INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

STRENGTHENING INDIA'S CYBER DEFENSE: THE IMPERATIVE FOR ENHANCED CYBER LAWS AND COUNTERTERRORISM MEASURES

AUTHORED BY - PRANAV DEEPANKAR KETHINENI
- 190401427055
BBA LLB (HONS) 2019-2024

Abstract:

Cyber terrorism is one of the growing issues in India that needs to be addressed as soon as possible. Cyber terrorism is defined as the use of devices such as of computers and Information Technology, in complementary use of internet, with the aim to cause disturbances in the society. Disruption can include supporting political activism which is also a big concern. Other types of disruptions include crating mass chaos, hacktivism and other issues that will be covered in the paper.

India is having a substantial rise of cyber-attacks and if not addressed as soon as possible then there will be a possibility that in the future, if there is any legal vacuum there then it can be taken undue advantage of.

The paper aims to explain the different types of cyber-crimes that India as growing country might be subject and especially those kinds of cyber-crimes that may affect the country as very and further to analyze the cyber terrorism laws which are in place currently and another perspective around the analysis would also include if the current laws in India are enough to address the cyber terrorist attacks in different forms. Further the paper aims to make required suggestions on any reforms necessary for the protection of cyberspace in India. The paper shall aim to suggest more types of laws that are required to be covered under this area as to aim that all the kind of issues are covered which India can be a subject or the victim of in case of a cyber-attack.

Keywords: cyber- attack, cyber terrorism, cyber warfare, cyber space, cyber-crimes, disruption, chaos.

 ISSN: 2582-6433

SYNOPSIS

1.1) Overview –

Cyber-crime -

Cyber-crime can be defined as offenses that are committed against an individual or any group of individuals with the aim of causing a physical or mental trauma through electronic means which can be defined as cybercrime.[1]

Cyber-crime is categorized as–

- The computer is deemed as a Target -the offenders use one computer to attack other computers. The example of these cyber-attacks is as below -
  e.g. Hacking, Virus/Worm attacks, DOS attack etc.
- The computer is deemed as a weapon -the computer is being used to commit crime in the real world. It is done through causing disturbance in the digital space.
  e.g. Cyber Terrorism, IPR violations,

Cyber-terrorism –

Cyber-terrorism is the clash of terrorism and cyber-space. Cyber-terrorism is generally understood as unlawful attacks against a network of computers and the information stored is used to coerce a government, so that the offenders can achieve their religious, social or political agendas achieved.

Cyber terrorism also poses a threat to the actual and virtual world.

The offence comprises committing acts which include destruction, alteration, acquisition, or transfer against the following:

- Defence Forces
- Financial infrastructure
- Civilians
- Destroyed smart city control and data acquisition systems
- Investigated smart army, among other things.

It would be highly devastating, if the cyber-attacks target the basic infrastructure or the financial systems, conducted in collaboration with a traditional attack with other capabilities. This would

1Cyber Laws of India, Ministry of Electronics and Information Technology, Govt of India (February 17th 2024) https://infosecawareness.in/cyber-laws-of-india

 ISSN: 2582-6433

be a deadly combination of Cyber techniques with traditional resources.

The Cyber security is not a choice but a national responsibility. The Indian Govt. has made satisfactory steps for the development and implementation of national cyber security strategy, but there are still many more steps that are to be take both by the government as well as citizens towards cyber – security.

Initiatives taken by Government of India with respect to Cyber-Security –

Information Technology Act: Cyber terror Law of India

The Information Technology Act (hereafter the Act) sanctions legal provisions concerning cyber terrorism.

1.2) Literature Review: -

1. ***Cyber Terrorism in India: A Physical Reality or Virtual Myth by*** **Shiv Raman, Nidhi Sharma.** The researcher refers to this article to understand the seriousness about cyber terrorism. This article talks about this history as well as various cyber terrorist attacks around the world. The article also covers various lws to tacle the offense of cyber terrorism under the ambit of Indian law. [2]
2. ***Legal Dimensions of Dreaded Cyber Terrorism in India*** **by Maneela Bansal.** The article gives in-depth research about the various cases that India has been a subject or victim of with respect to cyber-terrorism, which the researcher has used to understand how serious of problem is cyber-terrorism in the country of India.[3]
3. ***CYBER TERRORISM IN INDIA*** **by Ankit, Dr. Harshita thalwal.** This article has been used by the researcher for a better understanding on the legislative framework in India with respect to cyber-terrorism in India. The article covers various steps that were taken by the government with respect to controlling cyber terrorism in India.[4]
4. ***CYBER WARFARE AND CYBER TERRORISM*** **by Medha Surabhi.** This paper talks deeply about the similarities of cyber warfare and cyber terrorism. And the factors casuing these attacks. The researcher has referred the article for the same. [5]
5. ***Cybersecurity and Threats: Cyberterrorism and the Order Today*** **by Rebant Juyal.** The article examines cyber terrorism can be called as a subset of cyber threats and also aims to analyse the constitutional duty upon the policy makers of the country to protect the cybers-

