A COMPARATIVE STUDY OF CYBERTERRORISM LAWS IN INDIA WITH THE UNITED STATES OF AMERICA AND THE EUROPEAN UNION

* Ms. Ritupriya Gurtoo [1] **Dr. Ankita Nirwani [2]

SVKM'S NMIMS, INDORE

ABSTRACT

Cyberterrorism conjures images of ruthless terrorists unleashing devastating attacks on computer networks, wreaking havoc and paralyzing nations. This terrifying scenario has the possibility of being a reality in the future. From a psychological standpoint, the term "cyberterrorism" combines two of the greatest modern-day fears. Fear of random, violent victimization blends well with skepticism and outright fear of computer technology. Terrorists could bring down a country's critical military, financial, and service computer systems, resulting in an economic meltdown. Cyberterrorism is a modern age viable option for terrorist groups seeking to achieve their objectives. While bombing physical targets may draw unwelcome attention and raise the stakes of failure of a terrorist group, Cyberterrorist attacks can be more precisely and easily orchestrated, and the perpetrators are less detectable due to their remote location. Furthermore, cyberterrorism is a far more pressing concern for the government than physical threats, since computers are at the heart of any nation's infrastructure, performing critical functions such as storing vital information and controlling power delivery, communications, aviation, and financial services.

This paper examines the insight into the cyberterrorism-related laws passed by the legislature in India, the United States of America (USA), and the European Union (EU). It shall also deal with the laxity of the approach of the government despite cyberterrorism being a major concern. An analysis shall be done on the loopholes in the existing system of law. The researcher shall also recommend the myriad ways that the government can adopt to combat the threat of cyberterrorism.

KEYWORDS: Cyber Security, Critical Infrastructure, Cyberterrorism, Non- State Actors, and Legislative Means.

[1] Ms. Ritupriya Gurtoo, Assistant Professor, School of Law, Narsee Monjee Institute of Management Studies, Indore

[2] Dr. Ankita Nirwani, Head of Department (Law), Oriental University, Indore

The Twenty-First century has seen a massive increase in the use of technology and the internet, leading to the "Cyber Revolution." The relevance of a cyber revolution in today's world cannot be overstated. It encompasses a wide range of factors that impact individuals, societies, economies, and governments. A cyber revolution encourages the development and adoption of emerging technologies like Artificial Intelligence, Blockchain technology, etc. These technologies have the potential to reshape industries, improve efficiency, and drive innovation across various sectors. The cyber revolution has had a profound impact on the world, and its effects will continue to be felt for many years to come. It has opened up new opportunities for innovation and collaboration, but it has also brought with it new challenges and risks that we must address as a society.

As digital technologies advance, so do the tactics and techniques used by cybercriminals. Sophisticated cyberattacks, including hacking, ransomware, and phishing, can lead to data breaches, financial losses, and disruptions to critical infrastructure. The risks that organizations confront while storing data in cyberspace have created a completely new global battlefield.[3] Cyberspace has emerged as a new battleground, with a plethora of adversaries. Foreign governments, international terrorist organizations, and organized criminals target individuals, businesses, and governments on a regular basis.[4] As a result of crucial information being held in cyberspace, the number of possible adversaries like cybercrimes to the States has increased substantially. Cyberattacks, unlike traditional combat operations, do not require advanced weaponry to carry out their battle. It is available to individuals at the click of a button with minimum resources. The challenge lies in developing advanced cybersecurity measures and robust data protection frameworks to counteract the growing threat of cyberattacks and data breaches.

CYBERTERRORISM: A VIRTUAL MYTH OR AN IMPENDING APOCALYPSE

One of the cybercrimes that has gained prominence over the recent years has been Cyberterrorism. Since the concept of cyberterrorism is relatively new, a commonly accepted definition does not exist. Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California, coined the term ‘cyberterrorism’ in the 1980s. The concept is

[3] 161 Cong. Rec. H2426 (daily ed. April 23, 2015) (statement of Rep. Loudermilk), https://www.congress.gov/amendment/ 114th-congress/house-amendment/99/text. Last accessed on July 20 2022
[4] ibid

composed of two elements: cyberspace and terrorism.[5] Cyberspace can be defined as "*that place where computer programs run and data moves*".[6] According to him, Terrorism is a more difficult concept to define. Terrorism is defined as *"premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually with the intention of influencing an audience.[7]"* Combining these definitions yields a working definition of cyberterrorism as premeditated, politically motivated attacks against information, computer systems, computer programs, and data by subnational groups or clandestine operatives that result in violence against non-combatant targets.

