# CYBER TERRORISM/HATE SPEECH ON SOCIAL MEDIA: A REVIEW OF INDIAN LEGAL FRAMEWORK

Written by Rakesh Chandra

Research Scholar, Faculty of Law, Lucknow University

# **ABSTRACT**

The offence of cyber terrorism was introduced for the first time in the form of an amendment to the Information Technology Act,2000. During the last decade, India has been a witness to an unprecedented upsurge of terrorism. It is also an open secret that the terrorists are using cyber space in a big way. However, fight against cyber terrorism by any nation can't be won by one single provision alone. There is need for creating secondary legislation with regard to practices and procedures to be followed, in the context of cyber terrorism.

Presently, social media platforms' coverage spans the whole country. It's worst effect is reflected in its role of spreading hate speech. Mobile internet has added fuel to the fire. Section 66-A of the I.T. Act dealing with hate speech was struck down by the Supreme Court. An Expert Committee constituted by the Centre to suggest further steps and Law Commission both recommended inserting two new provisions in the IPC. The Criminal Law (Amendment) Bill, 2017 suggested by the Commission proposed to add section 153C and Section 505A in the IPC and make the necessary changes in the Cr.P.C Thus, either in cyber terrorism or hate speech, India still needs stringent laws.

*Keywords*: Cyber Terrorism, Social Media, Mobile Internet, Information Technology Act, Indian Penal Code.

# INTRODUCTION

The emergence and diffusion of hate speech online is an evolving phenomenon and collected efforts are needed to understand its significance and consequence as well as to develop effective responses. Hate speech in the times of Internet spreads like fire and it hurts collectively. Timothy Garton Ash in her phenomenal work, Free Speech, has aptly described the situation by stating,<sup>1</sup> "The internet has brought an explosion of offensive, extreme expression, exacerbated by the online norm of anonymity. Reacting instantly, behind the mask of a pseudonym, people jerk out things online that they would never say when using their real name in a face-to-face encounter or public meeting. If we believe in openness and robust civility, we must address this challenge."

Incitement is the natural corollary of hate speech. Sometimes, the root cause of terrorism is found to remain seeded in hate speech. The American analyst Susan Benesch has developed a set of five guidelines for determining when have speech becomes dangerous speech. One of her guidelines speaks about 'a means of dissemination that is influential in itself, for example because it is the sole or primary source of news for the relevant audience.' This element-the means of dissemination- is the one that has been transformed in our time.<sup>2</sup>

Sometimes the causal connection between hateful things expressed and atrocities committed seems relatively clear. For example, one study of the mass murder of Tutsis (and of some moderate Hutus) by Hutus in Rwanda in 1994 argued that there were 65 to 77 per cent more killings in villages which received the signal of Radio Television Libra des Mille Collines (RTLM), a popular radio station that broadcast repeated calls for a 'final war' to 'exterminate the cockroaches'. Even those analysts who question whether hate radio made such a decisive contribution to the genocide do not doubt that it played a part. <sup>3</sup>

Terrorism is the biggest danger for the survival of humanity in present times. Terrorists are taking help of information technology to spread their tentacles in far off places. How far online hate speech and cyber terrorism are denting the peaceful fabric of our society and how much

<sup>3</sup> *Ibid*. p135

<sup>&</sup>lt;sup>1</sup> Timothy Garton Ash; Free Speech, Ten Principles for a connected World, Atlantic Books, London, 2016, p.

<sup>&</sup>lt;sup>2</sup> *Ibid* p. 135.

150

we are equipped, legally to deal with these menacing problems, are the focus of the present study.