[2]Indian Journal of Law and Human Behavior Volume 5 Number 2 (Special Issue), May - August 2019
[3]Computers & Law May 2010
[4] Journal of Critical reviews, Vol 7, Issue 15, 2020
[5]Surabhi, Medha, Cyber Warfare and Cyber Terrorism, SSRN (February 18th 2024) http://dx.doi.org/10.2139/ssrn.2122633

 ISSN: 2582-6433

space. The researcher refers to this article to understand, why is there a constitutional obligation to protect cyberspace. [6]

6. ***Emerging Cyber Security India's Concern and Threats*** **by Aadil Ahmad Shairgojri and Showkat Ahmad Dar.** The Legal paper examines about the threat of cyber security in India. The article also talks about the sectors that can be affected by Cyber-attacks. The researcher has referred to the research in order to understand about the sectors that can be affected by cyber-attacks.[7]
7. ***Growing Menace of Cyber Terrorism-Challenges and the Way Forward*** **by S. Maanasa and Aswathy Rajan.** The research gives knowledge about the concept of cyber - terrorism. The research talks about the need for new laws revolving around cyber-terrorism. the challenges associated with the current laws. The research also talks about the measures to be taken to deal with cyber-security challenges and the researcher has referred the article for the same.[8]

1.3) Research Problem –

As per the reports of the year 2023 which was based on the subjected "India Threat Landscape Report" and was published by a cybersecurity firm called Cyfirma which is based in Singapore, India is one of the most targeted countries globally. It faces upto 13.7% of all the cyber-attacks. This may be a big issue in India if not addressed immediately. The study is about the current cyber-terrorism laws and its effectiveness. The researcher questions if there is a requirement of better cyber-terrorism laws in India.

1.4) Research Questions

1 What are the various interpretation on cyber-terrorism and has India been a part of any cyber-terrorist attacks?

2 Are there any cyber -terrorism law in India and if so, are they effective enough?

3 Is there a need for an updated and much more stringent legislation to deal with cyber-terrorism?

[6]Manohar Parrikar Institute For Defence Studies And Analyses Journal of Defense studies, April-June, 2021, Volume:15

[7] Emerging Cyber Security India's Concern and Threats Aadil Ahmad Shairgojri1* , Showkat Ahmad Dar2

[8] S, & Rajan. (n.d.). Growing Menace of Cyber Terrorism-Challenges and the Way Forward. *International Journal of Pure and Applied Mathematics, Volume 119 No. 17*(1314–3395).

 ISSN: 2582-6433

1.5) Objectives

- To analyse the concept of cyber- terrorism.
- To examine the current laws revolving around cyber terrorism.
- To study about the cyber-attacks which India were a part of.
- To analyse if the current laws on cyber terrorism are adequate enough

1.6) Hypothesis

The hypothesis that the researcher is assuming for this area of research is that the country of India does lack proper laws to fight cyber- terrorism issues.

1.7) Scope and Limitation of the Study

To study about the concept of cyber terrorism and the laws revolving around it in India as well as aiming to suggest if there is a scope of better cyber terrorism laws in India. The limitation of this paper shall be with respect to whether there is a need of strict cyber terrorism laws in India.

1.8) Methodology of the Study

The research will follow the doctrinal method as it is mostly influx of data from various places. The sources are mostly secondary. We have consulted as many sources of books and Journals and also different articles and lectures of leading legal thinkers from India and around the world. Original articles and books by leading thinkers on the respective ideologies are the most important all the sources. The following methods will be relied upon to fulfill the objectives of the study and collection of necessary data. In addition, various case laws both Indian and Foreign are referred which involves this construction.

1. Study of the existing books.
2. Primary and secondary source of books and journals.
3. Internet sources.
4. Visiting the different libraries.
5. Listening to the lectures of leading jurists

 ISSN: 2582-6433

CHAPTER 2 – STUDY OF THE CYBER STRUCTURE AND ATTACKS IN INDIA

Digital Structure of India

India is a at the stage where there is a rapid rise in the increase in the digital economy. The digital infrastructure is gradually increasing. This strong infrastructure shall also support in the building of a robust economy. But this can also be hindered due to cyber-attacks in India.

