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

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

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

ISSN: 2582-6433

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

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

CYBER TERRORISM

AUTHORED BY: MS. PAYAL SAINI
Student, BB.A LL.B, 3rd Year
Bharati Vidyapeeth (Deemed To Be University), New Law College, Pune

ABSTRACT

This study aims to contribute to efforts against cyber threats such as terrorism and criminality. The article aims to highlight future cyber security challenges, including growing dangers such as cyber war, terrorism, and criminality.

Cyber risks such as cyber war, terrorism, and criminality significantly undermine cyber security. As ICT advances, the methods and assets used to combat asymmetric threats, such as cyber terrorism and cybercrime, grow increasingly complicated.

The whole idea of this paper is to cite how cyber weapons are more dangerous than traditional methods of terrorism, it is clear that hardware is employed to launch bullets, whereas software can cause damage or have negative consequences.

KEYWORDS

Cyber-crime, cyber space, cyber terrorism, threat actors

INTRODUCTION

With an aim to achieve heights and growth for the enormous technological advancement the ways, forms and mediums for crimes have multiplied manifold. For the economical and infrastructural development it is important to liberate the country for the whole and expand the human intervention in diverse areas. Since when, the information technology was adapted by the society, it opens the door in every sector making it ubiquitous in nature. At present, most of the economic, commercial, cultural, social and governmental activities and interactions of countries, at all levels, including individuals, non-governmental organizations and government and governmental institutions, are carried out in cyberspace However, the rapid development and large-scale integration of technology into various aspects of society have indeed brought many phenomenon of cyber threats. Anyone either individually or an organization can by exploited by threat actors in

ISSN: 2582-6433

the cyber space. And currently many criminals has adopted the modern way of spreading terror and fear in the society.

The threat of terrorism arises from the instant growth and technological advancement. Due to the increased in the dependency of the computer applications and software it gives easy access to the threat actors to insert fear among the groups or institutions. The whole of billions of worldly population is alive and connected through cyber world. Though this artificial world has united us in one but it arises the fear of terror or unethical breach in privacy and safety. This phenomena of bombing people with artificial weapons has grabbed the eyes of many terrorist organizations. Cyber space gives an easy excess to the terrorists to electronically enter into the devices and take control of the over the system, not only into the lives of the people but also arises threat to national security.

WHAT IS CYBER TERRORISM?

The concept of cyber terrorism originated in the early 1990s, when studies on the hazards faced by the increasingly networked and technologically dependent United States were prompted by the rapid rise of the Internet and the burgeoning "information society" debate.

The term cyber terrorism was first coined in the mid-eighties by Barry C. Collin, a senior person research fellow of the Institute for Security and Intelligence in California (Akhgar et al., 2014). Collin had, at that time, defined cyber terrorism simply as "*the convergence of cybernetics and terrorism*."[1]

Defense analyst Dorothy Denning defines cyber terrorism as: *"Unlawful attacks and threats of 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."*[2]

So the definition of terrorism was concluded with the following components:

1. the unlawful use of terror, violence, or force to instill fear,

[1] Jordan J. Plotnek, Jill Slay, Cyber Terrorism : A Homogenized Taxonomy and definition, Science Direct, https://www.sciencedirect.com/science/article/abs/pii/S0167404820304181
[2] Dorothy Denning, Cyber Security and Cyber Terrorism, Fairleigh Dickinson University Online, https://online.fdu.edu/program-resources/cybersecurity-and-cyber-terrorism/

ISSN: 2582-6433

2. for religious, political, or ideological reasons,
3. targeted against the larger range of society, and
4. it can be committed by governments, non-state actors, or undercover personnel serving on behalf of their respective organizations.

Hence, we can say terrorism is "the illegal use or threatening use of force or violence by a person."

Within the few years of invention of computer applications 1990, there were concerns that the use of computers could be harmful. That year, the National Academy of Sciences released a research report claiming, "*We are at risk. Increasingly, America depends on computers…. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb*."[3]

A clear line of difference between Cybercrime, cyber warfare, and cyber terrorism represent distinct facets of the complex and interconnected world of cyber security.

Cybercrime involves illicit activities conducted by individuals or organized criminal groups with the primary goal of financial gain. This may include activities such as hacking, identity theft, and online fraud, targeting individuals, businesses, or governments.

