7.4	8	10.6	23.2	50.8
Personal data protection is affected due to cyber terrorism.	7.6	10.8	5.2	24.2	52.2
Public finance is at higher risk due to cyber terrorism.	14	12	10	28	36
Lack of proper implementation of laws increases cyber terrorism.	8.6	7.6	7	22.8	54

Immediate steps are highly needed to combat cyber terrorism.	8.4	12.8	10.8	18.6	49.4
--	-----	------	------	------	------

Across all the ten statements, post-intervention mean scores were consistently higher than pre-intervention scores. This indicates that an increased awareness and perceived severity of cyber terrorism after the informational intervention has been provided to respondents.

59

SUBODH NEXUS VOLUME V ISSUE I, JUNE 26' ISSN No: 3048-5371

Pre-intervention survey results indicated moderate awareness among respondents regarding cyber terrorism as a national and societal threat (Mean range: 2.98-3.38). Following the awareness intervention, post-intervention mean scores increased significantly across all statements (Mean range: 3.60-4.06). Paired-sample t-test results confirmed that the increase in perception scores was statistically significant for all items ($p < 0.001$). This suggests that increased awareness substantially altered public perception regarding national security threats which was caused by cyber terrorism, data privacy risks due to cyber-attacks, disruption of critical infrastructure which majorly affect the country, financial vulnerability faced by people due to cyber terrorism and urgency of legal and policy responses to counter cyber terror attacks.

Analysis Result for Pre and Post Intervention for Each Statement¹⁴

Statements	Pre-Mean	Pre-SD	Post-Mean	Post SD	Mean Difference
S1	3.02	1.39	4.05	1.35	1.02
S2	3.02	1.40	3.80	1.39	0.78
S3	3.12	1.47	3.95	1.38	0.83
S4	2.98	1.44	3.76	1.33	0.78
S5	3.24	1.57	3.86	1.30	0.62
S6	3.32	1.57	4.02	1.27	0.70
S7	3.23	1.58	4.03	1.30	0.80
S8	3.21	1.58	3.60	1.43	0.39
S9	3.25	1.52	4.06	1.30	0.81

S10	3.38	1.49	3.88	1.36	0.50
------------	------	------	------	------	------

The quantitative findings demonstrate that public perception of cyber terrorism is significantly shaped by awareness and exposure to information on cyber terrorism. Prior to intervention,

¹⁴In the table S1 to S10 refers to all the statements on which data has been collected. Pre-Mean refers to pre-intervention mean whereas Post-Mean refers to post-intervention calculated mean. Pre-SD refers to standard deviation of pre intervention and Post-SD refers to standard deviation of post intervention data.

60

SUBODH NEXUS VOLUME V ISSUE I, JUNE 26' ISSN No: 3048-5371

respondents exhibited moderate concern on cyber terrorism, however, post-intervention responses reflect a wide understanding on cyber terrorism as a serious national, economic and psychological threat on people. The statistically significant across all dimensions confirms the study's hypothesis that through intervention, awareness is provided to individuals to play a crucial role in shaping societal perception and resilience against cyber terrorism.

FINDINGS OF HYPOTHESES TESTING

To assess the magnitude of the intervention's impact on respondents, Cohen's d was calculated using the mean difference divided by the pooled standard deviation. For small effect ($d \approx 0.2$), medium effect ($d \approx 0.5$) and large effect $d \geq 0.8$ has been taken. Across all the ten statements, effect sizes ranged from moderate to large, indicating that the intervention had substantively impacted the perception of people. This demonstrates that awareness intervention substantially enhances public understanding of cyber terrorism. The results confirm that awareness intervention significantly increases public perception of cyber terrorism as a serious threat to national security and societal stability. This proves the first hypothesis.