The strong growth of the digital infrastructure portrays the growth of the country towards a developing economy.

Various factors such as technological advancements, government initiatives, increasing the access of Internet and the support towards the growing digital economy. This is happening because of the below reasons –

1. Digital India Initiative- This was one of the programs that was launched by the Indian government with the aim to transform the society by empowering it digitally. It focuses on various areas which includes the strengthening of the digital infrastructure, increasing of the digital literacy. This is the first step towards the shaping of India's cyber security infrastructure.[9]
2. Digital Payments – this is one of the most remarkable achievements in the Indian Digital Economy. India has seen a rise of digital payments since demonetization. But what has been more remarkable is the access that citizens got through these digital payments. There has been a vast increase in bank accounts. From big businesses to small vendors are using accepting digital payments. This technology has enhanced the cyber structure of the country. Cashless transactions have also helped as they were considered as a curb towards the elimination of black money.[10]
3. E- Governance - India has been promoting the digital structure through enhancing digital platforms through the delivery of public services. Projects like Aadhar Biometric identification, Unified Payments Interface (UPI) contributed majorly in increasing the efficiency in various sectors which contribute to the development of India's cyber structure.[11]

[9] Journal of Positive School Psychology http://journalppw.com 2022, Vol. 6, No. 2, 284 – 290
[10] *ibid*
11 Nair, A. k. (2023, September 7). Role of E-governance and Digital India in empowering Indian citizens.

 ISSN: 2582-6433

4. Digital Connectivity – India has gradually developed with respect to their internet services. It has gradually increased from 2g to currently 5G, but what is remarkable is the access of this to users. There has been a surge in the number of digital users. Companies like Reliance have also played a major role regarding this. Jio a subsidiary of reliance was launched which gave free internet services through their Sim which increased the users.[12]

These initiatives are playing a major role in the development of a robust digital structure of the country. Till date it can be said that the programs have bought successful changes in the strengthening of the digital structure. IT has been embedded in various services such as health, education, banking and agriculture as well.

India's Vulnerability to Cyber Attacks –

India has been pushing the limits of its digital infrastructure. India was having a steady advancement in the digital sector but the pandemic had boosted the need of heavy digital advancements.

There had been an extensive increase in the digital networks, but there has been a major concern that had come up on the parallel road. That is the concern of security. The security threats are can be considered as key factors that could affect the digital infrastructure of the Country. Maintenance of security is the most crucial factor, because when the digital infrastructure is growing, if no adequate measures are taken to safeguard, then that hinders the growth and affects the digital infrastructure. [13]

Types of security concerns or cyber- attacks that India may be or is being subject to –

1. Hacking – Hacking refers to the act of making an attempt to enter a computer network with having authenticated authorization, the offence also includes the offender corrupting the device of the victim by uploading malicious content on the device such ascomputer, laptop, smartphone, Tablet of the victim. Hacking can also cause leaking of private data. which in turn may affect the significant life of the user. being a victim of hacking can lead to the loss of private and important data or it can also lead to financial loss.
2. Phishing – Phishing is a type of fraudulent activity that involves stealing information related to the person's banking account card details via email.

B.PAC. https://bpac.in/role-of-e-governance-and-digital-india-in-empowering-indian-citizens/
[12] Journal of Positive School Psychology http://journalppw.com 2022, Vol. 6, No. 2, 284 – 290
[13]] Dr. Shrish Kumar Tiwari, Cyber Crimes: A Threat to Humanity, 2 HSSR 1, 94-101 (2014)

 ISSN: 2582-6433

3. Vishing (Also Known AsVoice Phishing) – The Banking account details are taken by offender through the means of a telephone. This is one of the most common type of scam in India. people who are not digitally literate can be victims of such crimes.
4. Identity Theft - – Impersonation of an individual who is on the internet or creation of an identity which is fake in order to acquire information from any individual is known as identity theft.[14]

The biggest security concern that could have strong impact on the growth of the digital sector as well as affect other sectors in turn which can affect the economy is cyber-terrorism.