In contrast, cyber warfare is a state-sponsored or nation-state-driven endeavor that leverages cyber capabilities as a component of military strategy. Motivated by geopolitical or strategic objectives, cyber warfare includes activities like espionage, sabotage, and attacks on critical infrastructure in the context of warfare.

On the other hand, cyber terrorism is characterized by non-state actors, such as terrorist groups or hacktivists, utilizing cyber tactics to advance political, ideological, or religious goals. The primary objective of cyber terrorism is to instill fear, create chaos, or disrupt societal order by targeting critical infrastructure or compromising sensitive information.

While each term encompasses activities in the digital realm, the key distinctions lie in the actors involved, their motivations, and the overarching context within which these actions take place.

[3] Ross Hall, What is the Terrorist Threat in Cyber Space, E-International Relations, July-26-2011, https://www.e-ir.info/pdf/11022

ISSN: 2582-6433

Understanding these differences is crucial for developing effective strategies to counter the diverse and evolving threats in cyberspace.

UNRAVELING THE THREAT OF CYBER TERRORISM IN MODERN TIMES

Cyber terrorism appeals to modern terrorists for several reasons, including its cost-effectiveness compared to traditional approaches. Terrorists only need a computer and an online connection. Terrorists can deliver computer viruses via phone lines, cables, or wireless connections, eliminating the need for physical weapons.

Second, cyber terrorism provides greater anonymity than traditional terrorist means. Terrorists often utilize "screen names" or "guest user" accounts on websites, making it difficult for security officials to identify them and police teams to determine the terrorists' true identities. Cyberspace eliminates physical obstacles, including checkpoints, borders, and customs officials Third, the diversity and quantity of targets is immense. Cyber terrorists may target government, individual, public utility, or private airline computers and networks. Terrorists can exploit loopholes and vulnerabilities due to the numerous and complex targets. Critical infrastructures, including electric power grids and emergency services, are vulnerable to cyber terrorist attacks due to their complex computer systems and inability to eliminate all weaknesses.

Fourth, cyber terrorism may be carried out remotely, which is particularly enticing to terrorists. Cyber terrorism needs less physical training, psychological investment, risk of fatality, and travel compared to traditional forms of terrorism, making it simpler for terrorist organizations to attract and keep adherents.

Lastly if any virus pops up, cyber terrorism possesses the capability to impact a more extensive population compared to conventional terrorist approaches, thereby eliciting increased media coverage—a desired outcome for terrorists.

MOTIVATION

Motivation involves influencing people and their decisions. Cyber terrorism is driven by social, political, and belief factors. Terrorists are motivated by psychological factors to commit acts of

ISSN: 2582-6433

terrorism. Cyber terrorism occurs when individuals or groups have a political or ideological objective that drives their actions.

For instance, the Chinese Republican Army participates in terrorist activity to retain and strengthen political authority.

IMPACT OF CYBER TERRORISM

Cyber terrorism is unique in that it targets both a specific target and a larger audience. Cyber terrorism differs from other forms of terrorism by involving intentional violence against individuals or property, disruption of critical services, fear, bodily injury, severe economic loss, and threats to national security and public safety.

Cyber terrorism occurs when an attack on a computer system results in violence against individuals or property, causing fear, death, or bodily injury. Cyber terrorism aims to create significant economic or financial harm. According to Rollins and Wilson, if terrorists execute a cyber strike, the economy is likely to be the primary goal, with death and destruction as collateral consequence. Terrorist cyber assaults can target CBRN computer network installation. A successful attack on these installations would result in serious economic disruption and harm to civilians, including death and bodily injuries.

As critical infrastructure sectors become more interconnected, cyber terrorists may choose targets that can cause the most impact.

Cyber-attacks by terrorists are likely to target key infrastructure. Cyber strikes in one area might affect other industries. A large-scale terrorist cyber strike can have unanticipated and long-term consequences for other sectors and the country's economy.

WHY SHOULD INDIA WORRY ABOUT CYBER TERRORISM?

The World Economic Forum's 2021 Global Risk Report identifies cyber security failure as a significant challenge for humanity in the coming decade.

With a population of 1.5 Billion, India can be the world's first-largest internet market, after China. India has benefited from technology, but has also been targeted by terrorists who used it to their

ISSN: 2582-6433

advantage.