In the nascent stage, cyberterrorism can be defined as *"the calculated use of unlawful violence against tangible property to intimidate or coerce governments or societies in the pursuit of goals that are political, religious or ideological"*. One of the comprehensive definitions of cyberterrorism given way back in the early 2000s was the convergence of terrorism and cyberspace. It is generally understood as an unlawful attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives which should result in violence against persons or property, or at least cause enough harm to generate fear.[8]

Furthermore, Cyberterrorism involves the use of computer viruses, hacking, and other forms of cyber-attacks to cause harm to individuals, and organizations and thereby destabilize the government.[9] One must understand the basic elements of cyberterrorism consist of cybercriminals, Cyberspace, usage of cyber methods, and Cyber Arsenal, Targets, such as government agencies, businesses, locations, people, or digital infrastructure, and motivation which can either be religious, communal, or vindictive

The goals of cyberterrorism may vary, but they often involve causing disruption, damage, or fear among the citizens to achieve political or ideological objectives. Examples of cyberterrorism could include attacks on critical infrastructure, such as power grids or water supplies, or the theft of sensitive information such as financial data or government secrets. It also includes the use of social media and other online platforms to spread propaganda or to

[5] D. E. Denning, "Cyberterrorism Testimony before the Special Oversight Panel on Terrorism," Georgetown University, Georgetown, 2000.
[6] Collin, B. (1996) The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge. Paper presented at the 11th Annual International Symposium on Criminal Justice Issues, University of Illinois at Chicago.
[7] M. M. Pollitt, "Cyberterrorism: Fact or Fancy?," Computer Fraud & Security, pp. 8-10, 1998.
[8] Emery, N. E. (2005). The Myth of Cyberterrorism. *Journal of Information Warfare*, *4*(1), 80–89
[9] Gabriel Weimann, "Cyberterrorism: The Sum of All Fears?" Studies in Conflict and Terrorism, Vol. 28, No. 2, 2005, p. 131

recruit new members to a terrorist group.[10] Critical Infrastructure connotes a denial of services of national and economic importance like telecommunications networks, military command systems, and financial transactions or even collapsing the stock exchange[11] are some of the methods to conduct cyberterrorism to make a political statement, by terrorist groups, and thereby inflict psychological and physical damage on the state.[12]

Cyberterrorism slowly impacts an economy or has limited or isolated success on critical infrastructure, but they have the same dramatic effect as an explosion, but a lesser psychological effect. In other words, in cyberterrorism, terrorists commit crimes against nations through technology to destroy the framework and foundation which either causes injury or death of people or undermines economies and organizations. Cyberterrorism is a criminal act executed by the use of computers and telecommunication capabilities bringing about viciousness, destruction, and/or disruption of services to create fear within a given population to influence a government or population to conform to a specific political, social, or ideological agenda.[13]

However, not all cyber-attacks come under the ambit of cyberterrorism. Cyberterrorism is specifically aimed at weakening the economy and thereby paralyzing the government, whereas other cyber-attacks may have different objectives such as financial gain or espionage. Cyberterrorism differs from Cyber-attack in many aspects. Myriad cyber incidents are erroneously attributed to cyber terrorism, which has "become a 'catch all' term that can be pulled from the 'trick bag' to fit any number of scenarios or purposes" [14] Often these incidents are simply criminal. They create frustration, economic losses, and perhaps panic, but not terror. And when the acts lack political motivation and the intent to persuade, then they are not within the ambit of cyberterrorism.[15]

By extrapolating some of the most widely used definitions of cyberterrorism, it is evident that an act must take place in cyberspace and involve the use of a computer system in order to be classified as cyberterrorism. The target computer system or any data it may contain must also be the target of the attack. The act of cyberterrorism is carried out by a cyberterrorist using a