Cyber Security can be analyzed from four different perspectives. These perspectives are, the missions with respect to cyber terrorism, the methods that are followed by the aim of cyber terrorism, the results of these cyber terrorism attacks and the role of laws in combating the same. The targets of cyber- terrorism are as below -

1. The crime is committed to communicate a message which is particularly destructive in nature to the target governments.
2. The different types of methods which are deployed to communicate their message, through the use of cyber space such as threatening emails, corrupting the government websites, hacking of governmental systems or disrupting the civil society by destroying the proper working of the digital information systems, etc.
3. the aim to affects the computers and the connected networks as to affect the entire system being governed, so it could affect the target population as well as create a threat.
4. The crime is motivated by religious, social and political ideologies.

India is a country which is still at a developing phase. Crimes like cyber-terrorism are something that can target India fueled by political, social or religious settings. The digital infrastructure still has a long way to go ahead for the development of robust security features. [15]

Effect of Cyber-terrorism attacks in India

Cyber-terrorism was one of the key factors that had played a role in the Attacks of 26/11.

The investigation of the attacks that happened in Mumbai on 26 November, 2008 had revealed that communication took place took place between the terrorists using the help of cyber space. The use of cyber- space in order to communicate helped the terrorists to get familiar with the areas they were targeting as well as the population with respect to the same areas, which resulted

[14] 2020 IJCRT | Volume 8, Issue 11 November 2020
[15] Maneela Bansal, Legal Dimensions of Dreaded Cyber Terrorism in India, 3 CLJ 8, 20-22 (2010)

 ISSN: 2582-6433

in panic in the entire nation and loss of lives as well.

During July 2011, there was usage of digital technology for the committing of bomb blasts in the market which was in the area of in Jhaveri Bazaar, Mumbai. During the year of 2010, another bomb blast happened in Varanasi, and upn investigation it came into light that there was cyber communication that took place in order to facilitate the blast.

A huge impact was created due to which the Government of India took strong steps to strengthen the infrastructure of the cyber security network in the country. This included measures to be taken to prohibit terrorist activities and their utilization of cyber space. This was done by amending the Indian information Technology Act, 2000.

In the country of India, extremist activities are carried out to disrupt the sovereignty and integrity are regulated by the Prevention of Terrorism Act, 2002 (repeal ordinance, 2004), besides there are various provisions under the Indian Penal code, in chapter VI, that deals with offences against the State.

The main focus of these legislations is to restrict and make an attempt to curb the activities of terrorists in the country. They also placed regulation which would give authorization on the forensic evidences that can helping tracing the motive behind, the attack plan as well as the mastermind behind these activities and the people who are recruited to execute these plans.

As the trajectory of digital communications is on a rise, the Indian Evidence Act has also been updated and has started accepting cyber forensic specimens as evidences for extremist ideologies and activities. [16]

The IT Act, 2008 shows that aspecpt of cyber terrorism with respect to the provision of section 69 F[17], but has failed to give recognition the proper meaning of terrorism or the terrorist activities through the use of cyberspace. The law has stayed a shadow of the existing anti -terrorism legislations. Vandalizing activities on the cyber space can also be fallen under the ambit of cyber terrorism, but the communication being carried out in order to which is being carried out to disrupt

[16] Shaily Jain and Shrishti Soumya, A Study of Acts of Terrorism through Cyberspace in India: Prevention and Remedies dealing with Cyber and Technology related crimes, 1 DPILJCC 3, 1-16 (2016)
[17] Information Technology Act, 2000

 ISSN: 2582-6433

the peace of a civil society cannot be ignored.

Cyber- Attacks in India

In the recent times of globalization, not only for a developing country like India but the other countries also face the issue of Cyber Threats. India has been facing a number of cyber – attacks. India's developing digital infrastructure is also inviting equal number of troubles which are to be deal with. In the year of 2023, India had received 2,138 weekly attacks per organization, compared to the year of 2022, the cyber-attacks have increased by approximately 15%.[18]

From the statistics, it can be interpreted that India is being a subject to Cyber-attacks from all around the world. This would highlight the need for stringent legislations with a quick approach to punish the people committing these crimes, as to portray to the external threats that the development of the country cannot be hindered.

