Sri Lanka Journal of Social Sciences 2021 ***44*** *(1): 71-81*
DOI: https://dx.doi.org/10.4038/sljss.v44i1.7997

RESEARCH ARTICLE

Cyber terrorism and Indian legal regime: a critical appraisal of Section 66 (F) of the Information Technology Act

Vijay P. Singh
Legal Management, Indian Institute of Management, Lucknow, India.

Abstract: The menace of terrorism, when boosted by information and communication technology, incarnates into cyber-terrorism. This new avatar of terrorism is more sophisticated than the traditional one. By virtue of its labyrinthine and trans-border, cyber terrorism presents a fundamental challenge to democratic states. Many countries, curbed and curtailed the freedom of speech and expression, liberty, privacy and other fundamental rights in order to combat the menace of cyber terrorism. India, one of the world's largest democracies, enacted specific anti-terrorism laws to tackle the threat of terrorism and included a provision concerning cyber terrorism in the Information Technology Act. However, combating the blatant and hidden acts of cyber terrorism is not a regular criminal justice-endeavour; instead, it is a challenge to the state machinery. This paper aims to make an inquiry into the conceptual framework of cyber terrorism and highlights the Indian legal regime to tackle the menace of cyber terrorism. The article further critically examines Section 66 (F) of the Information Technology Act to prove the hypothesis that this provision is a stringent measure, and is against the very structure of democracy and the rule of law.

Keywords: Cyber terrorism, internet, computer, legal framework.

INTRODUCTION

The phenomenon of terrorism is as old as human history (Weingberg, 2006; Halder, 2011). In the present era, every country in the world is witnessing the threat of terrorism. Acts of terrorist violence perpetrated by terrorist groups in one or the other parts of the world are experienced by many, everyday. It has engulfed the entire globe and has created an unusual challenge before the world. Several people are run-downed of their lives, family and possessions because of terrorism. It has affected individuals' lives and the economic, social and political development and growth (Laquer, 1987; Martin, 2011). With the growth and progress in Information and Communication Technology (ICT), the evil of terrorism also attained immense strength to perpetuate destructive activities (Ramsay, 2008). September 11 attack on the United States of America exhibited that terrorist organisations are operating with increasing complexity, audacity and lethality and has attained a new outlook (Gupta, 2004) Now territorial boundaries are not obstacles in perpetuating the terrorist activities (Gupta, 2004; Mahapatra & Tripathi, 2007; Mali, 2012). The world is bleeding due to the ruthless temper of terrorism (Guelke, 2010) and such inhumane terrorist activities are responsible for the massacre of the number of innocent people. The world has witnessed many terrorist attacks, such as the World Trade Centre's attack, Mumbai bomb explosion to Boston Marathon Bomb Blast in 2013 and the Paris attack on 13th November 2015. Recently the terrorist attack on Sri Lanka in April 2019 has revealed that terrorists are against humanity and are inhumane. This menace is an assault on democratic society which is getting more dreadful with science and technology (Branscomb, 2007).

The technologies had enabled our life to be more comfortable and empowered terrorist groups to undermine security and inflict harm. For example, modern

*Corresponding author (vijaypalsingh3@gmail.com; vpsing@iiml.ac.in; https://orcid.org/0000-0002-4592-6654)

This article is published under the Creative Commons CC-BY-ND License (http://creativecommons.org/licenses/by-nd/4.0/).This license permits use, distribution and reproduction, commercial and non-commercial, provided that the original work is properly cited and is not changed anyway.

communication technologies from satellite phones to the internet have aided a decentralised structure of terrorist groups, marshalling their resources to increase terrorist activities throughout the world (Mates, 2001; Oh *et al*., 2011). Such technologies facilitate the encryption of messages, provides critical access information and scores of sites provide information concerning the creation of explosives and other destructible materials (Robertson, 2010). Thus, by exploiting the ability of the internet, the terrorists have magnified their disruptive power. For example, Osama bin Laden's Arab Afghan crusade's unique feature was its capability to rearrange the operations rapidly from one place to another as the situation demanded (Kaplan, 2003).

In the year 1997, a report revealed that Arab Afghan played an active role in activities carried out by Algeria's GIA and Egypt's IG and aided the Islamic Liberation Party (ILP) while conducting operations in Somalia. They relocated crusaders to Xinxiang Uighur Province in the Western part of China, to crusade a religious war against the Chinese regime. The attack on US embassies in Kenya and Tanzania by Al Qaeda demonstrated the smooth and swift mobility of members of Al Qaeda from one place to another, and it becomes possible because of adaption and use of information technology by the new generation of terrorist organisations (Kaplan, 2003; Post *et al*., 2001).

The terrorists are exploiting the internet technology efficiently in their favour. Many contemporary terrorist leaders are willing to adopt the latest technology to inspire and motivate young people to join the organisation and spread disruptive activities worldwide. Such technological innovations have given extremists a great conduit to disseminate their rhetoric and strategies to a large extent of the population (Minei & Matusitz, 2012). The traditional types of ethnic/nationalist, separatist and ideological groups have joined other organisations with no nationalistic or ideological motivations and transformed their *modus operandi* using new technologies and lethality in recent years (Rajput, 2020). For such distinctive networking of various terrorist organisations and change in the *modus operandi*, the diffusion of information technology across the world and increased and accessible movement across the international boundaries, are the two most significant factors (Martin, 2006).

India has been the prime target of militancy and terrorist group. In India, terrorist groups apply new technologies to champion their cause. They have acquired many weapons and established their relations with the terrorist groups outside India (Chawla, 2019). At present, perhaps all the terrorist groups based in India have some links and allocate resources with international terrorist networks such as Al Qaeda (Kamath, 2001; Mishra, 2002). The terrorist groups based in India may have an association with ISIS, considering the global outreach of ISIS. Such a development raises pressing concerns for India.