# HATE SPEECH/ CYBER HATE

Hate speech refers to expressions that advocate incitement to harm (particularly, discrimination, hostility or violence) based upon the target's being identified with a certain social or demographic group. It may include, but is not limited to, speech that advocates, threatens, or encourage violent acts. Hate speech lies in a complex nexus with freedom of expression, individual, group and minority rights as well as concepts of dignity, liberty and equality.<sup>4</sup>

Cyber hate, defined as "the use of any electronic technology to spread bigoted, discriminatory, terrorist and extremist information," manifests itself on website and blogs, as well as in chat rooms, social media, comment sections and gaming. In short, hate is present in many forms on the internet, creating a hostile environment and reducing equal access to its benefits for those targeted by hatred and intimidation.<sup>5</sup>

In an ideal world, people would not choose to communicate hate. But in the real world they do, all too often. And hate expressed online can lead to real-world violence, nearby or far away. Cyber hate poses additional challenges, because everyone can be a publisher on the internet. Hateful content can spread around the globe literally in seconds, and it often goes unchallenged.<sup>6</sup>

Cyber hate or hate in the cyberspace dates back to a decade. Initially hate was spread in emails and chat rooms. But now social networking websites is being used as the medium to spread hate. Social networking websites like Orkut, Facebook and Myspace was originally intended to allow people to "socialize with known or unknown individuals for the purpose of research, entertainment, establishment of friendships or relationships due to feelings of loneliness, and

Commonwealth Law Review Journal (CLRJ)

<sup>&</sup>lt;sup>4</sup> Countering Online Hate Speech, UNESCO SERIES ON INTERNET FREEDOM, available at http://unesdoc.unesco.org/images/0023/002332/233231e.pdf, accessed on 18.1.2018.

<sup>&</sup>lt;sup>5</sup> Responding To Cyber hate, Anti-Defamation League, March2016, available at http s://www.adl.org/sites/default/ files/ documents/ assets/pdf/combating-hate/ 2016-ADL-Responding-to-Cyber hate- Progress- and- Trends-Report.pdf, accessed on 18.01.2018.

sexual gratification" (Fraim, 2006, para 1). But these sites are now misused to the greatest possible extent.<sup>7</sup>

Hate speech can stay online for a long time in different formats across platforms, which can be linked repeatedly. As Andre Oboler, the CEO of the Online Hate Prevention Institute, has noted, "The Longer the content stays available, the more damage it can inflict on the victims and empower the perpetrations. If you remove the content at an early stage you can limit the exposure. This is just like clearing litter, it does not stop people from littering but if you do not take care of the problem it just piles up and further exacerbates." The architecture characterizing different platforms may allow topics to stay alive for shorter or longer periods of time. Twitter's conversations organized around trending topics may facilitate the quick and wide spreading of hateful messages, but they also offer the opportunity for influential speakers to shun messages and possibly end popular threads inciting violence. Facebook, on the contrary, may allow multiple threads to continue in parallel and go unnoticed; creating longer lasting spaces where certain individuals and groups are offended, ridiculed and discriminated.

The endurance of hate speech materials online is unique due to its low cost and potential for immediate revival, ensuring its contained relevance in particular spheres of discourse. Anonymity can also present a challenge to dealing with hate speech online. As Drew Boyd, Director of Operations at the Sentinel Project, has stated, "the internet grants individuals the ability to say horrific things because they think they will not be discovered. This is what makes online hate speech so unique, because people feel much more comfortable speaking hate as opposed to real life when they have to deal with the consequences of what they say." <sup>10</sup>

# Hate Speech Online: Legal And Non-Legal Measures

Recently, Cyber hate has become a legal issue in many countries, and custodial sentences have been given to people who use the Web to spread and incite hatred based on individual characteristics such as race, religion and sexual orientation. Arguably the U.K. (England and Wales) is the most progressive in this area. Legislation Pertaining to England and Wales that

<sup>&</sup>lt;sup>7</sup> K. Jaishankar, Cyber Hate: Antisocial networking in the Internet, Editorial, Open Access, July- December, 2008, Vol. 2 (2),16-20, available at http://www.cybercrimejournal.com/editorialijccjuly 2008.pdf, accessed on 18.1.2018.

<sup>&</sup>lt;sup>8</sup> Cited in Countering Online Hate Speech, UNESCO SERIES ON INTERNET FREEDOM, available at http://unesdoc.unesco.org/images/0023/002332/233231 e.pdf, accessed on 18.01.2018.