Sectors that can be affected by Cyber- attacks –

1. Defense Sector of India –

India's armed forces is one of the strongest forces around the world. The industry is robust and does not lack resources. The increase of reliance on modern technology has also affected the defense industry of the country. If not having strict security measures, it would put the country at risk. In the year of 2012, a group of hackers had aimed to hack the eastern command computer systems installed in the Indian Navy. They had supervision over the missile tests of the submarine, infected systems had sent documents and data to Chinese IP addresses. Till date it has not been revealed as to what data had been leaked. There is a requirement of real time cyber defense to protect the data. These kinds of issues half the time would not even come to light. This is why there should be legislations where the leaks are to be restricted and reported as well.[19]

2. Finance –

India is growing country. The integration of the financial system and the digital infrastructure can

18 Pti. (2024, January 22). India witnesses 15% rise in cyber attack cases in 2023. mint. https://www.livemint.com/news/india/india-witnesses-15-rise-in-cyber-attack-cases-in-2023-emerges-as-2nd-most-targeted-nation-11705939863447.html#:~:text=Organisations%20across%20the%20globe%20experienced,per%20cent%20surge%20since%202022.

19 Emerging Cyber Security India's Concern and Threats Aadil Ahmad Shairgojri1* , Showkat Ahmad Dar2 1Research scholars of Political Science & public administration Annamalai University Tamil Nadu, India

 ISSN: 2582-6433

be considered as one of the most remarkable achievements. This is also helping in the boost of the economy as well. But the reliance on this has introduced new concerns. Hackers are highly motivated with the idea of financial gain. This is gives them the incentive to hack back accounts for money. This has happened several times in the past as well. But at the current times, India's financial sector is on a rise. These are the times where there are to be guidelines on protection of the financial sector, and there are to be strict laws to be set up. These laws should permit the ethical hackers working for the government to trace back to the hackers and equivalently punish these people as a measure. Setting up such laws and actions would cause fear to commit such crimes.[20]

3. Health care system –

India is building a robust health care system. This has included the integration of the digital infrastructure to the health care system. Cyber-attacks on health care organizations could lead to breach of data, ransomware attacks, which could pose as a risk to public health and safety. Medical records of patients are personal and leaking them could be affecting the lives of the patients.

4. Small and Medium Enterprises (hereinafter referred to as MSMEs) –

These businesses are what fuel the Indian Economy. Cyber-attacks on MSMEs could lead to potential breach of data as well as heavy financial losses. These losses could be critical to the functioning of the businesses. It is one of the major sectors that is to be protected in order to fuel development for the country.

5. Individual Customers –

a common man is vulnerable to a number of cyber- attacks. These cyber-attacks may include being a victim of hacking, it could be that he is a victim of identity theft, malware theft or phishing. These kind of cyber-attacks on individuals would result in causing financial loss, privacy breach, personal safety would be put at jeopardy.

6. Government and Public Services –

Government agencies such as the CBI, central and state governments, as well as municipal

[20] *ibid*

 ISSN: 2582-6433

bodies, are targeted by cyber-attacks as the attackers seek to steal sensitive information, with the aim to disrupt government operations, and undermine public trust on the government. Cyber-attacks on government institutions have the potential to compromise the trust on national security, it would disrupt essential services, and impair governance functions.

7. Educational Institutions –

Educational institutions such as schools, colleges, and universities, also pose as a target as by the launch of by cyber-attacks on them would be as to seeking to steal sensitive research data, personal information of students and faculty, and have the potential to disrupt academic activities. Cyber-attacks on educational institutions can damage institutional reputation, and disrupt learning environments.[21]

These are only few of the sectors as pointed out by the researcher. But there are many other sectors which can be victim of cyber-attacks. The attack on these sectors would cause massive disruption to the order of peace and civil in the society, which cannot be afforded. If any heavy damage is done to any of the pointed-out sectors by the researcher, the loss could be unbearable. This would affect the development of the country, and the loss that is caused can be to an extent that will can be non-recoverable. This highlights the need as to why there is a requirement of much stringent laws in regard to cyber terrorism.

Protection of these sectors is a high necessity. It requires a multilayered approach to ensure maximum protection. This would involve formulating cybersecurity policies on companies and imposing them on companies so it could be followed. There should be collaborations between government agencies and cyber -security companies to develop robust cyber – security features. All the sectors while growing should be being built with cyber-resilience. There should be regulations being dealt with the same.

[21] Emerging Cyber Security India's Concern and Threats Aadil Ahmad Shairgojri , Showkat Ahmad Dar

 ISSN: 2582-6433

CHAPTER 3 – ANALYZING THE DEFICIENCIES OF THE CURRENT CYBER LAWS AND SUGGESTION ON IMPROVEMENT

The government has taken initiatives to protect the digital space. The Information Technology Act which was initiated during the year of 2000 is considered as the foundational legislation which governed the cyberspace jurisdiction.

