ISSN: 2582-6433

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed6th Edition

VOLUME 2 ISSUE 7

 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

AN ANALYSIS OF LAW RELATING TO CYBER TERRORISM IN INTERNATIONAL PERSPECTIVE

AUTHORED BY - SUDHAKAR ROLAN
PHD Research Scholar
Department of Law
University of Rajasthan, Jaipur

Introduction

Cyber crimes are criminal offenses committed using the internet, computer systems, and other forms of technology. The international legal framework for addressing cyber crimes is made up of a variety of international treaties, agreements, and conventions, including:

Budapest Convention on Cybercrime: This is the first international treaty addressing cybercrime, and it provides a framework for cooperation between countries in investigating and prosecuting cyber criminals. It also sets standards for criminalizing cyber crimes and protecting digital evidence.

United Nations Convention against Transnational Organized Crime: This convention addresses organized crime, including cybercrime, and encourages international cooperation in investigating and prosecuting such offenses.

Council of Europe Convention on the Prevention of Terrorism: This convention criminalizes the use of the internet and other technologies for terrorist purposes, such as inciting or recruiting individuals for terrorist activities.

United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances: This convention addresses the use of the internet and other technologies in drug trafficking and related offenses.

ISSN: 2582-6433

International Covenant on Civil and Political Rights: This treaty protects freedom of expression and privacy online, while also criminalizing certain types of hate speech and incitement to violence.

In addition to these international treaties, many countries have developed their own national laws and regulations to address cyber crimes. It is important for countries to have strong legal frameworks in place to address cyber crimes, as these offenses can have serious consequences for individuals, organizations, and national security. International cooperation and coordination are also essential for addressing the global nature of cyber crimes and ensuring that cyber criminals can be brought to justice.

Cyber terrorism refers to the use of the internet, computer systems, and other technological tools to carry out acts of terrorism. Cyber terrorists may use these tools to attack critical infrastructure, cause widespread disruption, steal sensitive information, or spread propaganda and misinformation.

Cyber terrorism can take many forms, including:
Cyber attacks on critical infrastructure such as power grids, transportation systems, or communication networks, which can cause significant disruption and potentially lead to loss of life.

Use of social media and other online platforms to spread propaganda, recruit new members, or radicalize individuals.

Theft of sensitive information such as personal data, financial records, or trade secrets, which can have significant economic and national security implications.

Distributed denial-of-service (DDoS) attacks, which flood a website or network with traffic to render it inaccessible to users.

Ransomware attacks, which encrypt data or systems and demand payment in exchange for the decryption key.

ISSN: 2582-6433

Cyber terrorism poses a significant threat to national security, public safety, and the global economy. Governments, organizations, and individuals must take steps to protect themselves against cyber attacks and ensure the security of their digital infrastructure. This includes implementing strong cybersecurity measures, investing in cybersecurity training and education, and promoting international cooperation to address the global threat of cyber terrorism.

Cyber terrorism is a growing threat worldwide, and many countries have enacted laws to combat it. However, the definitions and legal approaches to cyber terrorism can vary significantly across different jurisdictions.

In general, cyber terrorism can be defined as the use of computers, networks, and the internet to carry out terrorist activities, such as attacks on critical infrastructure or the dissemination of propaganda.

Cyber terrorism laws and regulations from around the world:

United States: The USA PATRIOT Act of 2001 amended existing federal laws to include cyber terrorism as a criminal offense. The law allows for enhanced surveillance and intelligence-gathering activities to prevent and investigate cyber terrorism.

United Kingdom: The UK's Terrorism Act of 2000 includes provisions for prosecuting cyber terrorism offenses. The law defines a cyber terrorist act as an act or threat which involves serious damage to property or endangerment of life, which is intended to advance a political, religious, or ideological cause.

European Union: The EU adopted the Directive on Attacks against Information Systems in 2013, which establishes minimum standards for combating cyber attacks and cyber terrorism. The directive requires member states to establish criminal offenses for cyber attacks and to provide for penalties and sanctions.

