INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 2 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

CYBER TERRORISM: A THREAT TO NATIONAL SECURITY

AUTHOR - JASHVI DODHIA, STUDENT AT MKES COLLEGE OF LAW

BEST CITATION - JASHVI DODHIA, CYBER TERRORISM: A THREAT TO NATIONAL SECURITY, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (2) OF 2025, PG. 56-60, APIS – 3920 – 0001 & ISSN - 2583-2344.

This article is published in the collaborated special issue of M.K.E.S. College of Law and the Institute of Legal Education (ILE), titled "Current Trends in Indian Legal Frameworks: A Special Edition" (ISBN: 978-81-968842-8-4).

ABSTRACT

Information technology has opened doors of opportunity for the world by creating multiple sources for the growth of people's financial infrastructures. With over 900 million internet users, India was the second largest online market in the world, behind China.[72] Cyberspace runs in the veins of modern digital transactions, businesses, and other essential services. But where there is power, there will be misuse of power. With the invention of cyberspace, there has also been an increase in cybercrimes. Criminals use many tactics to scam people and extort money from them. There is a lot of unawareness and ignorance among the citizens, due to which people get scammed. The slow process of the executive and judiciary also adds to the cybercrimes every day. One of the most recent types of cybercrime is digital arrest. Due to people's lack of knowledge and awareness, they think that one can be digitally arrested now and become vulnerable and end up falling into the traps of these criminals. Cyberattacks have the tendency to depict lethal, non-lethal, and psychological well-being of the citizens, public confidence of the government bodies, and political attitudes of the parties. Even terrorist groups use cyberspace to achieve their motives. Cyber terrorism imposes a threat on national security.[73]

Keywords: Cyber Crime, cyber terrorism, cyber law, Information Technology Act, 2000

[72] https://www.statista.com/topics/2157/internet-usage-in-india/

[73] Shiv Raman, Nidhi Sharma, Cyber Terrorism in India: A Physical Reality or Virtual Myth, 5, 2, (special issue) IJLHR, 133-135, 2019, https://journals.indexcopernicus.com/api/file/viewByFileId/783266.pdf.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 2 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Introduction

One of the most threatening forms of cybercrime in today's world is cyber terrorism. As the name suggests, cyber terrorism means "unlawful attacks or threats of exploitation through computers, networks, and locations with the intent of intimidating or humiliating a person or persons of a nation or nations to achieve political or social goals."

Barry Collin was the first person to use the word "cyber terrorism" in the 1980s.[74] According to him, cyber terrorism is "the international abuse of a digital information system, network, or component toward an end that supports and facilitates a terrorist campaign or action." Pollitt (1998) defined "cyber terrorism as a premeditated, politically motivated attack against information, computer systems, computer programmers, and data that results in violence against noncombatant targets by subnational groups or clandestine agents."

It is an attack without the use of arms and ammunition but can have the same impact on a nation. The nature of the cyber terrorism can be international, domestic, or even political. Cyber warfare might replace traditional forms of war and make cyberspace a battleground of the future and will create even greater amount of destruction in the world.

Cyber terrorism requires publicity and a forum of communication, as it is a politically motivated act. Cyberspace offers political areas to the terrorist organizations to be exploited. It is used as a tool to spread personal propaganda by generating media attention.[75]

Threat to National Security

India is one of the fastest-growing digital technology marketplaces. Due to the government's efforts, there is a drastic change of businesses and organizations going digital. This brings cybersecurity issues in the country, which poses as threat to the country's national security.

Many governmental organizations and large businesses hold secretive information like power and transportation networks, military databases, aviation, etc., which are frequently dependent on technology. There can be potential disruption if any information reaches the attackers. A successful cyberattack can have far-reaching consequences. For example, if there is a successful cyberattack on digitalized power supply systems, it can lead to disruptions in energy delivery, compromised operational control, and data breaches. [76]

On October 30, 2019, the Kudankulam Nuclear Power Plant near Kanyakumari had been a target of a cyberattack. The attack was unsuccessful. But if the attackers got access to the OT network, then it could have escalated their privileges to a level where they could send control commands that would cause harm to national security. For instance, in the Stuxnet case in 2010 where the attackers were able to target nuclear centrifuges in Iran.[77]