The below sections of the IT act, 2000 talks about the sections that cover the offenses related to cyber terrorism or cyber-attacks.[22]

- 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 monitor and collect traffic data or information through any computer resource for cyber security.
- Sec.70B: Indian Computer Emergency Response Team to serve as national agency for incident response.
- Sec. 84B: Punishment for abetment of offences.
- Sec. 84C: Punishment for attempt to commit offences.
- 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.

[22] Information Technology Act, 2000

 ISSN: 2582-6433

- 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.

The government has been pushing beyond limits to improve the digital infrastructure. It can be seen that the digital access has been increased to citizens as well. Cyberspace interacts with economic, business and every major sector of India. For achieving India's aims of the cyberspace keeping in mind their sovereign, economic and business interests in the cyberspace, the government has to make stringent legislations and cybersecurity reforms. There should be development of new mechanisms and reform steps and they are of high need to be introduced with the main focus on the constitutional duty of the state under Article 19(1)(g)[23] and Article 355[24] of the Indian Constitution.

In the year of 2008, the Information Technology Act had been amended in order to incorporate provisions with respect to cyber terrorism. However, from the year 2008 till the year of 2021, the exploitation of cyberspace by terrorist organizations or any group with the initiative to disrupt the peace in the society has undergone a robust systematic transformation. The evolution of destructive technologies with the conglomeration of technology has made the ideology of cyber terrorism highly complex to deal with. Cyber terrorists utilize creative ways in order to exploit the use cyberspace for the radicalization of youth and to trigger cyber-attacks which can cause destruction on a very high scale.[25]

The legislation can be called outdated. The cyber laws have been enacted years ago, but there have been rapid advancements in technology till date and the advancements continue to do so. Though the advancements have been made for the betterment of society, it has also given rise to complexities and cyber threats. The legislation needs to be continuously updated to keep pace with the emerging cyber threats.

The biggest issue with the Information Technology Act, 2000, the Indian Authorities have the jurisdiction to investigate and prosecute only those cybercrimes which occur within its territorial

[23] Article 19 (1) (G) Freedom to practice Profession, Occupation, Trade or Business
[24] Duty of the Union to protect states against external aggression and disturbances
25 Somya, S. (n.d.). Cyber terrorism and laws in India. Legal Service India - Law, Lawyers and Legal Resources. https://www.legalserviceindia.com/legal/article-8949-cyber-terrorism-and-laws-in-india.html

 ISSN: 2582-6433

boundaries. But cybercrimes can transcend geographical boundaries. This make it a challenge to determine the jurisdiction under which the offenders can be prosecuted, if they operate from outside the country.

Issue with the Cyber terrorism Law in India –

Cyberspace, has proven to be an effective weapon for demolishing the national critical infrastructure of the country or to threaten a government with the aim of extortion or meet demands made by the terrorists. Cyberspace has the potential to cause destruction without the risk of exposure to terrorists. The government should believe that terrorists have the access to cyber technology which could be used by them with malicious intentions. Government has the duty and obligation to invest resources to install security measures to protect security measures and strict regulations against cyberterrorism.[26]

Section 66F had been introduced with the aim to cover the aspect of Cyber Terrorism and punishment for the crime as well. The section includes all such activities carried with respect to cyber-terrorism, that are considered as a threat to the ideology of the nation include unity, integrity, sovereignty as well as security to the nation or also create fear in the minds of people the unauthorised access to a computer and cause damage to the computer grid.

These acts have the potential to cause injuries to persons, cause death, damage or cause destruction of any property, cause a hit on the essential supplies or services, and majorly damage the critical information structure, it becomes an offence which is by nature punishable. The punishment for this offence as per law is for a minimum of three years of imprisonment which can also extend up to life imprisonment, which depends on the gravity of the act.

The main issue with this section is that, while this section makes an attempt to define the term "cyber-terrorism" it fails to cover the entire concept of cyber-terrorism. It is impossible for just one section to include all the actions that can fall under the ambit of cyber-terrorism. For example, the acting of using internet to brainwash or influence people towards terrorism can also be under the ambit of cyber-terrorism.

This issue is not only with respect to India, but there are other countries who are equally prone to

[26] Narula. S and Jindal. N, Social Media, Indian Youth and Cyber Terrorism Awareness: A Comparative Analysis, 5 JMCJ 2, 1-4 (2015)

 ISSN: 2582-6433

the issue of cyber-terrorism and have not come up with a clear definition nor has created a tailored solution to deal with it.

On the domestic level, the term "cyber security" from a legal perspective has to be widened and as per the Information Technology Act, 2000 it must be stretched to cover various factors such as cyber communication and any other relevant factors which aid the terrorists in achieving success in their terror missions.