[10] Maura Conway, "What Is Cyberterrorism?" Current History, Vol. 101, No. 659, December 2002; Weimann.
[11] Nehla Hani, M., & Rajan, A. (2018). A Critical Study on Cyber Terrorism with Reference with 26/11 Mumbai Attack. International Journal of Pure and Applied Mathematics, 19(17), 1617–1636.
[12] ibid
[13] Pujari, A. (2016). Cyber Terrorism. World Wide Weponisation! TN Police Sesquicentennial Anniversary Souvenir.
[14] N. E. Emery, "The Myth of Cyberterrorism" Journal of Information Warfare , Vol. 4, No. 1 (2005), pp. 80-89
[15] Collin, B. (1997) The Future of Cyberterrorism, Crime and Justice International.

computer that can be considered a weapon, and it must be intended to incite fear through acts of violence or injury to people or property, as well as having political, religious, or ideological motivations.[16]

The question as to whether cyberterrorism is a myth or a reality is debatable. Cyber security experts believe it is virtually impossible to use the Internet to inflict death on a large scale.[17] Some argue that terrorists can sit at one computer connected to one network and can create worldwide havoc without the need of a bomb or explosives in order to cripple the critical infrastructure of the state.[18] The cyberterrorism threat is real and rapidly expanding and the cyber-terrorist is either politically or religiously motivated in order to create fear and alarm within a given population through disruption or destruction of critical national infrastructure. It is apparent that like conventional terrorism, cyberterrorism is a controversial subject with some believing that it can only be considered cyberterrorism if there is some form of loss of life or damage to property. Whilst cyberterrorism may do this indirectly the stumbling block in a cyberterrorist attack appears to be whether it is even possible to achieve terrorism through the use of computer technologies.[19]

In this research paper, the researcher shall focus on the threat of Cyberterrorism to the United States of America, the European Union, and India. Cyberterrorists are using technology to attack a country's economy by invading computer systems and networks and causing disruption. For example, in the United States (U.S.) and the European Union, government agencies and critical infrastructure are the primary targets of cyberterrorism. These attacks can have significant consequences, including the loss of sensitive information, financial losses, and even threats to national security. The United States has seen several high-profile cyberterrorism attacks in recent years. In India, cyber terrorism has been on the rise in recent years, with attacks targeting government agencies, financial institutions, and critical infrastructure. The wide use of the internet in India for administration and communication made cyberterrorism possible without much expense. At present Cyber attackers are highly motivated, well-funded, and technically advanced. Their attacks posed a threat to initiatives of nations like India such as Smart Cities, E-Governance, etc. Government and military organizations and other businesses use cyberspace to store and process significant volumes of confidential data. One of the biggest

[16] A. Jones, "Cyberterrorism: fact or Fiction," Computer Fraud & Security, vol. 6, pp. 4-7, 2005.
[17] J. Green, "The Myth of Cyberterrorism," Washington Monthly, Washington, 2002.
[18] G. Weimann, "Cyberterrorism, How Real Is the Threat?," United States Institute of Peace, Washington DC, 2004.
[19] A. Jones, "Cyberterrorism: fact or Fiction," Computer Fraud & Security, vol. 6, pp. 4-7, 2005.

challenges faced by the state in countering cyberterrorism under cyberspace is balancing Fundamental Rights in the name of Freedom of Speech, Security, and Privacy laws.[20]

Overall, the threat of cyberterrorism is a significant concern for governments, businesses, and individuals worldwide, and measures need to be taken to strengthen cybersecurity and prevent these attacks from happening. This includes investing in cybersecurity technology and training, sharing threat intelligence, and developing international agreements and protocols to address cyberterrorism

OBJECTIVES OF THE RESEARCH PAPER

1. To identify the existing statutory provisions to counter cyberterrorism in India, The United States of America, and the European Union
2. To examine the role of the governments of India, The United States of America, and the European Union to protect their critical infrastructure from Cyberterrorism.
3. To recommend strategies and policies to be implemented as cyber security measures by the State actors to combat Cyberterrorism

METHODOLOGY

The Methodology used in this research paper is the Doctrinal Method. The paper is a descriptive analysis of the existing statutory provisions in India, the United States of America, and the European Union. The secondary data on cyberterrorism had been collected from authentic sources. The data used here has been collected from different books, articles, magazines, journals, and legislation.