Kinds of Cyber Terrorism

Many cybersecurity professionals agree that an incident can be called as cyber terrorism if it causes fatalities or bodily harm, either direct or indirect. Usually, there is no necessity of physical injury for the attack to be referred to as cyber terrorism. A cyberattack that uses or exploits computers or communication networks to create "sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal" can be referred as cyber terrorism by NATO.[78]

[74] https://repository.law.uic.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1091&context=jitpl

[75] Aditya Kumar & Dr. Anand K. Singh, Cyberterrorism in India: A Novel Facet in the Warfare Domain, 10, Issue 12, JETIR a63-64, https://www.jetir.org/papers/JETIR2312009.pdf.

[76] Chayanika Choudhury, Cyber Security Concerns: A Threat to India's National Security, Modern Diplomacy (Feb 17, 2023), https://moderndiplomacy.eu/2023/02/17/cyber-security-concerns-a-threat-to-indias-national-security/.

[77] Kartik Palani & Prashant Anantharaman, What Happened when the Kudankulam nuclear plant was hacked- and what real danger did it pose?, Scroll.in (Nov 20,2019, 6:30 am), https://scroll.in/article/943954/what-happened-when-the-kudankulam-nuclear-plant-was-hacked-and-what-real-danger-did-it-pose.

[78] (NATO) North Atlantic Treaty Organization, 1949.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 2 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Advanced Persistent Threat (APT) attacks

APT attackers obtain network access using focused and sophisticated penetration techniques. Once they are within the network, attackers attempt to steal data while they are yet undiscovered. They often target organizations with highly valuable information like national defence, manufacturing, and financial sectors.

Malware

Malware is specifically designed to damage, disrupt, or gain unauthorized access to a computer system. Attackers are employed to access military systems, transportation networks, power grids, and critical infrastructure by specifically targeting IT control systems.

Denial of Service (DoS) Attacks

Attackers restrict bar authorized users from accessing specific computer systems, devices, and other computer networks. They usually target government and vital infrastructures.

Hacking-

Hackers attack government websites, commercial enterprises, and military information to gain unauthorized access to collect fragile data, which can cause a threat to national security. Many hackers collect information illegally and sell it on dark web for millions.

Ransomware-

Data and information are kept hostage until the victim pays hefty amounts as ransom. Some ransomware assaults exfiltrate data.

Phishing-

When attackers gather information from the victim's email and use it to gain access to other systems or steal the victim's identity.

Spoofing-

When a computer or a person effectively identifies as another by faking information to obtain an unfair advantage. It causes a major threat to information security, particularly network security.[79]

Initiatives by Government-

The Indian Computer Emergency Response Team (CERT-In)

The CERT-In operates as a national agency for the protection of the country's cybersecurity. Its function encompasses varying from cyber security audits, cybersecurity awareness programs, and giving out advisories for improving the cybersecurity landscape of India.[80]

Cyber Surakshit Bharat-

CSB was commenced by the Prime Minister in 2018 to ensure the safety and security of government officials and organizations by developing cybersecurity awareness.

National Critical Information Infrastructure Protection Centre (NCIIPC)-

NCIIPC was formed by the central government to protect critical information about the nation, which can have an impact on national security, economic growth, and public health care.

Appointment of Chief Information Security Officers-

The Government of India published a written guideline for appointment of CISOs of government organizations, outlining best practices for safeguarding apps, infrastructure, and compliance.

Digital Personal Data Protection Act, 2023

The Act stores and processes any critical information related to the citizens of India. It aims to make social media companies more responsive and accountable for the spread of offensive content and misuse of data. Before

[79] Kerem Gulen, The war never ends on the cyber front, Data Conomy (Oct 11, 2022), https://dataconomy.com/2022/10/11/cyber-terrorism-definition-attacks/.

