ISSN: 2582-6433

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed6th Edition

VOLUME 2 ISSUE 7

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

Byte Is The New Bomb: A Critical Analysis Of The Situation Of Cyber Terrorism In India

Authored By-1. Harshitaa Arora
2. Charvi Singh
3. Akshat Kalra

Abstract

The public is blessed by the reality of cyberspace. On the other hand, when it is used improperly with foul intentions, it proves to be one of the most dreadful technological breakthroughs ever. Although terrorism has existed since the beginning of time, with the advancement of technology, conventional terrorism has found its way into the cyberspace and is now a way for terrorists to disrupt the peaceful coexistence of nation states. Cyberterrorism harms emerging nations like India and has the potential to completely devastate an economy and administrative structure. Since the first cyberattack, termed "Digital Pearl Harbor" in 1990, there have been an increasing number of cyberattacks that have successfully disrupted the national peace and security of practically all countries. Almost all governments are investing their time and effort developing strict regulations to safeguard their country since it poses a threat to national security. Following the 26/11 attack in Mumbai, which led to the acknowledgment of terminology like "cyberwarfare" and "cyberterrorism," India too has undertaken various measures to combat this atrocity. Combating the overt and covert actions of cyber terrorism, however, is a challenge to the state apparatus as opposed to a typical criminal justice endeavour. This paper tries to concentrate on the theoretical underpinnings of cyberterrorism. It further clarifies if Indian laws have been able to control the rising number of cyberterrorism incidents in India.

Keywords – Cyber, Terrorism, Internet, Information technology, Crime.

ISSN: 2582-6433

Hypothesis

The researcher is convinced that, just as technology is developing, so are the tactics used by terrorists to undermine a nation's national security. The government must not only make new policies and alter old ones, but also strictly enforce them. The internet has been weaponized, and terrorists and their followers frequently utilise it to incite hatred among the populace and encourage them to follow their leaders. A targeted piece of legislation that regulates cyberspace and strengthens the nation's cybersecurity measures is necessary.

Methodology

The document-based and analytical approaches are used in this paper. Majority of the literature was gathered from research journal, newspaper, publications, weeklies, fortnightly magazine, government report, Information Technology Act 2000, Information Technology Act 2008, reports published by Cyber security authorities, etc.

Introduction

"Just as a modern thief can steal more with a computer than with a bag, tomorrow's terrorist may be able to cause more damage with a computer mouse than with a bullet or a bomb." – National Research Council

Terrorism has existed throughout human existence.[1] Currently, terrorism poses a menace to every nation in the world.[2] It has overtaken the entire world and presented the world with an extraordinary dilemma. Because of terrorism, many individuals have lost their lives, families, and assets. It has had an impact on people's lives as well as the development and growth of the economy, society, and politics.[3] The development of Information and Communication Technology (ICT) has given the evil of terrorism a great deal of power to carry out deadly acts.[4] In 1990, the first cyberattack, popularly known as "Digital Pearl Harbor"[5] was experienced and warned about by the National Academy of Sciences.

[1] Weingberg, L. (2006) Global Terrorism: A Beginner's Guide, 1st Ed., London, UK: One World Publication.
[2] Halder, D. (2011) Information Technology Act and Cyber Terrorism: A Critical Review, SSRN 1964261 [Online] Available from: https://papers.ssrn.com/sol3/papers. cfm?abstract_id=1964261.
[3] Laquer, W. (1987) The Age of Terrorism, 1st Ed., Boston, USA: Little, Brown and Company.
[4] Ramsay, G. (2008) Conceptualising Online Terrorism, Perspective on Terrorism, 2(7), pp: 3–10.
[5] Weimann, G. (2004) Cyberterrorism: How Real is the Threat? [Online] Available from: https://www.usip.org/sites/default/ files/sr119.pdf

ISSN: 2582-6433

Cyberterrorism, which was in its infancy over two decades ago, is now a terrible threat that has caught everyone off guard.