<sup>9</sup> *Ibid* 

 $<sup>^{10}</sup>$  Ibid

protects people from threatening, harassing, or grossly offensive speech online includes the Offences Against the Person Act, 1861, the Public Order Act 1986, the Malicious Communications Act 1988, the Protection from Harassment Act 1997, and the Criminal Justice Act 2003. Similar laws also apply in France, Denmark and the Netherlands. In the U.S. there are protections against posting harassing messages on the Web, without exposing personal identity. <sup>11</sup>Cyber hate continues largely unchallenged by law enforcement due to freedom of speech protections in the United States. Lewin (2002) studied how US right-wing groups promoted their goals on the web largely unchallenged by law enforcement, concluding that the online medium has been useful in hatemongers because it is economic, far reaching and protected by the First Amendment. <sup>12</sup>

## Position in India:

Law Commission of India defines hate speech as an "incitement to hatred primarily against a group of persons defined in terms of race, ethnicity, gender, sexual orientation, religious belief and the like", Thus, "hate speech is any word written or spoken, signs, visible representations within the hearing or sight of a person with the intention to cause fear or alarm, or incitement to violence." The Commission refers to hate speech as an expression likely to cause distress, offence or incite hostility towards a particular group.

The Law Commission in its 267<sup>th</sup> Report on 'hate speech' compares how the U.S. gives a wide berth to hate speech while international human rights Covenants and other Western democracies like Canada, Germany, and the U.K regulate it and subject it to sanctions.<sup>13</sup>

Section 66A of the Information Technology Act, 2000 contains the punishment for online hate speech offences. The Supreme Court struck down the controversial Section 66A in Shreya Singhal<sup>14</sup> case in 2015. Central Government Constituted an Expert Committee after the

<sup>&</sup>lt;sup>11</sup> Pete Burnap and Matthew L. Williams, Us and them: Identifying Cyber hate on Twitter across multiple protected characteristics, EPJ Data Science, a Springer Open Journal, available at http://link.springer.com/content/pdf/ 10.1140% 2 Fepjds% 2 Fs 13688-016-0072-6.pdf, accessed on 18.1.2018.

<sup>&</sup>lt;sup>12</sup> Matthew L. Williams and Pete Burnap, Cyberhate on Social media in the aftermath of woolwich: A case study in computational criminology and Big Data, available at https://academic.oup.com/bjc/article-pdf/56/2/211/7451319/ azv 059.pdf, accessed on 18.1.2018.

<sup>&</sup>lt;sup>13</sup> Krishnadas RajaGopal, Redefining hate speech, The Hindu, dt. 15.12.2017

<sup>&</sup>lt;sup>14</sup> Shreya Singhel Vs. Union of India, w.p(criminal)no.167 of 2012, Supreme Court of India.

Supreme Court struck down section66A, headed by former Law Secretary, Mr. T.K. Viswanathan. The Committee has recommended the following amendments<sup>15</sup>:

- Amend IPC section 153C to include in communication "spoken or written words, signs, visible representation, information, audio, video, or combination of both, transmitted, retransmitted through any telecommunication service, communication device or computer resource."
  - Punishment: Up to two years or fine of Rs.5000 or both.
- ii. By amending IPC section505A, punishment of any person or group of persons who intentionally, on grounds of religion, race, cast or community, gender, sexual orientation, place of birth, residence, language, disability or tribe, uses any means of communication to communicate.
  - Punishment: Up to a year, or fine of Rs.5000 or both.
- iii. Add sections 25B and 25C in the Code of Criminal Procedure, 1973, creating the post of a State Cyber Crime Coordinator and District Cyber Crime Cell, respectively.
- iv. Amendment to section 78 of the Information Technology Act, 2000: Allows a police officer not below the rank of Sub-Inspector to investigate any offence under this act. (report specifies young police officers, directly recruited as Sis, better equipped and trained to investigate cyber offences.)