To examine the psychological, financial and privacy-related impacts of cyber terrorism on society, statements related to personal safety, data privacy and public finance (S3, S4, S7, S8) showed a significant increase in post-intervention mean scores, with effect sizes ranging from moderate to large. This indicates more awareness has increased psychological fear and insecurity, anticipating risk of personal data leakage and increased financial risks associated with cyber terror attacks. The findings align with expert opinions that cyber terrorism aligns with expert opinions that cyber terrorism creates long-term psychological distress and behavioural changes,

such as reluctance to engage with digital platforms. This confirms the second hypothesis that cyber terrorism significantly impacts psychological security, data privacy perceptions and financial trust among the public.

To assess the impact of cyber terrorism on critical national infrastructure, statements concerning disruption of critical infrastructure and national stability (S2, S6) recorded some of the highest post intervention mean scores (Mean>4.0). Respondents increasingly perceived cyber terrorism capable of causing systematic disruption to essential services such as banking, transportation, healthcare and governance platforms. Compared to traditional terrorism, cyber terrorism was perceived as more pervasive, less detectable and capable of causing prolonged disruption without

physical violence on the crucial national infrastructure and as a result widely impacts the society. This confirms the third hypothesis that cyber terrorism is perceived to have a broader and more sustained impact on critical national infrastructure compared to traditional terrorist attacks.

To analyse the role of legal and institutional frameworks in controlling cyber terrorism specifically intervention impact on the ninth statement has been analysed. S9 demonstrated a substantial increase in agreement on lack of proper implementation of cyber terrorism, when a post-intervention survey is done with Mean difference calculated as 0.81. This quantitative finding is strongly reinforced by qualitative data, where experts consistently identified gaps in international cyber law, jurisdictional ambiguity in cyber terrorism cases and lack of effective enforcement of cyber terror laws. This confirms the fourth hypothesis that perceived inadequacy in legal and institutional frameworks significantly contributes to the persistence of cyber terrorism.

To assess public demand for policy reform and immediate counter measures for controlling cyber terrorism responses for statement S10 (Immediate steps are highly needed to combat cyber terrorism) was recorded and analysed. It has been seen that there is significant rise in post-intervention agreement, reflecting increased public demand for proactive legal and policy measures for combatting cyber terrorism. The results indicate that increased awareness directly influences public expectations regarding enactment of strict cyber laws with stronger enforcement and a more enhanced national cyber resilience strategy that can address the emerging challenges created by incorporation of advanced technologies in cyber terror attacks.

The change in post-intervention responses confirms the last hypothesis that awareness and information dissemination significantly influence public demand for immediate policy and legal intervention.

FINDINGS OF THE THEMATIC ANALYSIS FOR SEMI-STRUCTURE INTERVIEWS CONDUCTED WITH EXPERTS

After identifying with the above paired sample t-test that cyber terrorism hugely impacts the people. The qualitative data has been collected mainly through legal and cyber experts to identify legal and systematic challenges and explore policy measures for strengthening reforms in India. For this semi-structure interview has been done with 30 legal professionals and 30 cyber experts. While interviewing with top officials, basically two main questions have been asked:

62

SUBODH NEXUS VOLUME V ISSUE I, JUNE 26' ISSN No: 3048-5371

- What are the legal and systematic challenges they identify which actually causes cyber terrorism?
- Which reforms would they recommend for controlling cyber terrorism?

This section presents the findings from the interview conducted with legal professionals and cyber security experts, focusing on the expert's views on the legal and systematic challenges that increase the threats of cyber terrorism. Through their vast experience in the field they have suggested different strategies to mitigate them. The analysis has provided three principal themes, with numerous sub-themes, that are discussed below:

Theme 1: Gaps in International law – Lack of Enforcement

The most dominant theme identified across all expert interviews was the presence of gaps in existing international law and domestic statutes. This theme directly relates to the lack of clear legal authority to investigate, prosecute or enforce judgments across borders. Cyberterrorism is a transnational crime, but unfortunately there is no single legal framework to address cross border cyber-crimes. This makes it difficult to determine which country has jurisdiction to decide these cases. Existing traditional laws are not sufficient in countering major issues related with cyber terrorism. There is no universally recognised law that has to be followed across all the nations, as a result transnational cyber-terrorist organisations are increasing day-by-day. Two sub-themes emerge from this theme:

- **First sub-theme: Jurisdictional Ambiguity in Cross-Border Cyber Terrorism** Experts emphasised that cyber terrorist activities often originate in one country, are executed through servers in another country and target victims in multiple jurisdictions. The multi-layered structure creates ambiguity regarding jurisdiction, leading to delays in investigation and prosecution of cyber terrorism cases. Though there are various Mutual Legal Assistance Treaties (MLATs), they are time consuming and ineffective in addressing Fast-paced cyber terrorist attacks. Experts have highlighted that the absence of a real-time cross-border cooperation system allows cyber terrorists to exploit legal loopholes and evade accountability.
- **Second sub-theme: Inadequacy of existing domestic cyber laws-** Legal experts pointed out that many domestic cyber laws were drafted to address conventional cybercrimes rather than ideologically motivated cyber terrorism. In India, although Section 66F of the

63

SUBODH NEXUS VOLUME V ISSUE I, JUNE 26' ISSN No: 3048-5371

Information Technology Act, 2000 addresses cyber terrorism, enforcement remains weak due to lack of technical expertise, procedural delays and evidentiary challenges. Experts stressed that existing laws fail to adequately address emerging threats such as AI-driven attacks, deep-fake based misinformation campaigns and cyber warfare targeting critical national infrastructure.

Theme 2: Weak Institutional Capacity and Technical Expertise

The next theme identified by the experts was lack of adequate institutional capacity to combat cyber terrorism effectively. This is due to the significant barrier to national and international security is the weak institutional capacity and the lack of technical expertise required to combat cyber terrorism. Many governing bodies and law enforcement agencies operate with fragmented frameworks and insufficient funding, leading to a “governance gap” where digital threats outpace bureaucratic response times. This issue is compounded by a global shortage of cyber security professionals, making it difficult for institutions to attract and retain the high-level talent needed for complex cases like forensic attribution and the protection of critical information infrastructure. Lacking robust organizational structures and a work force trained in advanced technical defense, states remain reactive rather than proactive in countering cyber terrorism cases, leaving essential services such as power grids, financial networks and health care systems

vulnerable to increasingly cyber terror attacks. It has two sub-themes:

- **First Sub-theme: Shortage of skilled cybersecurity professionals-** Cyber experts highlighted that law enforcement agencies face an acute shortage of trained cybersecurity professionals capable of handling sophisticated cyber terrorist attacks. Rapid technological advancements have outpaced the skill development of investigative agencies, making it difficult to track, attribute and neutralise cyber threats in real time.
- **Second Sub-theme: Fragmented Coordination among Agencies-** Moreover, experts have also stressed that multiple agencies are involved in cyber security and counter-terrorism efforts, but coordination among them remains fragmented. Lack of clarity about jurisdictions in the international level cyber terrorism cases, inadequate data sharing mechanisms and absence of a unified command structure weaken India's overall cyber defense system. This institutional fragmentation results in delayed responses during major cyber terror attacks.

Theme 3: Low Public Awareness and Psychological Impact of Cyber Terrorism

The third theme focused on societal vulnerabilities that indirectly strengthen cyber terrorism. Low public awareness of cyber terrorism significantly contributes to societal vulnerability, as many individuals and organisations lack a clear understanding of the nature, methods and potential consequences of cyber-based attacks. Unlike conventional terrorism, cyber terrorism often operates invisibly, targeting digital infrastructure, information systems and online platforms without any physical damage. This invisibility leads to underestimation of the threat, weak cyber security practices and delayed responses during attacks. Limited digital literacy, inadequate knowledge about cyber laws among public and insufficient media focus further exacerbate this issue, allowing cyber terrorists to exploit human error, misinformation and systematic unpreparedness to achieve their objectives with minimal resistance.