A Southern Poverty Law Centre expert named Mark Potok stated[6]: "The internet is a crucial component of the decentralised struggle strategy. It enables lone wolves to stay updated about acts, changes in philosophy, and discussions of tactics — all of which may have an impact on his individual target selection. The internet, more so than print media, enables the lone wolf to continue to be a part of a larger movement despite attending no meetings, putting his name on no lists, and generally attempting to blend in. An excellent illustration of this is Mathew Williams, the confessed killer of a gay couple in California, who, prior to pulling the trigger, discreetly researched a number of radical ideas on the internet"[7].

Many of the terrorist organisations on the US State Department's list operate websites using labelled domain names. The majority of the group tends to use the internet to propagate their ideology, while US officials suspect that some of those terrorist groups used encrypted emails to plot terrorist attacks[8]. A computer hacker who destroyed a portion of a US-based Internet Service Provider's (ISP) record-keeping system in 1996 forced the ISP to shut down, signing off with a threatening message that stated "***you have yet to witness actual electronic terrorism. This is a promise***"[9]. In 1998, when the Euskal Herria Journal, a New York-based journal that supported Basque in independence, had a website hosted by the Institute for Global Communication (IGC), Spanish protestors assaulted the IGC with thousands of spurious emails demanding that they remove the website.[10] The warning in the hundreds of emails sent daily by the ethnic militants to Sri Lankan embassies said, "***We are the internet black Tigers and are going to disrupt communication***". According to reports, it was the first known terrorist cyberattack on a nation's computer network. In 1999, during the conflict in Kosovo, denial of service assaults and an onslaught of emails were directed at NATO computers.[11]

[6] Singh, V. P. (2021). Cyber terrorism and Indian legal regime: a critical appraisal of Section 66 (F) of the Information Technology Act. Sri Lanka Journal of Social Sciences, 44(1), 71-81.
[7] Sue, P. Griest & Mahan, S. (2003) Terrorism in Perspective, 1st Ed., California: Sage Publications Inc.
[8] Ramsay, G. (2008) Conceptualising Online Terrorism, Perspective on Terrorism, 2(7), pp: 3–10.
[9] Singh, V. P. (2021). Cyber terrorism and Indian legal regime: a critical appraisal of Section 66 (F) of the Information Technology Act. Sri Lanka Journal of Social Sciences, 44(1), 71-81.
[10] Mali, P. (2012) Cyber Law and Cyber Crime, 1st Ed., New Delhi: Snow White Publishers.
[11] Ibid

ISSN: 2582-6433

Conceptualizing Cyber Terrorism

The idea of cyber-terrorism can be traced back to the early 1990s, when the utilization of the Internet was rapidly increasing and conversations about the 'information society' were in full swing. At that time, numerous studies were conducted on the potential threats facing the United States which was at that time increasingly networked and heavily reliant on high tech. Although there may not be a physical threat from cyberterrorism, its psychological consequences on vulnerable communities are just as devastating as terrorist explosives.[12] In the current day, one of the most important economic and national security challenges that a nation faces, in the opinion of former US President Barack Obama, is the cyber threat.[13]

In the midst of the 1980s, Barry C. Collin, a senior person research fellow at the Institute for Security and Intelligence in California[14], first coined the term "cyber terrorism". Collin's definition of cyber terrorism at the time was simply "the intersection of cybernetics and terrorism"[15]. It most definitely is a broad term. The process of creating a precise and unified definition of the term "cyberterrorism" has run across a number of obstacles. The majority of the discussion around cyberterrorism has occurred in the mainstream media, where journalists are more intrigued by the drama and controversy than in providing a uniform and practical definition to the newly discovered terms. Additionally, it has become increasingly common for people who use computers to create new phrases by simply prefixing them with "cyber", "computer", or "information". As a result, a plethora of terminology, including cyberterrorism, cybercrime, cyber-tactics, cyberattack, and cyber-break-ins, are used to define what some political strategists refer to as "new terrorism" of our times.[16]