IMPACT OF CYBERTERRORISM ON NATIONAL SECURITY OF THE STATE

Cyberterrorism can have a significant impact on the economies of the world in several ways thereby compromising national security. At the outset, it can cause financial losses to individuals, businesses, and governments. This in turn can lead to theft of funds, disruption of financial systems, and the loss of intellectual property. These losses can have a significant impact on the economy. Critical infrastructure such as power grids, water supply systems, and transportation networks, if targeted through cyberterrorism can have a significant impact on the economy by causing widespread disruption to business operations and transportation.

[20] Christou, G. (2019)'The Collective Securitisation of Cyberspace in the European Union'. West European Politics, Vol. 42, No. 2

One of the potential impacts of cyberterrorism is it reduces investor confidence, resulting in a drop in the stock price of the company. This can lead to a chain reaction of effects on the economy. More than anything else, these types of terrorist activities via computer damage the reputation of government at world forums. This can result in decreased consumer confidence and reduced demand for goods and services, thereby impacting the economy. Overall, the impact of cyberterrorism on the economy can be significant and far-reaching. It is important for governments and businesses to invest in cybersecurity measures to minimize the risk of cyberterrorism and to prepare for the potential economic impact of such attacks.

DECODING CYBERTERRORISM ATTACKS THROUGH THE LENS OF RECENT EVENTS

There have been several instances of cyberterrorism in recent years. These cases demonstrate the various forms that cyberterrorism can take, from state-sponsored espionage to criminal activity such as ransomware attacks.[21] They have also paved the way to the development of new cybersecurity measures and legislation to better protect against cyberterrorism. In 2020, a cyber-attack on the power grid in Mumbai caused a blackout in parts of the city. The attack was carried out by a group of hackers who targeted a specific piece of software used by the power company. In 2021, several high-profile social media accounts, including those of the Indian National Congress party and the journalist Ravish Kumar, were hacked. The hackers posted messages in support of Pakistan and against India.

WannaCry was a ransomware attack that affected over 200,000 computers in 150 countries. The attack highlighted the vulnerability of computer systems to ransomware and the importance of cybersecurity measures. The Sony Pictures hack was a cyber-attack on Sony Pictures Entertainment by a group of hackers calling themselves the "Guardians of Peace." The group stole and released confidential data and caused significant disruption to the company's operations. Stuxnet was a computer worm that targeted Iran's nuclear program. The worm was designed to cause physical damage to centrifuges used in the program, and it was the first

[21] Conway; Dorothy E. Denning, “Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy,” in John Arquilla and David Ronfeldt, eds., Networks and Netwars, Santa Monica, CA: RAND, 2001, pp. 239-288, Dorothy Denning, “Stuxnet: What Has Changed?” Future Internet, Vol. 4, 2012; Michael Stohl, “Cyber terrorism: a clear and present danger, the sum of all fears, breaking point, or patriot games?” Crime, Law and Social Change Vol. 46, No. 4, 2006, pp. 223-238; Weimann.

known example of a cyber-attack with physical consequences attack was attributed to Chinese hackers and highlighted the risks of state-sponsored cyberterrorism.[22]

The threat of a cyber-attack on India has been continually raised by the Central Bureau of Investigation (CBI), India, and cyber specialists. In 2010, the CBI website was also compromised by the "Pakistani Cyber Army" hackers. Dr. Abdul Kalam, the former president of India, raised concerns in his 2005 talk on cyberterrorism. Instead, the "Cyber security system" is not a field in which India is yet an expert. It should be viewed as a significant loss for India. Companies, governmental and private institutions, as well as the financial and insurance sectors, in India, spend less and are less concerned with cyber security. Indira Gandhi International Airport (IGI) was the target of a cyberattack in August 2013. 'Technical Snag', a damaging viral software, disrupted the operations of Terminal number 3. This malicious software was disseminated remotely in order to breach "the airport security system." Attackers on the internet tried to exploit security system flaws. They used the CUPPS (Common Use Passengers Processing System) to transfer the virus program from 'check-in centres' at boarding gates to the system's operation in the end, which has an impact on the airlines' online reservation system, anticipated departure time, and waiting room capacity.[23] The investigation into the 26/11 Mumbai attack uncovered evidence of terrorists' use of cyberspace to communicate and gain access to information such as maps, demographic statistics, and local infrastructure. They employ "Google Earth" to carry out their strategy, a mobile network for command and control, and social media to monitor the movement of Indian defense and rescue forces. Additionally, they employ technology for the "conversion of audio signals into data," which rendered it hard for "Indian defense forces" to trace the source of Information.[24]