Determined to combat terrorism, the Indian government enacted anti-terrorism laws from time to time. For example, in the year 1985, the government passed the Terrorists and Disruptive Activities (Prevention) Act 1985 (TADA), which was followed by the Prevention of Terrorism Act, 2002, and the Unlawful Activities Prevention Act, 1967 (UAPA), amended latest in 2019. With the emergence of cyber terrorism, the Indian government included few provisions in the Information Technology Act to combat cyber terrorism. This paper, by applying doctrinal research methodology, conceptualises cyber terrorism. It critically examines Section 66 (F) of the Information Technology Act. Further, with the help of case laws decided by various High Courts and the Surpeme Court of India, the paper negates the hypothesis that the provision relating to cyber terrorism is not adequate, and it is against the fundamental democratic principles.

METHODOLOGY

Doctrinal research means research carried out on a legal proposition or propositions by analysing the existing statutory provisions and cases by applying the reasoning power. The doctrinal legal research attempts to verify the hypothesis by a first-hand study of authoritative sources. Doctrinal research embarks upon the analysis of case law. It is arranging, ordering and systematising legal propositions. At the same time, it studies legal institutions, and it creates law through legal reasoning or rational deduction. In doctrinal research methodology, it requires a high level of critique and review as a contextual background. The doctrine's primary sources are the centre for reading and a guiding principle for reforming the law and legal system for research development in legal research.

Doctrinal research is underpinned by positivism and a view of the world where the law is objective, neutral and fixed. In the words of prominent jurist of positive school, H. L. A. Hart, doctrinal research "takes an internal, participant-oriented epistemological approach to its object of study". Thus the doctrinal legal analysis is knowledge-based research in law rather than research about the law. It does not go through the relationship of law with other disciplines of society. Though the law

itself is normative, which prescribes what people ought to do or what ought not to do, doctrinal research does not dig out the queries on human behaviour, conducts and the relationship of law with other social ingredients.

The researcher conducting doctrinal research usually analyses the existing laws for the sake of stability and certainty in the law, which could ultimately result in consistency in justice delivery.

The primary purpose of doctrinal legal research is to improve the law's substantial part by achieving the broader law goal. The ultimate goal of the law is justice rather than mere standard procedures, texts and jargons. Thus doctrinal legal research is often employed to enrich legal contents, code, and even interpret the legal statutes.

CYBER TERRORISM: AN EMERGING THREAT

Indeed, practices and predictions of terrorists acquiring destructive cyber capabilities date back many years. In the year 1990, the National Academy of Sciences alerted the first cyber-attack termed 'Digital Pearl Harbour' (Weimann, 2004). A decade earlier cyber terrorism was in its infancy, but now is a deadly threat leaving the world totally off guard; the approaches are fundamental and naive but, patron-less destruction advanced with a much higher degree of efficiency through the internet technology (Klein, 2015). Mark Potok, a Southern Poverty Law Centre analyst, viewed:

> "The internet is an important piece of the leaderless struggle approach. It permits lone wolves to keep well-informed of actions, alterations in ideology and discussions of tactics – all of which may impact his-own choice of target. Far more than hard copy publications the internet allow the lone-wolf to remain a part of a longer movement even though he attends no meetings, put his name on no lists, and generally try to remain invisible. A good example of this is Mathew Williams, the confessed murder of a gay couple in California, who used the internet to privately explore a variety of extremist ideologies before picking up the gun" (Sue & Mahan, 2003).

Many terrorist groups listed by the US State Department's list maintain labelled websites on the internet. While US officials believe that some terrorists used encrypted e-mail to plan acts of terrorism, most of the group appears to use the internet to spread their propaganda (Ramsay, 2008). In 1996, a US-based Internet Service Provider (ISP) was disabled by a computer hacker damaging part of its record-keeping system and signed off with the threat, "you have yet to see true electronic terrorism. This is a promise". In the year 1998, the Spanish protestors bombarded the Institute for Global Communication (IGC) with thousands of bogus e-mails because they demanded the IGC to stop hosting a website for the Euskal Herria Journal, a New York-based publication supporting Basque in independence (Mali, 2012). The ethnic guerrillas swamped Sri Lankan embassies with hundreds of e-mails per day and the message read "We are the internet black Tigers and are going to disrupt communication". It is said to be the first known attack by terrorists against a country's computer system. NATO computers were blasted with e-mails and hit by denial of service attacks during the Kosovo conflict in 1999 (Mali, 2012).

Some militant organisations also use the internet to propagate anti-western, anti-Israel objectives. Hezbollah manages at least three websites. One for the central press office at www.hizbollah.org, the organisation, sells books and publications with these websites. Other sites, www.moqawama.org and www.almanar.co.ib, were used to describe its attacks on Israeli targets, broadcast the news and information, and make information available on making bombs, instructions for making hazardous chemicals and explosives weapons. Websites devoted to bin Laden and jihadists sites, such as London-based azzam.com, deliver a wide range of products and services (Ramsay, 2008). A degree of the site's global reach can be comprehended in response to the death of a Saudi named Khallal al-Madani, who was killed in Chechnya in February 2000 while fighting under bin Laden's command. Within a day, messages for sustenance for al-Madani's family was received from several parts of the world (Peter, 2001). Chechen groups also maintained websites in more than twelve languages, from Albanian to Swedish (Addicot, 2011; Peter, 2001).