[12] Weimann, G. (2004). Cyberterrorism: How real is the threat? (Vol. 119). United States Institute of Peace.
[13] Obama, B. (2009, May 29). Remarks by the President on Securing Our Nation's Cyber Infrastructure | whitehouse.gov. Whitehouse.Gov; obamawhitehouse.archives.gov. https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure
[14] Akhgar, B., Staniforth, A., & Bosco, F. (2014, July 14). Cyber Crime and Cyber Terrorism Investigator's Handbook - 1st Edition. Cyber Crime and Cyber Terrorism www.elsevier.com.https://www.elsevier.com/books/cyber-crime-and-cyber-terrorism-investigators-handbook/akhgar/978-0-12-800743-3
[15] Plotnek, J. J., & Slay, J. (2021). Cyber terrorism: A homogenized taxonomy and definition. Computers & Security, 102, 102145.
[16] Alık, N. A. H. A. (2022). Emerging Cyber Security Threats: India's Concerns and Options. International Journal of Politics and Security, 4(1), 170-200.

ISSN: 2582-6433

All acts of cyberterrorism are cybercrimes but not all cybercrimes are acts of cyberterrorism.[17]

It would be erroneous to assume that cyber terrorism is a brand-new category of cybercrime since some studies have determined that an act of cybercrime encompasses two main sorts of activities: cybercrime and misuse of information technology[18]. While all cyberterrorism incidents are cybercrimes, not all cybercrimes may be categorised as cyberterrorism, which is an important distinction to make. Acts of cyberterrorism may only be defined as cybercrimes that have political or ideological motivations. An example of this distinction can be incident that took place at the Maroochy Shire Waste Water Plant in Sunshire Coast City, Australia where in order to express his discontent with the company's promotion policies, an engineer compromised the computers that ran the business in 2000.

As a result, millions of tonnes of sewage water were released into the city's parks and seashore, severely harming the ecosystem. It was incorrectly referred to as a cyberterrorist attack because it was not intended to cause harm to general public or disrupt nation's peace and security i.e., the idea was not politically motivated. Nevertheless, it was a serious cybercrime.[19]

Today's cyber terrorists' primary goal is to employ cyberattacks to destroy a nation's vital infrastructure in order to advance the causes they support as a terrorist organisation. Their wish lists include essential infrastructure such as banking and finance, water supply, fuel production and supply chains, military complexes, government operations, and emergency services.

Cyber Terrorism In India

India is no longer delusional about cyberterrorism.[20] The Anti India Crew (AIC) of Pakistan infiltrated the websites of India on April 2, 2002, and attempted to wipe and obliterate all of the data contained on the computer systems and computer networks of 88 websites[21], including the websites run by Indian Government.[22] The horrifying 26/11 Mumbai attack is a stark illustration

[17] Pujari, A. (n.d.). Cyber Terrorism: World Wide Weponisation. cii.in., Tamil Nadu Police Sesquicentennial Anniversary Souvenir, (2017).
[18] Schjolberg, S. (2007) Terrorism in Cyberspace - Myth or reality? http:// www.cybercrimelaw.net/documents/Cyberterrorism.pdf
[19] Pujari, A. (n.d.). Cyber Terrorism: World Wide Weponisation. cii.in., Tamil Nadu Police Sesquicentennial Anniversary Souvenir, (2017).
[20] India Risk Survey, 2018, Available From: https://ficci.in/SEDocument/20450/India%20Risk%20Survey%20-%202018.pdf
[21] Saxena, A. (2011) 117 Indian Government Websites Defaced Till July, Medianama [Online] Available from: https://www.medianama.com/2011/08/223-indiangovernment-websites-hacked/
[22] Bhansali, S. (2012) Commentary on Information Technology Act, 1st Ed., New Delhi: Universal Publication.