According to Committee member Dr.S.Sivakumar, who is also a member of the Law Commission, "There was no need to re-introduce Section 66A, but we need to strengthen the Indian Penal Code instead."

Hate speech poses complex challenges to freedom of speech and expression. The Supreme Court realized this before asking the Law Commission for recommendations to arm the Election Commission with Laws to combat Hate Speech "irrespective of whenever they are made". In March2017, the Law Commission, led by former Supreme Court Judge, Justice B.S.Chauhan, recommended inserting two new provisions in the IPC, including speech that instills "fear or alarm" in the listeners, probably goading them to violence <sup>16</sup>

<sup>&</sup>lt;sup>15</sup> Seema Chishti, Change law to punish hate speech online, The Indian Express, 6.10.2017.

<sup>&</sup>lt;sup>16</sup> Krishnadas RajaGopal, Redefining hate speech, The Hindu, dt. 15.12.2017

154

The Criminal Law (Amendment) Bill, 2017 suggested by the Law Commission proposes to add Section 153C (prohibiting incitement to hatred) and section 505A (causing fear, alarm, or provocation of violence in certain cases) in the IPC and make the necessary changes in the Criminal Procedure Code. Thus, law regarding online hate speech in India is in the making.

## CYBER TERRORISM

Terrorism is arguably, the most dangerous portent for the peaceful existence of humanity and human values on earth in the 21stt century. There may be umpteen reasons for an ordinary person to become a terrorist. In *Terrorism and the Constitution*, David Cole and James X. Dempsey<sup>17</sup> argue that stifling dissent- a basic vehicle by which we question authority and bring about social change-may encourage individuals who don't value peaceful change.

However, despite the exponential growth of terrorism world over, there is no universally accepted definition of "terrorism" under International Law. Sami Zeidan, a Lebanese scholar, has analyzed the obstacles, to define terrorism:

"There is no general consensus on the definition of terrorism. The difficulty of defining terrorism lies in the risk it entails of taking positions. The political value of the term currently prevails over its legal one. Left to its political meaning, terrorism easily falls prey to change that suits the interests of particular states at particular times.<sup>18</sup>

In 2002, the European Union Council adopted Framework Decision 2002/ 475/JHA on combating terrorism. The Framework Decision harmonizes the definition of terrorist offences in all EU countries by adopting a common definition of the term "terrorism". Article 1 of the 2002 Framework Decision defines terrorism as extending to acts including extensive destruction of government or public facilities or infrastructures. The acts must seriously damage any country or any international organization. The acts must aim to seriously

<sup>18</sup> Sami Zeidan, Desperately Seeking Definition: The International Community's Quest for Identifying the Specter of Terrorism, 36 Cornell Int. L.J. 491, 491-92 (2004), available at scholarship.law.cornell.edu/cgi/viewcontent.Cgi?article=1530&context=cilj, accessed on 23.1.2018.

Commonwealth Law Review Journal (CLRJ)

<sup>&</sup>lt;sup>17</sup> Cited in Heidi Boghosian, Spying on Democracy, Open Media Series/ City Lights Books, San Francisco, 203, p. 267

intimidate a population or "unduly compel" any government or international organization to destroy the fundamental structures of a country.<sup>19</sup>

## Terrorist Use of Social Media: A New Challenge

As Internet proficiency and the use of social media grow ever- more universal, so too do the efforts of terrorist groups to exploit new technology in order to make materials that justify and sanction violence more accessible and practical. They are using Facebook, Twitter, YouTube and various other emerging platforms to spread their messages.<sup>20</sup>

#### i. The Internet and Self-radicalization:

In the past, plots were directed by foreign terrorist organizations or their affiliates, and recruitment and planning generally required some direct, face-to-face interaction with terrorist operatives. Today, individuals can find analogous social networks, inspiration and encouragement online, packaged neatly together with bomb- making instructions. This enables adherent to self radicalize without face-to-face contact with an established terrorist group or cell. Furthermore, individual extremists, are also increasingly selfradicalizing online with no physical interactions with established terrorists groups or cells- a development that can make it more difficult for law enforcement to detect plots in their earliest stages.<sup>21</sup>