Terrorist groups are harnessing the technology to meet their end. They are using internet technology to design plans, raise funds, propagate their ideologies, and persuade the younger generation to join the camp (Ramsay, 2008). Indeed, such menace will rise in coming time as the leadership positions in terrorist organisations are increasingly filled with internet-savvy people (Sue & Mahan, 2003). In the year 2017, ISIS put out a call to their recruits, focussed on civilians in Europe, US, Australia, and India. These calls were realised with attacks in Manchester, London, France and a bomb attempt in Brussels during 2017 (Sultan, 2017).

Moreover, the terrorist groups are trying to use cryptocurrency to dodge traditional black market terror financing operations, as crypto-funding of terror

activities advances added peril (Sultan, 2017). The fact that ISIS has four online media publications apart from sophisticated online posts, video, tweets and retweets raises apprehension for the world to focus on cyber technology to control their impact on the population (Sultan, 2017).

CYBER TERRORISM IN INDIA

Cyber terrorism in India is no longer an illusion (India Risk Survey, 2018). On 2nd April 2002, the Anti-India Crew (AIC) of Pakistan had infected the websites of India and tried to destroy and delete the entire information stored in the computer, computer system or computer network of eighty-eight websites including the websites of Indian Government (Bhansali, 2012; Saxena, 2011). The horrific 26/11 Mumbai attack is a glaring example wherein the use of ICT by terrorist made it quite difficult for Indian security forces to differentiate and capture these perpetrators (Oh *et al*., 2011; Hani & Ranjan, 2018). On 13th July 2010, the ICT was exploited in Zaveri bomb blast. In 2010 Varanasi bomb blast, ICT was utilised for communication; Indian Mujahidin took responsibility for the explosion through e-mail, which was traced to WiFi connection in the Vashi, Navi Mumbai (Hani & Ranjan, 2018). Virtual SIMs were used by Jaish Mohammad suicide bomber in the Pulwama attack in Jammu and Kashmir on 14th February 2019 (Press Trust of India, 2019). The cyberspace has eventually become the platform for cyberwar and terrorist activity. The terrorist organisation appreciates cyber-attacks as an effective mechanism of jihad in executing crusade against their enemies. Terrorist groups have developed their abilities to abuse the virtual world (Dhar, 2017).

Cybersecurity and war experts Singer & Friedman (2014) assert that even though many research articles discuss the phenomenon of cyber terrorism, the world has not seen any physical injury or killing by cyber terrorism (Ramsay, 2008). India also has yet not experienced any occurrence of substantial cyber-attack which can be designated as terrorism. However, this does not mean that the terrorist groups will not abuse cyberspace to inflict death and destruction. There is a considerable increase in the number of talented and ambitious terrorist groups capable of severely causing cyber-attacks in any part of the world (Sultan, 2017).

The terrorist organisations by decentralised network arrangements are managing the activities of members spread all over the world. They are broadcasting information and associating with the organisation and supporting their businesses (Whine, 1998; Abuhasan, 2020). Indeed, every active terrorist organisation in the present era demonstrates their ability to exploit cyber technology by propagating their ideologies on websites owned by them or using or misusing cyber technologies to aid terrorist attacks (Hoffman, 2017; Weimann, 2010). Further, it is quite challenging to reckon with the ease and speed of terrorist groups in adopting and executing destructive cyber-attacks in the coming future. Therefore, a reasonable inference can be drawn that in an ever-growing digital world, cyber technology and strength of the terrorist groups entails a constant review of cyber-attack assiduously and needs an appropriate legal mechanism to combat this menace in India (Venkatachary *et al*., 2018).

LEGAL SCHEME TO FIGHT AGAINST CYBER TERRORISM IN INDIA

The problem of terrorism in India is not new, but after independence from British rule and more specifically during the 1980s, the situation became worse. To combat terrorism, the Indian government enacted its first anti-terrorism law, namely, Terrorist and Disruptive Activities (Preventive) Act, 1985 (TADA), which was repealed in 1995. In the year 2002, the second anti-terrorism law, Prevention of Terrorism Act (POTA) was enacted. The life of POTA was short; it lasted nearly a year. Both these laws were against the basic principle of criminal justice and drastically failed to tackle the grave situation created by terror groups. After the repeal of POTA, provisions to curb the menace of terrorism was enshrined in Unlawful Activities and (Prevention) Act 1967 (UAPA) after necessary amendments, but no rules were included to tackle cyber terrorism (Ade, 2015; Cardoso & Da Rosa, 2016).

Even though the threat of cyber-terrorist attacks is no more a myth (ICT, 2018), the Indian government has not enacted any specific cyber-terrorist legislation to combat this menace. In 2000, the Indian government legislated the Information Technology Act, 2000 (IT Act). Furthermore, this enactment was legislated primarily to acknowledge e-commerce and facilitate electronic filing of documents with the Government agencies. However, the Act (Chapter XI) lists few offences relating to the use and abuse of computer system which invites a penalty or imprisonment or both (Hani & Ranjan, 2018). The IT Act included the offences such as hacking, cyber obscenity, tampering with computer and data, misrepresentation before the Controller of Certifying Authorities or his assistants, breach of confidentiality and privacy, and a publication of the false digital signature certificate. However, cyber-offences such as cyber-stalking, cyber-theft and even cyber-defamation were not punished under this Act. Thus, the IT Act was an incomplete code dealing with few specific cyber-offence.

The reason for excluding several cyber offences may be the perception that the provisions of Indian Penal Code 1862 and other penal statutes are sufficient enough to tackle cyber issues. However, time belied such impression and the fast growth rate of cybercrimes, especially cyber terrorism, which compelled the government to expand the spectrum of the IT Act 2000. While the government has embarked on various legal initiatives to protect against the threat of terrorism, a growing number of issues related to cyber terrorism remain unanswered.