ISSN: 2582-6433

of how terrorists' use of ICT made it challenging for Indian security officials to identify and apprehend these culprits.[23] The ICT was misused in the Zaveri bombing on July 13, 2010. ICT was also used for communication during the 2010 Varanasi bombing[24]; the Indian Mujahidin claimed responsibility for the explosion via e-mail, which was linked to a WiFi connection in Vashi, Navi Mumbai.[25] In the Pulwama incident that took place on February 14, 2019, the suicide bomber from Jaish Mohammad used virtual SIM cards.[26] In the end, cyberspace has turned into a battlefield and a base for terrorist activities. The terrorist group views cyber-attacks as an effective jihadi tool for waging war against their adversaries. Terrorist organisations have become adept at abusing the online environment.[27]

How Vulnerable Is India To Cyber Terrorism

How susceptible are we to the possibility of cyberterrorism is the issue that gets raised very frequently. The degree to which a nation's critical infrastructure depends on networks strongly relates to that nation's susceptibility to cyber threats. India is on a path of ardent digital revolution. With over 1.2 billion users, the nation had the second-largest internet population in the world in 2020. Of these, 750 million users used their mobile phones to access the internet. India will have 1 billion smartphone users by 2026, according to a Deloitte report[28]. According to the DBS Digital Readiness survey conducted in 2021, almost 62% of large and middle-market enterprises in India are still in the early phases of digitalization. DDoS assaults (77%) and cloud infrastructure security (76%) were cited by more than half of major enterprises and middle-market companies as the most pressing cybersecurity threats[29].

[23] Oh, O., Agarwal, M. & Rao, H. R. (2011) Information control and terrorism: Tracking the Mumbai terrorist attack through twitter, Information Systems Frontiers, 13(1), pp: 33–43 [Online] Available from: https://link.springer.com/content/pdf/10.1007/s10796-010-9275-8.pdf

[24] Hani, N. M. & Ranjan, A. (2018) A Critical Study on Cyber Terrorism with Reference with 26/11 Mumbai Attack, International Journal of Pure and Ranjan, Aswathy, 119(17), pp: 1617–1636.

[25] Ibid

[26] Press Trust of India, 2019

[27] Dhar, P. (2017) Changing dimensions of criminal jurispudence in virtual reality: a critical evaluation of information technology laws, 'cybercrimes and crimes per se' in India, Bharati Law Review, 6(2), pp: 117–130.

[28] Kumar, B., & Vanamali, K. V. (2022, March 10). Is India prepared to protect itself from cyber-attacks? | Business Standard News. Is India Prepared to Protect Itself from Cyber-Attacks?; www.business-standard.com. https://www.business-standard.com/podcast/technology/is-india-prepared-to-protect-itself-from-cyber-attacks-122031000062_1.html

[29] Digital Readiness Survey, DBS. (2021, September 21). Indian large corporates and middle-market companies are focused on digital transformation as a priority, finds DBS survey. Indian Large Corporates and Middle-Market Companies Are Focused on Digital Transformation as a Priority, Finds DBS Survey; www.dbs.com. https://www.dbs.com/newsroom/indian_large_corporates_and_middlemarket_companies_are_focused_on_digital_transformation_as_a_priority_finds_dbs_survey

ISSN: 2582-6433

These are significant figures that demonstrate the size of the cyberspace that India must protect. The attackers are "demonstrating same level of online expertise as by US government agencies," according to a report CRS (Congress Research Service) given to US Congress[30]. According to the same report, Al-Qaeda has established web forums where its cadres can learn how to hack computers, how to make bombs, etc. Cyber terrorism has taken on a completely new dimension with the employment of cyber technology by some countries' intelligence services for not only snooping but also for undermining the vital infrastructure of other nations.

Cyber Security And Legislative Measures

One can define Cyber security as "***The collection of tools, policies, guidelines, training, actions, security concepts and safeguards, risk management approaches, assurance, and technologies that can be used to secure and protect the cyber environment as well as the organizations and user assets***"[31].

Its objectives include limiting unauthorised access to information, preventing inadvertent alteration or loss of information, and protecting networks, data, computer programmes, and information technology. In a world where sophisticated communication and technological infrastructure are essential to security and economic success, making the use of Internet safe and secure is becoming more and more crucial to government policy[32]. Joseph Migga Kizza has defined cyber security as having three components—***confidentiality, integrity, and availability***[33].