Thus, the researcher is of the opinion that there is a need to update cyber security laws and widen the coverage of Cyber-terrorism.

India has enacted several legislations to address the issue of cybercrimes, but there are gaps and inconsistencies. There is a need for a comprehensive and cohesive legal framework to deal with various aspects of cybercrimes as well as cyber-terrorism.

CHAPTER 4 – CONCLUSION

These are the reasons as to why the researcher is of the point of view there is a need for an updated legislation as to covering the new aspect of cyber security issues and cyber- terrorism issues. The Information Technology Act, 2000 lacks the features are as below –
Cyber-crimes are transcended across boundaries. But the Indian legislation only has the jurisdiction to deal with the cyber-crimes that are committed within the territory. The legislation in this regard has to be upgraded accordingly.

The policy makers are long due to consider enacting a new cybersecurity legislation, which should be solely dedicated to deal with present-day cybersecurity challenges and has strong and efficient guidelines to regulate all aspects of cybersecurity which should also be inclusive of cyber-terrorism.

Cyber-terrorism should be considered a matter of high importance as cyber – terrorism has the capacity to bring destruction from the virtual world to the physical world. This is one crime for which universal jurisdiction can and should be considered for being applied.

The administrators of the systems and the government always need to be alert for any warning that they can receive for any cyber-attack that could take place at any point of time.

 ISSN: 2582-6433

There should be security guidelines by the policy makers ensuring routine risk assessment of information infrastructures that by law should be conducted on a regular basis and also be given priority for proper risk management. There should be development of policies based on cyber-warfare encryption.

Services related to E-governance should be installed with additional security features. There should be a creation of a cyber security agency which should act as for the protection of government agencies and civil agencies which would improve the country's resilience against electronic attacks, and also enhance the security measures.

Maintenance of systems should be priority by instilling guidelines and regulations for the continuous check, it should always be seen that the software and antivirus programs are always up to date. There are active defense measures that should be adopted and should include, finding the source of attacks and the legislations should be stringent to impose serious risk and penalty, as well as counter attack measures. Each attack should be analyzed and proper steps are to be taken to make sure that these vulnerabilities are closed and cannot be a threat for the future compromising the cybersecurity features or the systems as well.

India should also make an attempt to make its laws and policies being complementary to the guidelines of international conventions. This would help in building strong connections with different nations all over the world. This would also eliminate the need of jurisdictional issues. if conventions and treaties cover this aspect. There should be a comprehensive analysis by the government of the needs and wants regarding cyber security guidelines between itself and the various nations and bais of that there should be comprehensive policy that should be formed and abided by.

As there has been an increase in digital access, the need for internet Literacy should also be increased, so that each individual can maintain cyber security at their own individual level.

The best way to combat cyber-terrorism can be by harmonizing the cyber laws of various countries through joining or being a part of international treaties. This can be considered a tremendously huge task. The initiation can be by adopting measures such as sharing of data on terrorists, sharing new technologies between two countries, quick response to bilateral requests

and being of help to Interpol and other international agencies.

It can also be seen that there is a high need for each individual to maintain personal relationships to make sure that the individual members of a family or their friends do not get influenced by terrorist organizations like the ISIS. Young minds are more vulnerable to fall for such influences and hence there is a need and obligation of parental control and parental guidance in order to save them from falling to the acts of being brainwashed by any terrorist organizations.

In Conclusion the researcher interprets that, cyber terrorism can be seen as tool which could be used to instigate terror through cyberspace. In light of the recent series of events that happened India and other nations have been highly alarming. It may be concluded that cyber-crime activities such as cyber terrorism, cyber warfare and cyber-crimes, are of a matter of serious concern.

With the advancing of science and technology, the world of cyber space aims to reach a level where is has the potential to become a medium to propagate terror activities. It has become important that the governments all around the world pay heed to the threat of cyber-terrorism and take all measure steps in order to stop the menace. National and international agencies are making efforts in order to build a safe and secure cyberspace. The evolving nature of the cyber world requires scrutiny and continuous upgrade in security measures.