The size and nature of cybercrime and the menace of cyber terrorism in India compelled the Indian government to reformulate the Information Technology Act 2000. Thus, in December 2008 as a spontaneous reaction against the Mumbai terror attack, the Information Technology (Amendments) Act, 2008 was hastily presented before the Parliament and was passed in one go without any debate whatsoever (Halder, 2011; Hani & Ranjan, 2018). The vital concern of the latest Information Technology Act, 2008 was on cybercrime and a substantial degree of cyber terrorism (Goel, 2020).

Section 66 (F) firmly dealt with cyber-terrorism by defining and severely punishing such an offence. Several other provisions were introduced by the Amendment Act 2008, which may be related to cyber terrorism, appeared to be a good and welcome step by the government to fight against evil. Section 70 (A) and Section 70 (B) of the Act aims to protect the critical infrastructure of the country and essential defence and scientific installations. These two Sections cover the investigatory process and at times can be used as a preventive measure too.

It is a well-accepted fact that terrorists are now using cloaking devices provided by encryption companies to keep security agencies from reading their communication (Stytz & Banks, 2014). Consequently, the Indian government, under Section 69 of the IT Act, can authorise any government authority to intercept, monitor or decrypt any information generated, transmitted or stored in any computer resource. Terrorists and the surveillance endanger the state security by the States or entities who supported such evil activities. Thus, the government is empowered under Section 69-A to block access of any information if there lies any reasonable apprehension causing a threat to the country's security (Reich, 2012).

Furthermore, the new eventualities of cybersecurity alarm like wiki leaks etc. perhaps stimulated India to implement the National Cyber Security Policy, 2013 (Desai & Bhatt, 2019). This policy aims to protect the State's cybersecurity, although it is not a statute but a welcome step to deal with the issues related to cybersecurity and cyber-terrorism (Desai & Bhatt, 2019). No doubt, (cyber) terrorism is the real threat to the present society. It is the government's principal obligation in a democratic rule to afford protection and security to the people. In achieving such objective, the governments are free to take all such essential and necessary actions they think appropriate (Halder, 2011). However, the State has to be very careful; care must be taken so that innocent people are not harassed, and their fundamental rights are not violated. All laws derive strength from the authority of the State and the support of the people. The physical correction is not merely in-laws; it is much more in the dynamic functioning of the administrative and political institutions (India, National Human Rights Commission, 200-2001).

Inequality before the law or economic, social-political, cultural factors and uneven application of the law must end, as these factors fuel the terrorism (Foggetti, 2010). The author firmly believes that the provision under Section 66 (F) is against the democratic rule and can be misused by the state machinery. The Supreme Court in case of *Shreya Singhal v Union of India* [(2015) 5 SCC] declared Section 66 (A) unconstitutional and observed that like Section 66 (A), Section 66 (F) is another narrowly drawn Section. Unfortunately, the Supreme Court has not dealt with the issue relating to Section 66 (F) as it was not raised before the court by the petitioner.

CRITICAL REVIEW OF SECTION 66 (F)

An analysis of cyber terrorism as defined under Section 66 (F) reveals that the impugned definition is ambiguous, unreasonable and broad enough to cover any act concerning to internet within the ambit of Cyber Terrorism. Such a loose definition opens the floodgate for arbitrary and selective application by the state machinery (Mohanty, 2011). It provides state agencies with ample opportunity to harass and exploit any person. Section 66 (F) embodies the principle expressed in the rule of '*actus reus not facit nisi mens sit rea'*. Both guilty and criminal acts are necessary to constitute the offence of cyber terrorism (Chawla, 2019).

Since the prosecution is based on the interpretation of the law enforcer's intent, Section 66 (F) can be applied to any person by the state machinery on the ground of suspicion. The person has to spend years in jail before the judiciary decides whether he is guilty of having that intention or not (Shourie, 2018). For example, in *Niranjan Singh Karan Singh v Jitendra Bhimraj Bijjaya* [(1990) 4 SCC 76], the accused was charged under Section 3 of TADA. It was alleged that the accused killed

their opponents to strike terror in the people or segment of people (residents of the locality) using weapons such as knives and iron rods. The Apex Court held that though the result of such acts is bound to create panic and fear, but the intention of committing the offence cannot be said to strike terror in the people or any section of society as defined under Section 3 of TADA. A mere statement to the effect that shows of such violence would create terror or fear in people's minds and, consequently, none would dare to oppose them is not sufficient to constitute an offence under section 3(1) of the Act.

Though the accused got the relief from the Supreme Court of India, it shows how state agencies were empowered with arbitrary power to charge any person under TADA who had committed the offence under another penal statute. This conclusion is further substantiated by numerous other cases that have occurred during the draconian regime of POTA (Singh, 2008). Thus, the experience creates apprehension that Section 66 (F) can be misused by state machinery in a likely manner. Further, the application of Section 66 (F) in a matrimonial case is a glaring example of how an ordinary member of the society can misuse it. However, the trial proceedings for offences under Section 498 (A), 506, 384, 120 (B) of Indian Penal Code and Sections 3 and 4 of Dowry Prohibition Act and Sections 66 (A), 66 (F) of the IT Act was quashed by the Karnataka High Court (*Pavan M. v State*, CRIMINAL PETITION NO.1247/2013).