Information Technology Act, 2000

Several governments implemented specialised laws to control online commerce and related e-governance after the United Nations Commission on International Trade Legislation (UNICITRAL)[34] model law on e-commerce was released in 1996. To integrate key sections of the UNICITRAL model law on e-commerce, the Indian parliament passed the Information

[30] Pujari, A. (n.d.). Cyber Terrorism: World Wide Weponisation. cii.in., Tamil Nadu Police Sesquicentennial Anniversary Souvenir, (2017).
[31] Sushma Devi Parmar. "Cybersecurity in India: An Evolving Concern for National Security." The Journal of Intelligence and Cyber Security 1, no.1 (2018).
[32] Marco Gercke. Understanding Cybercrime: A Guide for Developing Countries. (Geneva: ITU Publication, 2009).
[33] Kizza, J. M. (2014). *Computer network security and cyber ethics*. McFarland, 120.
[34] UN. (1996). "UNCITRAL Model Law on Electronic Commerce Guide to Enactment with 1996 with Additional Article 5 as Adopted in 1998." www.uncitral.org/pdf/english/texts/electcom/05- 89450_Ebook.pdf

ISSN: 2582-6433

Technology Act, 2000.

A close examination of the 26/11 attack in Mumbai[35] would reveal that the terrorists' use of the internet for communication and for learning about their target demographic and the location led to catastrophic outcomes in India. As a result of this, the Indian government took decisive action to improve cyber security, including revising the Indian Information Technology Act, 2000 to outlaw terrorist activity online.

The following examples are used to support the claim that, despite the modified IT Act of 2000's pledge to guarantee cyber security and the protection of data, particularly sensitive personal data, the law's provisions still have gaps.

a) In the Varanasi bombing case of 2010, the Indian Mujahiddin also made use of cyberspace to spread their message[36].
b) In July 2011, explosive attacks in a busy city market in Mumbai's Jhaveri Bazaar were also carried out using digital technology[37].
c) One of the largest cyberattacks on banking systems in history was the one that targeted Indian banks in 2016. About 6 lakh debit card details, including PINs, were stolen as part of a mass cybercrime. Also mentioned by victims was the unauthorised use of their credit card information coming from Chinese locations. SBI, YES Bank, and Axis Bank were the three banks that were most severely impacted.[38].
d) d) In 2018, 200 official government websites unintentionally published private Aadhaar data; the issue got so bad that one could easily access thousands of government databases containing sensitive information by just surfing Google for it[39]. Because unauthorised government employees were accessing Aadhaar data, the Indian Government was forced to restrict

[35] Desai, D. D., & Bhatt, P. (2019). Securing India's cities: Remembering 26/11, learning its lessons. Observer Research Foundation, Special Report, (92).
[36] Sharma, R. (2010, December 20). Signals From the Varanasi Blast – The Diplomat. Signals From the Varanasi Blast; thediplomat.com. https://thediplomat.com/2010/12/signals-from-the-varanasi-blast/
[37] Mumbai Bureau. (2011, July 13). 21 killed, 141 injured as terror strikes Mumbai again. The Hindu; https://www.thehindu.com/news/national//article60513438.ece
[38] ENS Economic Bureau. (2016, October 19). Cyber attacks hit banks: SBI blocks 6 lakh debit cards to ward off security threat - The Indian Express. indianexpress.com. https://indianexpress.com/article/business/banking-and-finance/cyber-attacks-hit-banks-sbi-blocks-6l-debit-cards-to-ward-off-security-threat-3092138/
[39] Tech2, News Staff. (2018, January 16). Aadhaar security breaches: Here are the major untoward incidents that have happened with Aadhaar and what was actually affected- Technology News, First Post. https://www.firstpost.com/tech/news-analysis/aadhaar-security-breaches-here-are-the-major-untoward-incidents-that-have-happened-with-aadhaar-and-what-was-actually-affected-4300349.html