[80] https://www.cert-in.org.in/

this enactment, protection of data was dealt under the Information Technology Act, 2000[81]

Cyber Swachhta Kendra (Bonet Cleaning and Malware Analysis Centre)

The Cyber Swachhta Kendra works in collaboration with the internet service providers and antivirus/product companies. It offers a secure cyberspace by diagnosing and preventing devices from experiencing a malware attack.[82]

Indian Cybercrime Coordination Centre

The Ministry of Home Affairs founded the Indian Cybercrime Coordination Centre to manage cybercrime-related issues. The scheme for this Centre was sanctioned on October 5, 2018, to address cybercrime that demands a concerted effort among various stakeholders. The Centre's mission is to combat cybercrime in the nation in a coordinated and effective manner.[83]

National Cyber Security Policy, 2013

The policy has been a framework for India to start its operations against cyberspace threats. It defines the roles of various parties in promoting a secure cyberspace.[84]

Legal Provisions

Information Technology Act, 2000[85]

The Information Technology Act, 2000 has a domain of cyber law in India and addresses various types of cybercrimes. The Information Technology Act 2000 is applicable to the whole of India, including any offense committed from out of India, if such breach involves a computer, computer system or computer network located in India. India with the adoption of information technology Act has entered the coveted world of the few countries that have separate law to deal with information technology issues.[86] It was amended in the year 2008 to incorporate cyber terrorism. Section 66F[87] penalizes any act that threatens the unity, integrity, security, or sovereignty of India.

Unlawful Activities (Prevention) Act, 1967[88]

The Act provides a framework for dealing with activities like cyber terrorism that threaten the sovereignty and integrity of the nation.

Indian Penal Code, 1860

The Indian Penal Code, 1860 does not specifically include any provisions for cyber terrorism but has certain provisions that can aid in the prosecution of cyber terrorism cases.[89]

Bhartiya Nyaya Sanhita, 2023

Bhartiya Nyaya Sanhita, 2023 does not include any specific punishments regarding cyber terrorism. But it has provisions for other cyber offenses and can still be used as an abatement for punishment of cyber terrorism.

Conclusion

Through cyberattacks, traditional concepts and methods of war and terrorism have taken new dimensions. These methods can prove to be more disruptive and deadly in nature. India is way back in providing cybersecurity to its citizens and making sure their personal information does not get leaked and misused by other countries. But in the recent years, the government has made many changes by which there are fewer cyberattacks happening. In 2020, the Indian government banned 59 Chinese apps, accusing China of breaching data privacy and using Indian citizens' data to keep a track on them. The ongoing attack on India's power grids also may have been a part of China's cyber espionage strategy to gather

[81] Kolekar, Y.P. (2015), Protection of Data under Information Technology Law in India, 27 April, 1-12. Available at SSRN: http://ssrn.com/abstract=2599493.
[82] https://www.csk.gov.in/
[83] https://ijlr.iledu.in/wp-content/uploads/2024/11/V4I433.pdf
[84] List of Cybersecurity Initiatives by the Government of India, StrongBoxIT, https://www.strongboxit.com/list-of-cybersecurity-initiatives-by-the-government-of-india/.
[85] As amended in 2008.
[86] Kolekar, Yogesh. 2015. "A Review of Information Technology Act, 2000." Available at SSRN 2611827.
[87] Punishment for cyber terrorism.
[88] As amended in 2019.
[89] Pankaj Kumar Srivastava, Cyber Terrorism: Threats and Responses in the Context of Indian Law, 12, INT-JECSE, 506, 511-512 (2020), https://www.int-jecse.net/media/article_pdfs/Cyber-1-1.pdf.

intelligence on the country's critical infrastructure.[90]

Due to the ongoing scams in India, the government has taken an initiative to add a prerecorded message instructing the citizens to be aware and safe from these types of scams. Two new numbers, 160 and 161, are to be allotted to banks only to prevent people from being scammed by people impersonating bank employees and asking for card details, OTP pins, etc. Recently, agencies blocked thousands of fraudulent SIM cards, mobile phones, and many bank accounts that were used in the operation of such scams. People also need to act more responsibly and aware of cyber terrorism so that they don't fall into the trap of attackers.

[90] Aditya Kumar & Dr. Anand K. Singh, Cyberterrorism in India: A Novel Facet in the Warfare Domain, 10, Issue 12, JETIR a63, a68, https://www.jetir.org/papers/JETIR2312009.pdf.