The misuse of digital technology has led to deadly terrorist attacks in India, such as the URI attack, Pulwama assault, and the devastating 26/11 Mumbai disaster.

The investigation into the Mumbai attack revealed the attackers' widespread use of digital communications. Terrorists gained access to India's map, population, infrastructure, and other information via the internet. They even employed "Google Earth" to carry out their scheme, Indian Rescue and Defense Forces use mobile networks for command and control, as well as social media to follow their movements. In 2020, CERT-In addressed 11,58,208 cyber terrorist threats. These threats included website intrusion and malware propagation, malicious code, phishing, distributed denial of service attacks, website defacements, unauthorized network scanning and probing, ransomware attacks, data breaches, and vulnerable services.

IS INDIA PREPARED TO FACE CYBER TERRORISM?

"Today, the enemy no longer needs to cross the border. He has the ability to target our security systems from beyond the borders. The Defense Minister, Rajnath Singh, stated during the 77th Staff Course at the Defense Services Staff College (DSSC) in Wellington that the changing global power dynamics have exacerbated security issues.[4]

To prepare India to tackle cyber terrorism, the government has taken the following steps:

i. The Defense Cyber Agency is established within the Ministry of Defense. This agency aims to eliminate cybercrime within the Indian Army, Navy, and Air Force.
ii. Cyber Emergency Response Teams (CERTs) are formed.
iii. The National Cyber Coordination Centre (NCCC) was established by the Indian government, marking a significant step forward. It addresses cyber dangers and cyber-terrorism. All CERTs and ISACs would be linked with NCCC to ensure timely and seamless sharing of cyber threat information across stakeholders.
iv. The Indian Cyber Crime Coordination Centre (I4C) was established by the Ministry of Home Affairs (MHA) to combat cybercrime and cyberterrorism.
v. Adequate cyber security measures, including audits, physical checks, and policy

[4] Rajnath Singh, Raksha Mantri Shri Rajnath Singh delivers keynote address at Defence Services Staff College, Wellington, Rajnath Singh, August 29, 2021, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1750207

ISSN: 2582-6433

guidelines, are in place to ensure the strength of the nation's military in cyberspace.

vi. Mock drills and exercises in cyber security are often performed.

vii. To prevent cyber-attacks, internet traffic from India is routed within its boundaries. The methods will be established in partnership with government ministries, ISPs, and NIXI.

viii. The Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) identifies hazardous applications and offers free removal solution.

SOME INTERNATIONAL ORGANIZATIONS

The United Nations has several agencies that seek to address in cyber terrorism, including, the United Nations Office of Counterterrorism, the United Nations Office on Drugs and Crime, the United Nations Office for Disarmament Affairs, the United Nations Institute for Disarmament Research, the United Nations Interregional Crime and Justice Research Institute, and the International Telecommunication Union. Both EUROPOL and INTERPOL also notably specialize on the subject.

Europol and Interpol both specialize in cyber terrorism operations, collaborating on various operations and hosting a combined cybercrime conference every year. Both institutions fight cybercrime, but they function in different ways. Europol establishes and coordinates cross-border operations against cybercriminals in the EU, whilst Interpol assists law enforcement and coordinates actions against cybercriminals worldwide.

CONCLUSION

This threat of security in cyber space arises due to inadequate security measures, leading to dangerous potential consequences that can impact not only individual users but arises a threat to national security. There is a risk that criminal organizations and terrorists may exploit vulnerabilities in cyberspace. It is crucial to identify which of these gaps may be utilized by actors with the intention to instigate violence or cause damage. Cyber terrorists can be identified by monitoring social networks, chat rooms, and other virtual spaces where hackers trade information anonymously.

Numerous research projects have been developed to prevent and mitigate the impact of terrorist and criminal actions. These studies aim to discover modern technologies, tactics, and approaches

ISSN: 2582-6433

related to cyber dangers.

To summarize, it is widely recognized that cyber security is a global responsibility. Each user bears responsibility for cyber security based on their affiliation. To protect against cyber assaults, all network users should contribute to enhancing security systems due to the extensive internal links and dependencies. Efforts should be made to boost cyber protection and security as part of a worldwide strategy, eliminating exceptions and neutralizing threats as much as possible.