This definition resembles clause (2) of Article 19 of the Indian Constitution (Nappinai, 2017). Article 19 (2) of the Constitution stipulates the parameters up to which the freedom of speech and expression can be legally restrained. Article 19 (2) of the Constitution authorises the legislature to impose reasonable restraint on the right to freedom of speech and expression enshrined under Article 19 (1)(a). A reasonable restriction can be enforced on the grounds mentioned under Article 19 (2) such as security of the State, friendly relations with foreign countries, public order, decency and morality, contempt of court, defamation, incitement of offence and sovereignty and integrity of India. These reasonable restrictions can only be imposed through enacted legislation and by executive order [*Express Newspaper (P) Ltd. v Union of India* (1986) 1 133; *Bijoe Emmanuel v State of Kerala* (1986) 3 SCC 615].

Further, Section 66 (F) states that any person knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to such information, data or computer database that is restricted for reasons for the security of the State or foreign relations, or any restricted information, data or a computer database, with reason to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interest 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, or to the advantage of any foreign nation, group of individuals or otherwise, commits the crime of cyber terrorism. In other words, grounds mentioned under Article 19(2) restricting the right to freedom of speech and expression can be characterised as cyber terrorism if any person knowingly or intentionally does any act prohibited under Section 66 (F) of the IT Act (Nappinai, 2017). In other words, Article 19(2) read with Section 66 (F) of the IT Act is cyber terrorism.

The other objectionable term used in this section is defamation, contempt of court and decency or morality; how these terms are related to cyber terrorism is not backed by any reasonable logic. The offence of defamation and contempt of court was outside the spectrum of 'Terrorist Activities' under TADA and Prevention of Terrorism Act 2002. Furthermore, Unlawful Activities and (Prevention) Act 1967, which defines 'Terrorist Act' does not include defamation and contempt of court within the definition of terrorist activities.

According to Section 2 of the Contempt of Courts Act, 1971, the term 'contempt of court' means civil or criminal contempt. For civil contempt, there should be willful disobedience to any judgment, decree, direction, order, writ or other processes of a court or deliberate breach of an undertaking given to the court. Moreover, contempt of court will be a criminal contempt if: (1) the publication of any matter or any act scandalises; or (2) tends to offend; or (3) lowers or tend to reduce the authority or dignity of any court or; (4) prejudices, interferes or tends to interfere with the due course of a judicial proceeding; or (5) in any manner interferes or tends to interfere with or obstruct or tends to impede the administration of justice (Venugopal & Subramanium, 2011). The Supreme Court and the High Court are authorised to punish people for contempt of court under Article 129 and 215 of the Constitution. Section 10 of the Contempt of Court Act 1971, empowers the High Court to punish any person for contempt of its subordinate courts.

The contempt of court is a concept having a legacy of Anglo-Saxon jurisprudence. The purpose behind the contempt of court is that the court should not become powerless in the face of disobedience of its order by the

executive and with no other means of implementing its directive (Reddy, 2010). It is a mechanism which the people themselves have given the courts and which courts keep properly sheathed to be used rarely but only when the public demands it.

To ensure that the task of the judiciary to maintain harmony and balance between the different parts of the government which is necessary for the growth and sustenance of democracy is not defeated Article 19(2) provides that right to speech and expression guaranteed under Article 19(1)(a) is subject to the State making any law in relation to any contempt of courts. However, an enactment about contempt which imposes an unreasonable restriction on the right of the citizens to freedom of speech and expression would be *pro tanto* ultra-vires [*E.M.S. Namoodaripad v T. Nayayanan Nambiar*, (1970) 2 SCC 325] (Chupika, 2016).

Moreover, it must be acknowledged that contempt is a matter between the court and the contemnor and State has no role to play in determining that a person has committed an act of contempt or not (Venugopal & Subramanium, 2011). The earlier anti-terrorism law in India and even present anti-terrorism law (UAPA 1967) does not permit contempt of court within the spectrum of terrorism. Still, the definition of cyber terrorism under Section 66(F) is so wide to include contempt of court within the ambit of the terrorist act.

Further, a man's reputation is as valuable as physical safety, property and any valuable security. It is rightly said that if money is lost nothing is lost but if reputation is lost everything is lost. The defamation hurts a man's reputation (*MC Verghese v T.J. Punnam*,1970 CriLJ 1651: AIR 1970 SC 1876). Therefore, Section 499 of the Indian Penal Code defines and punishes the act of defamation.

The essence of the offence of defamation is the publication of the imputation with the knowledge that it will harm the reputation of the person defamed (*Wahid Ullah v Emperor*, AIR 1935 All 743). Every citizen in India has a right to criticise the corrupt government without fear of litigation, as Article 19(1) provides the freedom of speech and expression with reasonable restriction. In case of *City of Chicago v tribune Co* [(1923) 307 ILL 595, p 607], Thompson CJ of the Supreme Court of Illinois observed that: 'Every citizen has the right to criticise an inefficient or corrupt government without fear of civil or criminal prosecution. This absolute privilege is founded on the principle that it is advantageous for the public interest that the citizen should not be in any way fettered in his statement. Where the public service or due administration of justice is involved, he shall have the right to speak his mind freely, the government, local authority, and other State organs, exercising governmental powers cannot maintain a suit for damages for defaming them [*Sic*]'.

However, an individual officeholder may agitate, if defamed, individually, but 'state' as such cannot sue a citizen on its behalf. The rule was established in the United States [*New York v Sullivan* (1964) 376 US 254]. In the United Kingdom this rule was created through *Derbyshire County Council v Times Newspaper Ltd.* [(1993) 1All ER 1011 (HL)] and accepted in India in case of *Raj Gopal v State of Tamil Nadu* (AIR 1995 SC 264, p. 277). However, in the case of New York v Sullivan [(1964) 376 US 254], it was observed that if a public official feels offended by the defamatory article concerning his official conduct, he could sue and recover damages. The right to disapprove of governance and politics in Australia has been an indispensable incident of the representative government under the Constitution, which explicitly contains no fundamental rights. Putting the offence of defamation within the ambit of Cyber Terrorism means that writing anything that is not suitable to the government amounts to cyber terrorism, which otherwise is no offence and such a provision is subject to abuse (Nippani, 2017).