COMBATING CYBERTERRORISM THROUGH LAWS AS INCORPORATED IN THE LEGISLATION

I. EUROPEAN UNION

European Union (EU) countries have their own national laws that address cyberterrorism. For example, in the United Kingdom when it used to be a part of the European Union, the Computer

[22] Teixeira A., Kupzog F., Sandberg H., Johansson K.H. (2015) *Smart Grid Security: Innovative Solutions for a Modernized Grid*, , pp. 149-183.

[23] Cyber terrorism and the reality of threat, Available at https://www.aspistrategist.org.au Last accessed on June 12, 2019

[24] Cyber terrorism: The Fifth Domain, available at: http://www.indiabloom.com Last accessed on March 13, 2019

Misuse Act 1990 criminalizes unauthorized access to computer systems with the intention to commit or facilitate further offenses, including cyberterrorism. Similarly, in France, the Criminal Code includes provisions that criminalize cyberterrorism and cyber espionage. While there is no one specific law that addresses cyberterrorism in Europe, there are several EU-wide laws and national laws that address the issue. These laws provide a framework for international cooperation, establish cybersecurity certification standards, require member states to ensure the security of their critical infrastructure, and criminalize cyberterrorism and other forms of cybercrime. Cyberterrorism laws in Europe vary from country to country, however there are several key EU-wide laws that address the issue.

The Convention on Cybercrime, also known as the Budapest Convention, is an international treaty that addresses various forms of cybercrime, including cyberterrorism. In 2001, the Council of Europe organized the Convention on Cybercrime, the first international treaty78 addressing Internet and computer crime, which was enforced in July 2004[25]. The treaty sought to "harmonize national laws," and coordinate with law enforcement agencies so as to align with their objectives.[26] It focused on some of the most widespread and problematic Internet crimes: copyright infringement, fraud, child pornography, hate crimes, and financial crime. The treaty has been signed by most EU countries and provides a framework for international cooperation in the investigation and prosecution of cybercrimes.

Furthermore, The EU Cybersecurity Act, adopted in 2019, establishes a European cybersecurity certification framework to increase trust in digital products and services. The Act also establishes a European Cybersecurity Agency to help member states in cybersecurity matters. In addition, The Network and Information Security (NIS) Directive is an EU-wide law that requires member states to adopt measures to ensure the security of their critical infrastructure. The directive requires member states to establish national cybersecurity strategies, designate national cybersecurity authorities, and establish incident response teams.

The European Union has created both strategic and operational initiatives. Beginning in 2004, the European Council agreed on a five-year plan called the Hague Programme to be developed in the areas of freedom, security, and justice. One of the primary areas for analysis and action was the fight against terrorism and that included indirect references to cyber terrorism. In 2005 the European Union Presidency and the Counter-Terrorism Coordinator presented the

[25] Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185, *available at* http://conventions.coe.int/Treaty/en/Freaties/html/185.htm. (Last accessed on July 02, 2022)
[26] United Nations Office on Drugs and Crime, The Use Of Internet For Terrorist Purpose 3 (2012)

European Union Council with a comprehensive strategy to prevent, protect, pursue, and respond to any cyberterrorism activities.[27] As of now apart from the Hague Programme; community policing and effective monitoring of the Internet are also prioritized as an integrated strategy.

II. UNITED STATES OF AMERICA

America is at Risk was declared by the National Academy of Sciences in 1990 at the outset of a report on computer security. America is becoming more and more reliant on computers, and a terrorist of the future could be able to cause more destruction with a keyboard than with a bomb. The term "electronic Pearl Harbor" was developed at the same time, connecting the prospect of a computer attack to a tragic period in American history.