#### ii. **Online Recruitment:**

Since 2014, the Islamic State of Iraq and Syria (ISIS) has been particularly aggressive in pursuing multiple sophisticated online recruiting and propaganda efforts. Twitter emerged as ISIS's platform of choice in part because it is able to conceal the identities of its users more effectively than other forums and social networking sites. ISIS's online presence is worldwide and presented in multiple languages. The terror group releases online magazines in Arabic, English, Turkish and French, and it has also released statements and videos in other languages, including Hebrew, Spanish's Russian, Kurdish and German.<sup>22</sup>

**June 2018** 

<sup>22</sup> Ibid

<sup>&</sup>lt;sup>19</sup> Cited in Ezekil Rdiker, The Incitement of Terrorism on the Internet: Legal Standards, Enforcement, and the Role of the European Union, Michigan Journal of International Law, Vol. 36, Issue 2, 2015.

<sup>&</sup>lt;sup>20</sup> Responding to Cyberhate, Progress and Trends, Anti Defamation League, New York, March 2016.

<sup>&</sup>lt;sup>21</sup> Ibid

## International Response to Cyber terrorism:

Since September 11,2001, the international community has orchestrated an organized response to terrorism n the Internet. The responses thereafter can be enumerated as such:

## (i) U.S.A.

A powerful weapon in the so-called 'war on terror' is the wiretap. Its use has predictably intensified since attacks of 11 Septemberr2001. Within six weeks of this date, the United States Congress had enacted the United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act). This was merely one of several measures that have been introduced to authorize the surveillance of a wide range of activities, including telephone calls, email, and Internet communications, by a number of law-enforcement officials. The provisions of a series of pre-11 September statutes- such as the Wiretap Statute, the Electronic Communications Privacy Act (ECAP), and the Foreign Intelligence Surveillance Act (FISA)- have been substantially amended, significantly diminishing their privacy safeguards.<sup>23</sup>

## (ii) European Union (EU):

The European Union has taken an active role in fighting cyber terrorism but cannot be said to have a unified and comprehensive approach.<sup>24</sup> The EU has actively encouraged its Member States to criminalize the incitement of terrorism. To this end, the EU has promoted a legal standard through the adoption of Framework Decisions<sup>25</sup> and the Council of Europe's Convention on the of Terrorism.<sup>26</sup>

In the United Kingdom, prosecutors, have wide discretion to determine when to prosecute the crime of inciting terrorism. They must take into account the right of freedom of speech, the context in which the statements were made, and the likelihood that they could effectively incite others to violence or hostility. In the wake of the 2005

<sup>&</sup>lt;sup>23</sup> Raymond Wacks, Privacy A very Short Introduction, Oxford University Press, New York, 2010, p. 73, 74.

<sup>&</sup>lt;sup>24</sup> EU Parliamentary Report, cited in Ezekeil Rediker, The Incitement of Terrorism on the Internet: Legal Standards, Enforcement, and the Role of the European Union, Michigan Journal of International Law, Vol. 36, Issue 2, 2015.

<sup>&</sup>lt;sup>25</sup> A Framework Decision is a legislative act of the EU used only within the EU's competences in police and judicial cooperation in criminal justice system. Ibid.

<sup>&</sup>lt;sup>26</sup> UNODC Report, Ibid.

London Bombings, the U.K. developed new policy guidelines. However, the 2006 Terrorism Bill ended up being a compromise since it dealt solely with the encouragement of terrorism, which" sill remains wider than the existing law of criminal incitement."<sup>27</sup>

## (iii) India:

India is facing a day-to-day trial of cross-border terrorism from its neighbour Pakistan. In fact, state of Jammu & Kashmir is constantly facing this crisis. In Kashmir, the local administration is facing dual crises. Apart from influx of terrorists from across the border there are home-grown terrorists in abundant numbers. Undoubtedly, these terrorists are indulging in cyber terrorism using advance cyber technology. Terrorists are uploading viral videos on social media sites as well. They are also making use of social media platforms like twitter, WhatsApp, Facebook etc. successfully to mould public opinion of Kashmiri people in their favour.