Decency or morality again has no nexus with cyber terrorism. Decency can be defined as a lack of obscenity. No person can be allowed to deteriorate and dilapidate society's social structure and morality, and for that reason, any obscenity should be suppressed and punished (Rajak, 2011). Further, the conception of morality differs from place to place and from time to time (Rajak, 2011). For example, birth control and contraceptives were once considered immoral and taboo, and indeed, there have been convictions for publishing literature dealing with contraception (*R v Bradlaugh*, 3 QBD 607). However, today, the outlook has transformed into the modern world, and it is no more taboo to discuss such matters. Instead, the State, by itself, encourages and promotes the use of contraceptives. Sometimes an act might be 'morally offensive' to one person need not be so to another person; the conduct is moral or immoral depends entirely on each person's culture and society he belongs (Rajak, 2011). This further buttresses the argument that the expressions used in Section 66 (F) are vague and ambiguous (Singh, 2019).

Thus, it can be concluded that the expression used in Section 66 (F) such as 'Contempt of Court', 'Defamation' 'Decency or Morality' and 'Public Order' are vague, elastic and general. Further, in the absence

of any precise definition, limitation or clarification as to extent and scope of each of the expressions, a reasonable man cannot ascertain whether his conduct is outside the scope of 66 (F) or not.

Moreover, the legislature has not looked beyond Section 43 and Section 66 to address the offences like cyber terrorism (Mohanty, 2011). The term "computer contaminant" used in Section 66 (F) is to have the same connotation as given in Section 43 of the Act, meaning thereby, any act which falls under Section 43 is also covered under Section 66 (F) of the Act. Moreover, Section 66 of the IT Act states that if any person, dishonestly or fraudulently does any act referred to in Section 43, he shall be punishable. It means that Sections 43 and 66 are covered under Section 66 (F) with graver punishment (Halder, 2011). Therefore, enactment of such a patently vague provision is wholly unjustified. Having the horrific past of TADA and POTA led to a situation where it is impossible to believe that having such an extensive provision cannot be misused by state machinery against any person.

Thus, Section 66 (F) suffers from the iniquity of elusiveness because the expression mentioned therein bear different consequences in a given situation and depends on the subjective opinion of the statutory authority without any objective standard or norm (Mohanty, 2011). In the context of the internet, the enforcement of Section 66 (F) is a treacherous form of suppression that India's Constitution does not authorise. Defining the offence concerning the medium employed for communication leads to arbitrariness. For example, an identical interface in a physical form would not be subjected to penal action. However, the same interface over an electronic platform exposes the person to criminal liability. Hence, it widens the scope of misuse of power by the state administration. Such provisions merely weaken and debilitate people's faith in a democratic system. The provision was hastily designed to combat cyber terrorism and be easily hijacked by state machinery to violate fundamental rights and freedoms. Thus, if any provision derogates any person's fundamental rights and is unreasonable and unfair, such provision should be erased from the statute book.

CONCLUSION

In brief, it may be concluded that cyber terrorism is undoubtedly one of the gravest threat in the present era and as terrorists are going for more lethal weapons and that their outlook of killing one and frightening hundreds is now transformed with time. They are of the view that killing more and more will make them win in the directionless war. Their nature has now become more lethal, and with the technological advancement, in the society, they too are benefited. They are exploiting the latest technology to create chaos and fearful environment. Cyber terrorism is the latest catchphrase within the domain of cyber-attacks, cyber-crime, or community warfare. In light of such a grave situation, it is the primary responsibility of the democratic State to provide protection and security to the people and, consequently, enact a statute to curb down the menace of cyber terrorism. However, the State has to be very cautious. Care must be taken so that innocent people are not beleaguered and their fundamental rights are not dishonoured, as all law derive strength not only from the authority of the State but also from the support of the people (Singh, 2008). There should be a balance between the security concern and human rights considerations. The regulatory and monitoring mechanisms, to deter, identify, and track terrorists, have to be there, but these should not jeopardise citizens' liberty and freedom (Singh, 2008).

To some extent, the impossibility of restraining terrorism while not jeopardising human rights cannot be denied. Still, if the misuse happens on a larger scale, it could be an onslaught on the democratic rule of law (Foggetti, 2010). In Niranjan Singh Karan Singh Punjabi v Jitendra Bhimraj (AIR 1990 SC 1962), the Supreme Court observed: 'When a law visits a person with serious penal consequences the State must take extra care. To ensure that innocent people are not roped in by stretching the language of the law [*Sic*]." Furthermore, Burke had rightly expressed his just apprehension more than two and half centuries ago in his letter to Hon. C.J. Fox (8 Oct. 1777), "People crushed by law have no hopes but from power. If laws are their enemies, they will be enemies to laws; and those, who have much to hope and nothing to lose, will always be dangerous, more or less". It is a well-accepted fact that society's security is, undisputably, the primary aim of a welfare state. Still, it is not the sole purpose; one of the most significant and foremost duties of the State is to protect the fundamental rights guaranteed in the Constitution. It would be ironic if, in the name of combating (cyber) terrorism, the rule of law is kept aside, and the State violates citizens' rights. Hence Section 66 (F) needs reconsideration as it is a disproportionate and discriminatory reaction to the menace of cyber terrorism. It is excessive and unfair as Section 66 (F) covers such acts which have no clear nexus with cyber terrorism. The sub-section (B) of Section 66 (F) should be deleted and should be restricted only to sub-clause (A) of Section 66 (F). Checks and balances need to be incorporated in Section 66 F by limiting its broad and unlimited scope. Thus, sub-Clause (B) of Section 66 (F) (1) needs to be deleted to narrow the content of the

definition of cyber-terrorism, and should not be a tool of exploiting the vulnerable section of the society.