China: China's National Security Law, enacted in 2015, includes provisions on cyber security and cyber terrorism. The law requires network operators to cooperate with government agencies to prevent and investigate cyber terrorism, and imposes penalties for cyber terrorist

ISSN: 2582-6433

activities.

Australia: Australia's Criminal Code Act of 1995 includes provisions for prosecuting cyber terrorism offenses. The law defines a cyber terrorist act as an act or threat which involves serious damage to property or endangerment of life, which is intended to advance a political, religious, or ideological cause.

It's important to note that there is no universally accepted definition of cyber terrorism, and different countries may have different interpretations and approaches to combating it. Additionally, there may be challenges in prosecuting cyber terrorism offenses due to the anonymity and global nature of the internet.

Cyber Terrorism Laws And International Organisations

International organizations also play a critical role in addressing cyber terrorism and promoting cybersecurity. Here are some examples of international organizations and their efforts to combat cyber terrorism:

United Nations: The United Nations (UN) has been actively engaged in addressing cyber threats and terrorism through its various entities, such as the UN Office of Counter-Terrorism (UNOCT) and the UN Interregional Crime and Justice Research Institute (UNICRI). The UN has also developed several cybersecurity frameworks, such as the UN Guiding Principles on Business and Human Rights, which outlines guidelines for businesses to respect human rights online.

Council of Europe: The Council of Europe has developed the Budapest Convention on Cybercrime, which is the first international treaty to address cybercrime and cyber terrorism. The convention provides a legal framework for countries to cooperate and address cybercrime, including cyber terrorism.

European Union: The European Union (EU) has established the European Cybercrime Centre (EC3) to combat cybercrime, including cyber terrorism. The EU has also developed the Network and Information Security (NIS) Directive, which aims to improve the security and resilience of critical infrastructure across the EU.

ISSN: 2582-6433

North Atlantic Treaty Organization: The North Atlantic Treaty Organization (NATO) has recognized the growing threat of cyber terrorism and has established a Cyber Defense Center of Excellence to promote cooperation and information-sharing among member countries.

International Criminal Police Organization: The International Criminal Police Organization (INTERPOL) has developed a Global Cybercrime Programme to enhance law enforcement cooperation and capacity-building to combat cybercrime and cyber terrorism.

These international organizations and their efforts are crucial in promoting international cooperation and addressing the global threat of cyber terrorism.

Cyber terrorism laws are important for several reasons:

Protection of National Security: Cyber terrorism poses a significant threat to national security, and laws are needed to ensure that law enforcement agencies and intelligence services have the necessary legal tools to prevent and investigate such activities.

Prevention of Cyber Attacks: Laws that criminalize cyber terrorism can act as a deterrent to potential attackers, helping to prevent cyber attacks before they occur.

Accountability and Punishment: Laws that define and criminalize cyber terrorism ensure that those who commit these crimes can be held accountable and punished accordingly.

International Cooperation: Cyber terrorism is a global threat, and international cooperation is essential for addressing it. Laws that define cyber terrorism and establish international standards for prosecuting cyber terrorists can facilitate cooperation between countries and promote a coordinated response to this threat.

Protection of Critical Infrastructure: Cyber attacks on critical infrastructure, such as power grids or communication networks, can have serious consequences. Laws that define and criminalize cyber terrorism can help ensure the security of critical infrastructure and prevent attacks that could result in widespread disruption or even loss of life.

In summary, cyber terrorism laws are necessary to protect national security, prevent cyber

ISSN: 2582-6433

attacks, hold cyber terrorists accountable, promote international cooperation, and protect critical infrastructure.

Cyber threats pose a significant risk to security agencies, including law enforcement and intelligence agencies, as they are responsible for protecting sensitive information and critical infrastructure. Here are some ways in which security agencies can be vulnerable to cyber threats:

Cyber Attacks: Security agencies are susceptible to cyber attacks that can steal sensitive information, disrupt operations, or damage infrastructure. Cyber attacks can take many forms, such as malware, phishing, and ransomware attacks.