Beyond technical damage, cyber terrorism exerts a profound psychological impact on society by instilling fear, uncertainty and a sense of loss of control among the public. Disruptions by essential services, data breaches and online propaganda campaigns can erode public trust in government institutions and digital systems. Even minor cyber incidents can trigger widespread

panic among citizens. This psychological dimension amplifies the effectiveness of cyber terrorism as fear and anxiety can spread faster than the attack itself, influencing public behaviour, social cohesion and national stability. As a result, addressing cyber terrorism requires not only technological defenses but also increased public awareness and psychological resilience. Two sub-themes highlighted by experts are:

- **First Sub theme: Low cyber knowledge among citizens-** Both legal and cyber experts have agreed that low level of cyber literacy among the general public significantly contribute to the success of cyber terrorist activities such as phishing, ransomware, hacking etc. Lack of awareness makes individuals easy targets, amplifying the reach and impact of cyber terrorism.
- **Second Sub-theme: Psychological Fear and Loss of the public trust-** Experts have also highlighted that repeated cyber incidents erode public trust in government institutions, digital governance platforms and financial systems. Psychological distress, fear of surveillance and reluctance to adopt digital services were identified as long-term consequences faced by society.

RESULTS AND DISCUSSION

This section presents and discusses the qualitative and quantitative findings of the study in relation to the stated research objectives and hypotheses. A mixed-method approach enabled a comprehensive understanding of public perception and the broader impact of cyber terrorism in India. The quantitative analysis revealed that there is significant increase in public perception of cyber terrorism as a serious threat to society in specific and nation at large following the awareness given to the respondents through intervention, Pre-intervention mean scores across all ten statements ranged from 2.98-3.38 indicating moderate awareness. Post-intervention mean scores increased substantially, ranging from 3.60-4.06. The findings of Paired-samples t-test results confirmed that structured awareness interventions play a critical role in shaping public understanding of cyber terrorism.

Respondents increasingly acknowledged that cyber terrorism creates psychological fear on the safety of personal data. These findings reveal that cyber terrorism creates deep psychological and

behavioural consequences. Unlike traditional terrorism which generates immediate physical fear, cyber terrorism creates sustained anxiety due to the use of advanced technologies in doing online crimes. The qualitative interviews further reinforced this interpretation, with experts emphasising that victims often experience stress, mistrust in digital platforms and reluctance to engage in online financial or governmental services. This convergence of qualitative and quantitative analysis confirms that cyber terrorism significantly impacts mental well-being and societal trust.

One of the most significant findings relates to the perceived impact of cyber terrorism on critical national infrastructure. In this post-intervention scores for statements addressing infrastructure disruption and national stability exceeded 4.0, reflecting strong agreement among respondents. Participants increasingly recognised that cyber terrorism can disrupt essential services such as banking systems, health care networks, transportation infrastructure and government digital platforms. Unlike traditional terrorist attacks, cyber-attacks can cause system-wide paralysis without physical destruction, often affecting multiple sectors simultaneously. From a comparative perspective, the findings suggest that cyber terrorism perceived as having a broader, more persistent and less predictable impact than conventional terrorism. Hence, it confirms that cyber terrorism poses a complex threat to national security, specifically in highly digitalized societies like India.

The study also examined perceptions regarding the adequacy of legal and institutional responses to cyber terrorism. A substantial post-intervention increase in agreement was observed for the statement asserting that lack of proper implementation of laws contributes to the growth of cyber terrorism. This qualitative result is strongly corroborated by the thematic analysis of expert interviews. Legal and cyber experts consistently identified that jurisdictional ambiguity in cross border cybercrimes, absence of a unified international legal framework and limited technical expertise among enforcement agencies. The discussion reveals that while India has enacted laws such as the Information Technology Act, 2000, enforcement challenges and outdated provisions reduce their effectiveness against evolving cyber terrorist techniques. The findings underscore the need for dynamic legal reform and institutional capacity building, rather than reliance on static legal instruments.

Further, this research focused on public demand for proactive counter cyber terrorism measures.

Post-intervention data showed a strong increase in agreement that immediate steps are necessary to combat cyber terrorism. This finding suggests a direct relationship between awareness and policy expectation. As individuals become more informed about cyber terrorism, their demand for government accountability, stronger cyber laws and increased institutional preparedness. This result emphasises the importance of transparent communication and public engagement in national cyber security strategies. Public support is essential for the successful implementation of strict cyber regulation and surveillance mechanisms.