REFERENCES

Abulhasan, N. (2020) Features of the Fight Against Modern Virtual Terrorism, *The American Journal of Interdisciplinary Innovations and Research,* 2(9), pp: 1–9.

DOI: https://doi.org/10.37547/tajiir/Volume02Issue09-01

Addicot, F. J. (2011) *Terrorism Law: Materials, Cases, Comments,* 1st Ed., Arizona: Lawyers & Judges Publishing Co.

Ade, P. (2015) Lone wolf Terrorism: How Prepared are India's Intelligence Agencies?, *Counter Terrorist Trends and Analyses,* 11(6), pp: 4–11.

Bhansali, S. (2012) *Commentary on Information Technology Act,* 1st Ed., New Delhi: Universal Publication.

Branscomb, M. L. (2007) *Science, Technology, and Countering Terrorism: The Search for a Sustainable Strategy: Proceedings of an Indo-USA Workshop* [Online] Available from: https://www.nap.edu/read/11848/chapter/2 [Accessed: 3rd October 2020].

Cardoso, T. D. A. & Da Rosa, R. S. G. (2016) Developments in the Global Legal Acknowledgment of Cyber Crimes and Cyber Terrorism: Uncertainties of a Modern Society, In Szkarat, M. & Mojska, K. (eds.) *New Technologies as a Factor of International Relations,* p. 278, Newcastle upon Tyne, UK: Cambridge Scholars Publishing.

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/story-TkUs7CAwKFEXwmWmMHkT8K.html [Accessed: 23rd October 2020].

Chupika, A. (2016) *The Strategies of Cyverterrorism: Is cyberterrorism an effective menas to Achieving the Goals of Terrorists?,* [Online] Available from: https://ruor.uottawa.ca/bitstream/10393/35695/1/CHUIPKA%2c%20Adam%2020169.pdf [Accessed: 15th September 2020].

Desai, D. & Bhatt, P. (2019) *Securing India's Cities: Remembering 26/11, Learning its Lesson* [Online] Available from: https://www.orfonline.org/research/securing-indias-cities-remembering-2611-learning-its-lessons-53066/ [Accessed: 3rd May 2020].

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

Foggetti, N. (2010) Cyber Terrorism and The Right to Privavcy in the Third Pillar Perspective, *Masaryk University Journal of Law and Technology,* 3(3), pp: 365–376.

Goel, S. (2020) National Cyber Security Strategy and the Emergence of Strong Digital Borders, *Connections: The Quarterly Journal,* Q19(1), pp: 73–86.

DOI: https://doi.org/10.11610/Connections.19.1.07

Guelke, A. (2010) *The New Age of Terrorism and the International Political System,* 1st Ed., New Delhi: Viva Books.

Gupta, S. (2004) The Changing Dimensions of International Terrorism and the Role of the Unites States: A Comprehensive and Multilateral Approach to Combat Global Terrorism, *The Indian Journal of Political Science,* 65(4), pp: 556–587.

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 [Accessed: 2nd October 2019].

DOI: https://doi.org/10.2139/ssrn.1964261

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.

Hoffman, B. (2017) *Inside Terrorism,* 3rd Ed., Columbia: Columbia University Press.

India, National Human Rights Commission (2000-2001) *National Human Rights Commission Annual Report 2000-2001* [Online] Available from: https://nhrc.nic.in/sites/default/files/Annual%20Report%202000-2001.pdf [Accessed: 3rd December 2019].

International Institute for Counter-Terrorism (ICT) (2018) Cyber-Crime and Cyber-Terrorism, In *Cyber Report 24 September-November 2017*, pp: 23-27, Herzlia, Israel: International Institute for Counter-Terrorism (ICT) [Online] Available from: http://www.jstor.org/stable/resrep17687.7 [Accessed: 23rd September 2019].

Kamath, P. M. (2001) Terrorism in India: Impact on national security, *Strategic Analysis,* 25(9), pp: 1081–1987.

DOI: https://doi.org/10.1080/09700160108459024

Kaplan, D. (2003) Playing Offense: The inside story of how U.S. terrorist, *U.S. News & World Report*, 2 June, pp: 19–29.

Kharmalki, G., Singh, N., Bipin, A., Gupta, S., Gupta, A., Dutta, S. & Gaur, G. (2018) *Indian Risk Survey 2018* [Online] Available from: http://ficci.in/Sedocument/20450/India%20Risk%20Survey%20-%202018.pdf [Accessed: 12th October 2019].

Klein, J. J. (2015) Deterring and Dissuading Cyberterrorism, *Journal of Strategic Security,* 8(4), pp: 23–38.
DOI: https://doi.org/10.5038/1944-0472.8.4.1460

Laquer, W. (1987) *The Age of Terrorism,* 1st Ed., Boston, USA: Little, Brown and Company.

Mahapatra, C. & Tripathi, A. (2007) *Transnational Terrorism: Perspective on Motives Measures and Impacy,* 1st Ed., New Delhi: Reference Publication.

Mali, P. (2012) *Cyber Law and Cyber Crime,* 1st Ed., New Delhi: Snow White Publishers.