According to research published in December 2003 (and covered by the Washington Post on January 31, 2004), the government's capacity to defend itself against cyberattacks was doubted by IT specialists.[28] The assessment, carried out over the course of a year by the House Government Reform Subcommittee on Technology, evaluated computer security in federal agencies and assigned grades. Scores were determined by a number of factors, including how well an agency trained its staff in security and the degree to which it adhered to security norms like limiting access to sensitive information and getting rid of passwords that were simple to guess. More than half of the assessed federal agencies scored a D or F. Of the twenty-four departments surveyed, the Department of Homeland Security, which includes a division devoted to observing cybersecurity, scored the lowest overall rating. The Justice Department, which is in charge of looking into and prosecuting incidents of hacking and other types of cybercrime, received an F as well. 13 agencies saw a minor increase in their grades from the year before, bringing the overall government grade from a F to a D. The chairman of the House Government Reform Subcommittee on Technology, Rep. Adam H. Putnam (R-Fla.), commented on these findings by stating that "the threat of cyberattack is real.[29]

Despite the controversy of cyberterrorism being a myth or reality, The United States has several laws and regulations that address cyberterrorism, which is defined as the use of computer

[27] COREPER, *Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism,* 3, Doc. No. 15175/08 (Nov. 14, 2008).

[28] Weimann, Gabriel. *Cyberterrorism: How Real Is the Threat?* US Institute of Peace, 2004. *JSTOR*, http://www.jstor.org/stable/resrep12222. Accessed 31 Aug. 2023.

[29] ibid

technology to conduct terrorist activities. Some of the key laws and regulations in this area include the Computer Fraud and Abuse Act (CFAA), 1986 law makes it a federal crime to intentionally access a computer without authorization or to exceed authorized access, causing damage to the computer or information stored on it. It also makes it illegal to use a computer to commit other federal crimes, including acts of terrorism. USA PATRIOT Act of 2001 law includes provisions related to cyberterrorism, such as the ability for law enforcement to conduct electronic surveillance and to access stored communications and data. Federal Information Security Management Act (FISMA), 2002 is a law that empowers federal agencies to develop and implement policies and procedures to secure their information systems and data. Cybersecurity Information Sharing Act (CISA), 2015 legislation encourages the sharing of cybersecurity threat information between the government and private sector entities to improve the overall security of critical infrastructure. National Institute of Standards and Technology (NIST) Cybersecurity Framework, 2018 is not a law, this framework provides guidance for organizations to manage and reduce cybersecurity risk. It is widely used by both public and private sector entities in the United States.

Additionally, the Department of Homeland Security (DHS) is responsible for protecting the nation's critical infrastructure from cyberattacks and has several programs and initiatives focused on cybersecurity, including the Cybersecurity and Infrastructure Security Agency (CISA) and the National Cybersecurity and Communications Integration Centre. It is important to note that the laws and regulations related to cyberterrorism in the United States are constantly evolving to keep pace with the changing threat.

One can conclude that while bin Laden may have his finger on the trigger, his grandchildren may be using the computer mouse, according to a frequently quoted statement by the Office of Homeland Security. It's possible that terrorists of the future may view cyberterrorism as having more promise than terrorists of the present. Furthermore, the next generation of terrorists is currently developing in a digital environment, where hacking tools are certain to improve in strength, usability, and accessibility. A terrorist organization may, For instance, a terrorist organization could detonate a bomb at a train station while also launching a cyberattack on the communications network, therefore amplifying the effect of the incident. If these systems are not rigorously secured in the most developed country of the world, it might be just as simple tomorrow to physically injure someone online as it is to hack into a website now.