Insider Threats: Security agencies may also face threats from insiders, such as employees or contractors, who have access to sensitive information and may use this access to steal or leak data.

Social Engineering: Social engineering attacks, such as pretexting or baiting, can be used to trick security agency employees into divulging sensitive information or granting unauthorized access to systems.

Vulnerabilities in Legacy Systems: Many security agencies still rely on legacy systems that may be outdated and vulnerable to cyber attacks. These systems can be easy targets for attackers seeking to exploit known vulnerabilities.

Lack of Cybersecurity Training: Many security agency employees may not receive adequate training in cybersecurity best practices, leaving them vulnerable to social engineering attacks or other cyber threats.

Given these risks, security agencies must prioritize cybersecurity and take steps to protect their systems and information. This includes implementing strong cybersecurity measures, such as multi-factor authentication and encryption, regularly updating software and systems, conducting regular security assessments, and providing regular cybersecurity training to employees.

ISSN: 2582-6433

Supreme court of USA on cyber terrorism

The Supreme Court of the United States has not issued any specific rulings on cyber terrorism, as there is no federal law that specifically defines cyber terrorism as a criminal offense. However, the Court has considered cases involving cybercrime and related issues.

In the 2008 case of United States v. Drew, the Court considered the case of a woman who created a fake MySpace account to harass and bully a young girl who later committed suicide. The Court held that Drew's conduct violated federal criminal statutes, including the Computer Fraud and Abuse Act (CFAA) and the Wire Fraud statute.

In the 2018 case of Carpenter v. United States, the Court held that law enforcement agencies must obtain a warrant to access historical cell-site location information from mobile phone providers, as this information constitutes a "search" under the Fourth Amendment of the U.S. Constitution.

While these cases do not specifically address cyber terrorism, they illustrate the Court's willingness to consider the impact of technology on criminal law and the importance of protecting individual privacy and security in the digital age. It is likely that the Court will continue to address cybercrime and related issues in future cases as technology continues to evolve and shape our society.

Reference:

- Vakul Sharma, Information Technology: Law and Practice, Universal Law Publication Co., New Delhi 2010
- Justice Yatindra Singh, Cyber Laws, Universal Law Publishing Co. Pvt. Ltd., 2010.
- Bary C. Collin, The Future of Cyber Terrorism, University of Illinois, Chicago, 1996.
- Dan Verton, Black Ice: The Invisible Threat of Cyber-Terrorism (New York: McGraw-Hill, 2003).
- Alexander, Y. (2002). Combating terrorism: strategies of ten countries. University of Michigan Press
- Gabriel Weimann, Terror on the Internet: The New Arena, the New Challenges (Washington, D.C., United States Institute of Peace Press, 2006)

ISSN: 2582-6433

- Scott Gerwehr and Sarah Daly, "Al-Qaida: terrorist selection and recruitment", in The McGraw-Hill Homeland Security Handbook, David Kamien, ed. (New York, McGraw-Hill, 2006)
- Michael Chissick, and Alistair Kelman, Electronic Commerce- Law and Practice, Sweet & Maxwell, London, 2000
- M. Gercke et al, Terrorist Use of the Internet and Legal Response, Freedom from Fear, Aug 2011, available at http://www.freedomfromfearmagazine.org/index.php?option¼com_content&view¼article&id¼306:terrorist-use-of-the-Internet-andlegal response&catid
- T. Oba, "Cyberterrorism seen as future threat," Computer Crime Research Centre Tech. Report, April 2004, http://www.crime-research.org/news/2003/04/Mess0103.html
- Z. Sütalan, "Current and future trends in terrorism," COE-DAT Newsletter vol.3 issue.16 p.37-49, July-September 2010.
- N. Muddaraju and Ramesh, "Cyber Crimes: Need an Effective Law", pp. 227-31, Criminal Law Journal, 2009 Aug