Martin, G. (2011) *Essentials of Terrorism: Concepts and Controversies,* 2nd Ed., California: Sage Publications Inc.

Martin, G. (2004) *The New Era of Terrorism,* 1st Ed., California: Sage Publications Inc.

Martin, G. (2006) *Understanding Terrorism: Challenges Perspective and Issues,* 6th Ed., California: Sage Publications Inc.

Mates, M. (2001) *Technology and Terrorism, Rapporteur Report at NATO Parliamentary Assembly.* [Online] Available from: https://www.tbmm.gov.tr/ul_kom/natopa/raporlar/bilim%20ve%20teknoloji/AU%20121%20STC%20Terrorism.htm [Accessed: 23rd May 2019].

Minei, E. & Matusitz, J. (2012) Cyberspace as a new arena for terroristic propaganda: an updated examination, *Poiesis Prax,* 9(1–2), pp: 163–176.
DOI: https://doi.org/10.1007/s10202-012-0108-3

Mishra, B. (2002) Next Stop for Al-Qaida, *Times of India* [Online] 16th September, Available from: https://timesofindia.indiatimes.com/next-stop-for-al-qaida/articleshow/22281489.cms [Accessed: 2nd October 2019].

Mohanty, A. (2011) New Crimes Under the Information Technology (Amendment) Act, *The Journal of Law and Technology,* 7, pp: 103–120.

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

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 [Accessed: 23rd September 2019].
DOI: https://doi.org/10.1007/s10796-010-9275-8

Peter, L. B. (2001) *Holy War, Inc.: Inside the Secret World of Osama bib Laden,* 1st Ed., London: Weidenfeld.

Post, M. J., Ruby, G. K. & Shaw, D. E. (2000) From car bombs to logic bombs: The growing threat from information terrorism, *Terrorism and Political Violence,* 12(2), pp: 97–122.
DOI: https://doi.org/10.1080/09546550008427563

Press Trust of India (2019) Virtual SIMs used in Pulwama terror attack; India to approach U.S. for help, *The Hindu* [Online] 24th March, Available from: https://www.thehindu.com/news/national/virtual-sims-used-in-pulwama-terror-attack-india-to-approach-us-for-help/article26625294.ece [Accessed: 3rd October 2019].

Rajak, B. (2011) *Pornography Law,* 1st Ed., New Dellhi: Universal Law Publication.

Rajput, B. (2020) Legal Framework for Cyber Economic Crimes: A Review, In B. Rajput (ed.) *Cyber Economic Crimes in India,* pp: 145–169, Denmark: Springer, Cham.
DOI: https://doi.org/10.1007/978-3-030-44655-0_7

Ramsay, G. (2008) Conceptualising Online Terrorism, *Perspective on Terrorism,* 2(7), pp: 3–10.

Reddy O, C. (2010) *The Court and the Constitution of India,* 1st Ed., New Delhi: Oxford University Press.

Reich, P. C. (2012) Case Study: India - Terrorism and Terrorist Use of the Internet/Technology, In P. C. Reich & E. Gelbestein (eds.) *Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization*, pp: 377–408, Pennsylvania, USA: IGI Global.
DOI: https://doi.org/10.4018/978-1-61520-831-9.ch014

Robertson E, A. (2010) *Terrorism and Global Security,* 1st Ed., New Delhi: Viva Books.

Saxena, A. (2011) 117 Indian Government Websites Defaced Till July, *Medianama* [Online] 4th August, Available from: https://www.medianama.com/2011/08/223-indian-government-websites-hacked/ [Accessed: 17th August 2019].

Shourie, A. (2018) *Courts and their Judgements,* 2nd Ed., Noida, India: HarperCollins Publishers.

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.

Singh, S. (2019) *India's National Cyber Security Policy: Gaps and the way Forward* [Online] Available from: https://www.sspconline.org/sites/default/files/2019-11/SSPC_SAURABH_Monograph-Web.pdf [Accessed: 3rd December 2020].

Stytz, M. & Banks, S. (2014) Towards Attaining Cyber Dominance, *Strategic Studies Quarterly,* 8(1), pp: 55–87.

Sue, P. Griest & Mahan, S. (2003) *Terrorism in Perspective,* 1st Ed., California: Sage Publications Inc.

Sultan, Oz. (2017) Combatting the Rise of ISIS 2.0 and Terrorism 3.0, *The Cyber Defense Review,* 2(3), pp: 41–50.

Venkatachary, S. K., Prasad, J. & Samikannu, R. (2018) Cybersecurity and cyber terrorism - in energy sector – a review, *Journal of Cyber Security Technology,* 2(3-4), pp: 111–130.
DOI: https://doi.org/10.1080/23742917.2018.1518057

Venugopal, K. K. & Subraminium, G. (2011) *Restatement of Indian Law of Contempt of Court,* 1st Ed., New Delhi: Indian Law Institute.

Weimann, G. (2004) *Cyberterrorism: How Real is the Threat?* [Online] Available from: https://www.usip.org/sites/default/files/sr119.pdf [Accessed: 12th Feburary 2019].

Weimann, G. (2010) *Terror on the Internet: The New Arena and the New Challenges* [Online] Available from: https://www.usip.org/publications/2010/05/terror-internet [Accessed: 12th Feburary 2019].

Weingberg, L. (2006) *Global Terrorism: A Beginner's Guide,* 1st Ed., London, UK: One World Publication.

Whine, M. (1998) *Islamist Organizations on the Internet* [Online] Available from: https://www.ict.org.il/Article/295/Islamist%20Organizations%20on%20the%20Internet#gsc.tab=0 [Accessed: 23rd September 2019].