ISSN: 2582-6433

approximately 5,000 workers[40]. The Tribune further stated that its reporters were able to locate an anonymous WhatsApp group that was offering to sell Aadhaar card details for as little as Rs 500 ($7.2 US). After the payment was completed, the journalists were given the Login ID and Username to a platform where they could readily view all the data associated with that person's Aadhaar number[41]. The Tribune calculated that over 100,000 persons had illegally accessed private Aadhaar information before this system vulnerability was rectified[42].

e) A conspicuous example of how Indian markets could be simple targets for financial crime syndicates was the cyberattack on Cosmos Bank in 2018, which resulted in consumers losing 94 crores. The case's investigator, Brijesh Singh, said that in only two and a half hours, fraudulent transactions had been executed in 29 different nations. The crime was perpetrated in a sophisticated manner, with extensive collaboration with foreign hackers. What was as stunning, he claimed, was how internet perpetrators employed unwitting bystanders as money couriers to finance various illegal enterprises[43].

f) In 2019, a security defect in the immensely popular WhatsApp messaging service made its 1.5 billion+ users vulnerable to "Pegasus"[44], one of the most dangerous spyware programmes in the world. A user's most private data stored on phone, including text messages, call logs, and location information, can be accessed remotely thanks to the spy program. Since the Pegasus program[45] was developed by an Israeli corporation called NSO[46], it was claimed that the Israeli government's spies were involved in the cyberattack. WhatsApp accused NSO of enabling government hacking campaigns in 20 countries in a suit brought before a federal court in San

[40] Ibid
[41] Khaira, R. (2018, January 5). Rs 500, 10 minutes, and you have access to billion Aadhaar details : The Tribune India. The Tribune; www.tribuneindia.com. https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361
[42] Tech2, News Staff. (2018, January 9). UIDAI blocks 5,000 officials from Aadhaar portal following reports of unauthorised usage- Technology News, Firstpost. www.firstpost.com. https://www.firstpost.com/tech/news-analysis/uidai-blocks-5000-officials-from-aadhar-portal-following-reports-of-unauthorised-usage-4294143.html
[43] Ahuja, N. B. (2022, January 16). Inside story of cyber attacks on India's banks, airlines, railways… and the fightback - The Week. The Week; www.theweek.in. https://www.theweek.in/theweek/cover/2022/01/06/inside-story-of-cyber-attacks-on-india-banks-airlines-railways-and-the-fightback.html.
[44] Clark, M. (2021, July 23). Here's what we know about NSO's Pegasus spyware. The Verge; www.theverge.com. https://www.theverge.com/22589942/nso-group-pegasus-project-amnesty-investigation-journalists-activists-targeted
[45] Shankland, S. (2022, July 19). Pegasus Spyware and Citizen Surveillance: Here's What You Should Know - CNET. www.cnet.com. https://www.cnet.com/tech/mobile/pegasus-spyware-and-citizen-surveillance-what-you-need-to-know/
[46] https://www.nsogroup.com/

ISSN: 2582-6433

Francisco[47]. In a statement, WhatsApp said that "100 members of civil society had been targeted", calling it "an unmistakable pattern of abuse"[48]. The application of Sections 69[49] and 69B[50] of the IT Act, 2000 has been the subject of intense controversy as a result of this case (amended in 2008).

g) Mumbai, India's financial hub, experienced a significant power outage on October 12, 2020. Water supply issues forced the cancellation of train services, and hospitals were forced to use generators. Up until the situation was addressed two hours later, businesses in Mumbai, Thane, and Navi Mumbai fought to maintain their operations. Cybersecurity experts believe that China's People's Liberation Army (PLA), which is now involved in a significant conflict with the Indian Army in Ladakh, may be involved, notwithstanding allegations of sabotage made by Maharashtra Power Minister Nitin Raut. 14 Trojan horses, a type of malware that may have been installed on the systems of the Maharashtra State Electricity Transmission Company, were the subject of suspicion[51].