III. INDIA

In India, cyberterrorism is dealt with under the Information Technology (IT) Act, of 2000, as amended in 2008. There is no specific legislation in India to address cyberterrorism. Sec. 66F was added as part of the 2008 amendment legislation to the Information Technology legislation of 2000 to address cyberterrorism. These laws and regulations complement other legal measures found in general and terrorism-specific legislation. The only provision that deals with and addresses acts committed with the intent to undermine India's unity, integrity, security, or sovereignty, as well as acts that promote terrorism through denial-of-service (DoS) attacks, the introduction of computer contaminants, unauthorized access to computer resources, theft of sensitive information, or any other information that could jeopardize India's interests in sovereignty or integrity, security, friendly relations. The IT Act defines cyberterrorism as any act of terrorism committed using a computer resource or a communication device.[30]

Under the IT Act, cyberterrorism is a punishable offense with penalties ranging from imprisonment for a term of up to life, along with fines. The Act also provides for the establishment of a Cyber Appellate Tribunal, which has the power to hear appeals against any order made by the adjudicating officer under the Act.

[30] 66-F. Punishment for cyber terrorism. (1) Whoever,—

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by—

(*i*) denying or cause the denial of access to any person authorised to access computer resource; or

(*ii*) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

(*iii*) introducing or causing to introduce any computer contaminant,

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under Section 70; or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

The Act also contains provisions relating to unauthorized access to a computer system, hacking, and the dissemination of offensive or menacing messages through communication devices. These offenses are punishable with imprisonment for a term of up to three years, along with fines.

In addition to the IT Act, India also has a National Cyber Security Policy, which aims to protect the country's cyberspace from cyber threats, including cyberterrorism. The policy outlines various measures such as creating a cyber-security framework, building capacities, and developing secure communication infrastructure to mitigate cyber risks. Overall, India has taken several steps to counter cyberterrorism and strengthen its cybersecurity framework to protect against cyber threats. In brief following are the provisions and complimentary rules to deal with Cyber terrorism:

• Sec. 66: Computer related offences including Hacking.

• Sec. 66A: Punishment for sending offensive messages through communication service etc

. • Sec. 66C: Punishment for Identity theft.

• Sec. 66D: Punishment for cheating by personation by using computer resource.

• Sec. 66F: Punishment of Cyber Terrorism.

• Sec. 69: Power to issue directions for interception or monitoring or decryption of any information through any computer resource.

• Sec. 69B: Power to authorize to monitoring and collection of traffic data or information through any computer resource for cyber security.

• Sec. 70B: Indian Computer Emergency Response Team to serve as the national agency for incident response.

• Sec. 84B: Punishment for abetment of offenses.

• Sec. 84C: Punishment for attempt to commit offenses.

• Implementation of Information Technology (IT) Security Guidelines, 2000.

• The Information Technology (Procedure and Safeguard for Interception Monitoring and Decryption of Information) Rules, 2009.

• The Information Technology (Procedure and Safeguard for Blocking for Access of Information by Public) Rules, 2009.

• The Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009.

• The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. • The Information Technology (Guidelines for Cyber Cafe) Rules, 2011.

• The Information Technology (Electronic Service Delivery) Rules, 2011.

• The Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties Rules, 2013.

SUGGESTIONS AND WAY FORWARD TO COMBAT CYBERTERRORISM

There are several ways that the legal system around the world can strengthen its existing laws to tackle cyberterrorism. One of the suggestions could be that states can enact stringent, comprehensive laws that criminalize cyberterrorism and establish penalties for those who commit such crimes. These laws can be used to prosecute cyber terrorists and hold them accountable for their actions. Cyberterrorism is a global problem, and it requires international cooperation to tackle it effectively. Combatting cyberterrorism by state requires a multi-faceted approach that involves various strategies and tactics. One of the ways to effectively combat cyberterrorism can be through Strong Cybersecurity Measures at the state level. Implementing robust cybersecurity measures, including firewalls, intrusion detection systems, encryption, and regular security audits, can help protect critical infrastructure, government networks, and sensitive data from cyber threats.

Another practice that can be adopted is establishing effective cyber intelligence and information-sharing mechanisms among different state agencies, law enforcement, intelligence agencies, and private sector entities that can facilitate timely detection and response to cyber threats. This includes sharing threat intelligence, vulnerabilities, and best practices for cybersecurity. Investing in building a skilled cybersecurity workforce within the state agencies and law enforcement, and providing regular training on cybersecurity awareness, incident response, and digital forensics can also enhance the state's ability to combat cyberterrorism effectively.