Taken together, the results indicate that cyber terrorism is not merely a technological challenge but a multi-dimensional social threat affecting psychological security, economic stability, public trust and national resilience. The findings demonstrate that awareness on threat created due to increase in cyber terrorism alters the public perceptions. Cyber terrorism generates a long-term psychological fear. Moreover, critical infrastructure is highly vulnerable due to the increase in cyber terrorism. Legal and institutional inadequacies further contribute to persistence of cyber terrorism. Increased awareness leads to stronger public demand for immediate policy reforms. The integration of quantitative and qualitative findings strengthens the validity of the study and highlights the necessity of a holistic approach combining legal reform, institutional coordination, technological innovation and public education to effectively counter cyber terrorism.

RECOMMENDATIONS

67

SUBODH NEXUS VOLUME V ISSUE I, JUNE 26' ISSN No: 3048-5371

Based on multi-faceted research into public perception, policy response and legal challenges of cyber terrorism following recommendations can be made:

- The capacity of judicial and law enforcement authorities should be enhanced by establishing dedicated courts or judicial benches who have mandatory and continuous training specifically in interpreting technical evidence which are presented against cyber terrorism. This will help in deciding the cyber terrorism cases.
- India should amend the Information Technology Act, 2000 to explicitly address emerging forms of cyber terrorism, including AI- driven cyber-attacks and attacks on critical infrastructure. Clear procedural guidelines for investigation and prosecution of cyber terrorism should be introduced and enforced strictly.

- There is an urgent need for a comprehensive international convention on cyber terrorism that establishes common definitions, jurisdictional clarity and enforcement mechanisms so that cyber terrorism can be countered successfully. Global cyber governance has to be properly shaped and monitored by collective efforts so that cyber terrorism can be controlled.
- There is also a need for dedicated cyber terrorism courts or specialised judicial benches should be established with judges specifically trained in cyber forensics and digital evidence analysis. This will ensure timely and effective adjudication of cyber terrorism cases.
- Continuous training programs should be conducted for law enforcement agencies, prosecutors and judges to keep pace with evolving cyber threats at global level. By recruiting more cyber security experts within police and other law investigation and enforcement agencies has to be prioritised.
- A unified cyber command structure should be created to improve coordination among CERT-IN, NCCC, I4C, intelligence agencies and law enforcement bodies. This will strengthen the collaboration among agencies.
- Large-scale cyber awareness initiatives should be launched to educate citizens about cybercrimes such as phishing, ransomware and data protection laws and practices that can be adopted by them. Moreover, educational institutions should integrate cyber security education in their curriculum.

- Government policies should include psychological counseling, financial compensation and legal assistance to the victims of cyber terrorism. This helps in restoring the trust and resilience of the public in the system.

CONCLUSION

Cyber terrorism has emerged as one of the most complex and dangerous threats to modern societies due to its international threat created across borders, low operational cost and high impact on critical infrastructure and psychological impact it has on the public. This research has demonstrated that cyber terrorism significantly affects national security, economic stability,

public trust and individual well-being. The quantitative findings clearly indicate a substantial shift in public perception after awareness intervention, highlighting the importance of education and informed discourse.

The qualitative insights further reveal deep structural and legal gaps that allow cyber terrorism to flourish, particularly in the absence of effective international mechanisms and institutional preparedness. While India has taken commendable steps through agencies like CERT-In, NCCC and I4C, the rapidly evolving cyber threat landscape demands stronger legal reforms, global cooperation and integrated policy responses.

Hence, we can conclude that combating cyber terrorism requires a holistic approach that goes beyond technical defenses. Legal reforms, institutional capacity building, international collaboration, public awareness and psychological resilience must collectively shape future counter cyber terrorism strategies. Only through such comprehensive efforts can societies ensure digital peace, national security and sustainable trust in law enforcement agencies that they can successfully counter cyber terrorism.