h) When SITA, the Geneva-based company that provides data for more than 90% of the world's airlines, alerted Air India in February 2021 that hackers had stolen the personal information of 4.5 million passengers, it created yet another obstacle for India's cybersecurity apparatus. Despite the fact that the incident took place outside of Indian territory, lakhs of Indians were impacted. According to a statement from Air India, the breach affected personal data that was exposed for almost ten years, from August 26, 2011, to February 3, 2021. Although, the cyber-warriors of India made every effort to minimise the harm wrought by the infringement, they eventually

[47] Columbia Global Freedom of Expression. (2009, December 10). WhatsApp Inc. v. NSO Group Technologies Limited. globalfreedomofexpression.columbia.edu. https://globalfreedomofexpression.columbia.edu/cases/whatsapp-inc-v-nso-group-technologies-limited/

[48] Reuters. (2019, October 30). WhatsApp sues Israel's NSO for allegedly helping spies hack phones around the world Technology News, The Indian Express. indianexpress.com. https://indianexpress.com/article/technology/tech-news-technology/whatsapp-sues-israels-nso-for-allegedly-helping-spies-hack-phones-around-the-world-6094140/

[49] Section 69 - Power to issue directions for interception or monitoring or decryption of any information through any computer resource. (n.d.). India Code; www.indiacode.nic.in. https://www.indiacode.nic.in/showdata?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=88#:~:text=%5B69,Power%20to%20issue%20directions%20for%20interception%20or%20monitoring%20or%20decryption,information%20through%20any%20computer%20resource.

[50] Section 69B - Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security. (n.d.). India Code; https://www.indiacode.nic.in/showdata?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=90

[51] Ahuja, N. B. (2022, January 16). Inside story of cyberattacks on India's banks, airlines, railways… and the fightback - The Week. The Week; www.theweek.in. https://www.theweek.in/theweek/cover/2022/01/06/inside-story-of-cyber-attacks-on-india-banks-airlines-railways-and-the-fightback.html.

ISSN: 2582-6433

discovered that it was difficult to conduct an inquiry into attacks that occurred outside of Indian cyberspace due to concerns with jurisdiction.[52]

While the first few instances may raise concerns about privacy and security breaches because the architecture of the e-governance system was not adequately protected, the last few examples raise concerns about security and privacy breaches from the standpoint of an intermediary that is utilised by the public at large for data and digital communication and by government agencies for e-governance[53].

Correlation between Article 19(2)[54] and Section 66F[55]

It is possible to infer from the definition given under Section 66F[56] that cyberterrorism is an act of hacking, blocking, and computer infesting in order to restrict legally authorised persons' access to computer resources generally and to gain or obtain unauthorised access to any information that is a "restricted information" for the purpose of security of the state, foreign relations, etc. These horrifying acts may cause death and injury to people, property damage, a disruption of civil services that are necessary for a community's survival, and also have an impact on the critical information infrastructure. They are performed with the intent to endanger the security, sovereignty, and integrity of India or to instil a sense of terror in the minds of people or a specific society.

In the instance of the 26/11 Mumbai attacks, it was clear that the terrorists had exploited communication services to further their heinous ambitions rather than to breach or obstruct the sensitive data. The intercepted messages that the Indian government used in the investigation of the Mumbai terror case makes it abundantly evident that the radicals were only using their own personal freedom of expression to communicate. However, when the message as a whole was examined, it became clear that this speech was being made in an effort to undermine India's sovereignty, peace, and security. As a result, it no longer qualifies as protected speech under Article 19A[57] of the Indian Constitution. It is a terrorist act instead. This specific element is

[52] Ibid
[53] PTI. (2014). "Delhi Police Launches WhatsApp Helpline to Curb Corruption." https://indianexpress.com/article/cities/delhi/delhi-police-launch-whatsapp-helpline-to-curb-corruption
[54] A significant article curbing the extent of freedom of speech and expression exercised by the citizens of India under Constitution of India, 1950.
[55] This section was added through an amendment to the original Information Technology Act, 2000 in the year 2008 which was the result of the infamous Mumbai Attack 26/11.
[56] Punishment for cyber terrorism. (n.d.). India Code; www.indiacode.nic.in. https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=82
[57] https://indiankanoon.org/doc/1218090/

ISSN: 2582-6433

conspicuously missing from the definition given by section 66F[58].