BIBLIOGRAPHY

- https://bpac.in/role-of-e-governance-and-digital-india-in-empowering-indian-citizens/
- https://medium.com/@praaj99341/indian-cyber-laws-and-deficiencies-1206fae59a80
- https://www.legalserviceindia.com/legal/article-8949-cyber-terrorism-and-laws-in-india.html
- https://journals.indexcopernicus.com/api/file/viewByFileId/783266.pdf
- https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india
- https://thediplomat.com/2023/11/indias-cyber-vulnerabilities-grow/#:~:text=According%20to%20the%20latest%20report,top%20three%20most%20attacked%20countries.
- https://www.business-standard.com/technology/tech-news/vulnerabilities-in-india-s-digital-infra-spur-rise-in-cyberattacks-experts-123111300949_1.html

- https://www.livemint.com/news/india/india-witnesses-15-rise-in-cyber-attack-cases-in-2023-emerges-as-2nd-most-targeted-nation-11705939863447.html#:~:text=%22In%202023%20India%20received%202%2C138,incidents%2C%22%20Check%20Point%20said.
- https://www.researchgate.net/publication/367148483_DIGITAL_INFRASTRUCTURE_DEVELOPMENT_IN_INDIA_FOR_CITIZEN_EMPOWERMENT
- https://www.investindia.gov.in/team-india-blogs/digital-india-revolutionising-tech-landscape
- https://egov.eletsonline.com/2024/05/gst-collections-breach-landmark-milestone-of-%e2%82%b92-lakh-crore/
- https://www.niti.gov.in/sites/default/files/2021-09/The-Role-of-Digital-Infrastructure-in-socio-economic-development-042021.pdf

REFERENCES

1. Narula. S and Jindal. N, Social Media, Indian Youth and Cyber Terrorism Awareness: A Comparative Analysis, 5 JMCJ 2, 1-4 (2015)
2. Article 19 (1) (G) Freedom to practice Profession, Occupation, Trade or Business
3. Duty of the Union to protect states against external aggression and disturbances
4. Somya, S. (n.d.). *Cyber terrorism and laws in India*. Legal Service India - Law, Lawyers and Legal Resources. https://www.legalserviceindia.com/legal/article-8949-cyber-terrorism-and-laws-in-india.html
5. Emerging Cyber Security India's Concern and Threats Aadil Ahmad Shairgojri , Showkat Ahmad Dar
6. Emerging Cyber Security India's Concern and Threats Aadil Ahmad Shairgojri1* , Showkat Ahmad Dar2 1Research scholars of Political Science & public administration Annamalai University Tamil Nadu, India
7. Pti. (2024, January 22). *India witnesses 15% rise in cyber attack cases in 2023*. mint. https://www.livemint.com/news/india/india-witnesses-15-rise-in-cyber-attack-cases-in-2023-emerges-as-2nd-most-targeted-nation-11705939863447.html#:~:text=Organisations%20across%20the%20globe%20experienced,per%20cent%20surge%20since%202022.

 ISSN: 2582-6433

8. Shaily Jain and Shrishti Soumya, A Study of Acts of Terrorism through Cyberspace in India: Prevention and Remedies dealing with Cyber and Technology related crimes, 1 DPILJCC 3, 1-16 (2016)
9. 2020 IJCRT | Volume 8, Issue 11 November 2020
10. Maneela Bansal, Legal Dimensions of Dreaded Cyber Terrorism in India, 3 CLJ 8, 20-22 (2010)
11. Journal of Positive School Psychology http://journalppw.com 2022, Vol. 6, No. 2, 284 – 290
12. Dr. Shrish Kumar Tiwari, Cyber Crimes: A Threat to Humanity, 2 HSSR 1, 94-101 (2014)
13. Nair, A. k. (2023, September 7). *Role of E-governance and Digital India in empowering Indian citizens.* B.PAC. https://bpac.in/role-of-e-governance-and-digital-india-in-empowering-indian-citizens/
14. Journal of Positive School Psychology http://journalppw.com 2022, Vol. 6, No. 2, 284 – 290
15. Journal of Critical reviews, Vol 7, Issue 15, 2020
16. Surabhi, Medha, Cyber Warfare and Cyber Terrorism, SSRN (February 18th 2024) http://dx.doi.org/10.2139/ssrn.2122633
17. Manohar Parrikar Institute For Defence Studies And Analyses Journal of Defense studies, April-June, 2021, Volume:15
18. Emerging Cyber Security India's Concern and Threats Aadil Ahmad Shairgojri1* , Showkat Ahmad Dar2
19. S, & Rajan. (n.d.). Growing Menace of Cyber Terrorism-Challenges and the Way Forward. *International Journal of Pure and Applied Mathematics*, *Volume 119 No. 17*(1314–3395).
20. Indian Journal of Law and Human Behavior Volume 5 Number 2 (Special Issue), May - August 2019
21. Computers & Law May 2010