Fostering international cooperation and collaboration among nations in sharing information, intelligence, and joint efforts to combat cyberterrorism is the need of the hour. Cyberterrorism is often transnational in nature, and cross-border collaboration is crucial in addressing this global threat.

It is time for all states to develop and enforce comprehensive legal and regulatory frameworks that address cyberterrorism, including laws related to cybercrime, data protection, information sharing, and critical infrastructure protection. This can help deter cyber terrorists and provide a legal basis for prosecuting cyber terrorists. Fostering strong partnerships between the government and private sector entities, including technology companies, critical infrastructure operators, and other stakeholders can facilitate coordinated efforts in addressing cyber threats and leveraging the expertise and resources of both sectors to combat cyber terrorism.

CONCLUSION

Overall, a comprehensive approach that involves legislation, international cooperation, law enforcement, cybersecurity measures, and public awareness can be effective in tackling cyberterrorism. Governments can also implement cybersecurity measures to protect their critical infrastructure and other sensitive information from cyberattacks. Developing and implementing robust incident response plans to effectively respond to cyber-attacks and mitigate their impact should be the primary objective of the state. This includes defining roles and responsibilities, establishing communication protocols, and conducting regular drills and exercises to test the preparedness of the state agencies.

They can also raise public awareness about cyberterrorism and how to prevent it. This can include campaigns to educate the public on safe online practices and the risks of cyberterrorism. Countries can work together to share information, intelligence, and best practices to combat cyberterrorism. Law enforcement agency's role in investigating cyberterrorism cases and identifying the perpetrators is also vital. They can also work with other countries to arrest and extradite cyberterrorists. Every country is preparing for the digital age and the widespread adoption of IT technologies. The risk is that once virus programs are sold on the open market, they can be purchased and used by hackers anywhere in the world. This is because it is getting easier to conceal one's identity online. In conclusion, combatting cyberterrorism by the state requires a multi-layered and proactive approach that involves strong cybersecurity measures, effective information sharing, capacity building, international cooperation, legal and regulatory frameworks, public-private partnerships, incident response planning, cyber awareness and

education, offensive cyber operations, and continuous monitoring and adaptation. Implementing these strategies collectively can significantly enhance a state's ability to detect, prevent, and respond to cyberterrorism effectively.

BIBLIOGRAPHY

1. Aly, A., Macdonald, S., Jarvis, L. and Chen, T. (2016). Violent Extremism Online: New Perspectives on Terrorism and the Internet. 1st ed. [ebook] New York: Routledge, pp.18-21. Available at: https://www.book2look.com/embed/9781317431879 [Accessed 5 Sep. 2016].
2. Andrew M. Colarik.(2006). Cyber Terrorism: Political and Economic Implications: Ideal Group Publishing
3. Bary C. Collin.(1996). The Future of Cyber Terrorism. Chicago: University of Illinois,
4. Daniel Cohen, 'Cyber terrorism: Case studies', in *Cyber Terrorism Investigator's Handbook*, Chapter 13.
5. Dr. M. Dasgupta.(2009).Cyber Crime in India: A Comparative Study, Kolkatta: Eastern Law House Publication.
6. Gabriel Weimann (2005) Cyberterrorism: The Sum of All Fears?, Studies in Conflict & Terrorism, 28:2, 129-149, DOI: 10.1080/10576100590905110
7. Pavan Duggal.(2013).Text Book on Cyberlaw:Universal Law Publishing Pvt. Ltd
8. Peter Stephenson.(2000). Investigating Computer- Related Crime. New York: CRC Press
9. Prichard, Janet & MacDonald, Laurie. (2004). Cyber Terrorism: A Study of the Extent of Coverage in Computer Science Textbooks. JITE. 3. 279-289. 10.28945/302.
10. Rodney D. Ryder.(2001). Guide to Cyber Laws (Information Technology Act, 2000, E-commerce, Data Protection and the Internet), Nagpur:Wadhwa Publication.

11. Wilson, J. R. (2007). Terrorist Capabilities for Cyberattack: Overview and Policy Issues. CRS Report for Congress.