The notion behind the rule "***actus reus not facit nisi mens sit rea***" is embodied in Section 66(F). An act of cyberterrorism must involve both criminal and immoral activities[59]. Article 19(2)[60] of the Indian Constitution is somewhat identical to this definition[61]. The Constitution's Article 19(2) specifies the limits beyond which the right to free speech and expression may be legally curtailed. Simply put, any conduct that violates Section 66(F) of the IT Act is a violation of the grounds listed in Article 19(2), which restricts the right to freedom of speech and expression, and is therefore considered cyberterrorism[62]. In light of this, cyber terrorism is indicated by Article 19(2) when read in conjunction with Section 66(F) of the IT Act[63].

[58] Alık, N. A. H. A. (2022). Emerging Cyber Security Threats: India's Concerns and Options. International Journal of Politics and Security, 4(1), 170-200.

[59] Chawla, G. (2019) Respond to the cyber intrusion, within the law [Online] Available from: https://www.hindustantimes.com/analysis/respond-to-the-cyber-intrusion-within-law-opinion/storyTkUs7CAwKFEXwmWmMHkT8K

[60] Article 19(2) states that "Nothing in sub clause (a) of clause (1) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub clause in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence"

[61] Nappinai, N. (2017) Technology Laws Decoded, 1st Ed., Gurgaon: Lexis Nexis.

[62] Ibid

[63] Singh, V. P. (2021). Cyber terrorism and Indian legal regime: a critical appraisal of Section 66 (F) of the Information Technology Act. Sri Lanka Journal of Social Sciences, 44(1), 71-81.

ISSN: 2582-6433

Conclusion

"The Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally transnational manner." Ban Ki-moon – Secretary General of the United Nations

It is tragic to point out that despite the changes and significant provisions implemented by the government to combat cybercrimes, India stands to be one of the major victims of cyberattacks and cyberterrorism as after the introduction of various amendments and new acts, the government still fails to have the robust cyber-security measures required to counter the growing threat posed by cyberterrorism. Cyber terrorism poses one of the greatest threats to all the nations in the modern era. Terrorists are increasingly turning to more dangerous weapons, and their original goal of terrorising hundreds of people while killing one has changed with time. They believe that by slaughtering more and more people, they will ultimately prevail in the aimless conflict. Their nature has evolved to be more dangerous, and they profit from society's technological growth as well. They are using modern technologies to their advantage to spread fear and chaos.

India's Computer Emergency Response Team (CERT-In) tracked and received reports on over 14 lakh cyberattack occurrences in 2021[64]. Ransomware attacks have surged by 120% in India, according to government statistics. Despite the numerous efforts by the government, India also has far less cybersecurity initiatives and activities than other advanced nations. Given this dire scenario, the democratic State's top priority should be to ensure the safety and security of its citizens, and as a result, it should pass legislation to reduce the threat of cyberterrorism[65]. The State must, however, use extreme caution. Since all laws are strengthened by both public support and the authority of the State, care must be taken to ensure that innocent people are not persecuted and their fundamental rights are not violated. Human rights considerations and security concerns should coexist in harmony[66]. To dissuade, recognise, and track terrorists, there must be regulatory and monitoring measures in place, but they should not undermine the rights and liberty of citizens.

[64] IANS. (2022, March 26). CERT-In detects over 14L cyber security incidents in 2021 - ET Telecom. https://telecom.economictimes.indiatimes.com/news/cert-in-detects-over-14l-cyber-security-incidents-in-2021/90452616

[65] Singh, P. (2008) Terrorism and the Rule of Law, In N. R. M. Menon (ed.) Rule of Law in a Free Society, pp: 147–173, New Delhi: Oxford University Press

[66] Ibid