Viral videos that capture militants at play and leisure, shocking videos of alleged rights excesses committed by security forces on Kashmiri civilians, the alleged use of instant messaging platforms to mobilize stone pelters and recruit foot soldiers for militants and the frequent gags on internet foot soldiers for militants and the frequent gags on internet are bringing a paradigm shift in the narrative of the valley's conflict. But the government seems to be losing the online war, with the militants and separatists seemingly always a step ahead. The week-long protest calendar by separatists to mark Wani's first death anniversary calls for a "Kashmir awareness" Campaign on social media.<sup>28</sup> The security establishment tries to keep pace through its cyber cells but the government's main response is to snap mobile internet services. The suspension of 3G and 4G services in April was to curb the uploading of multimedia content that could provoke violence, while letting users access the basic minimum internet on their phones. Similarly, the April 26 order by State Home Secretary to ban 22 sites said the step was taken because the government felt that "continued misuse of social networking sites and instant messaging services is likely to be detrimental to the interests of peace and tranquility

<sup>&</sup>lt;sup>27</sup> Ibid

<sup>&</sup>lt;sup>28</sup> Abhishek Saha, Separatism Stays a step ahead on social media, Hindustan Times, dt. 7.7.2017.

in the State." The social media ban turned out to be a colossal failure. Most Kashmiri users switched on to Virtual Private Network (VPN) apps to overcome the ban and what came as a real surprise was that the who's who of Kashmir were all leading a busy social media life throughout the ban.<sup>29</sup>

Twitter has blocked several accounts and withheld dozens of tweets in many others after it received official communication from the Indian Government asking it to block accounts and tweets, most of these related to Kashmir. Invoking Section 69A of the Information Technology Act, 2000, the Ministry of Electronics and Information Technology asked Twitter on August 24 for blocking 115 twitter handles/ tweets.

Under the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, a committee of joint secretaries, from the ministries of IT, law and Justice, Home Affairs, Information and Broadcasting and the Indian Computer Emergency Response, can decide on any content to be blocked under the IT Act. The Ministry also asked for compliance report from Twitter.<sup>30</sup>

The punishment for Cyber terrorism has been stipulated in section 66 F<sup>31</sup> of the Information Technology Act, 2000. According to the Section 66 F (2), the offence shall be punishable with imprisonment which may extend to imprisonment for life.

<sup>&</sup>lt;sup>29</sup> *Ibid*.

<sup>&</sup>lt;sup>30</sup> Krishn Kaushik, Twitter blocks accounts and tweets on Kashmir after prod from centre, The Indian Express, September 5, 2017.

<sup>&</sup>lt;sup>31</sup> Section 66F- Punishment for Cyber Terrorism.

<sup>&</sup>quot;(1) Whoever-

<sup>(</sup>A) With intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by-

<sup>(</sup>i) denying or cause the denial of access to any person authorized to access computer resource; or

<sup>(</sup>ii) attempting to penetrate or access a computer resource without authorization or exceeding authorized access;

<sup>(</sup>iii) introducing or causing to introduce any computer contaminant; and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under Section 70, or

<sup>(</sup>B) Knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to 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 computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to 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, deformation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

159

The offence of Cyber Terrorism was introduced for the first time in the history of independent India in the form of an amendment to the Information Technology Act,2000. A perusal of the entire section clearly shows that it is talking about computer resources as also data, information and computer databases. The section defines cyber terrorism in the widest possible terms known across the world. How-ever, the section has not been very extensively utilized so far.

Here, it should be kept in mind very clearly that the fight against cyber terrorism by any nation cannot be won by one single provision alone. India requires far more detailed legal provisions to assist the effective implementation and applicability of Section66F the amended Information Technology Act,2000. Further, comprehensive procedures, processes and presumptions in relation to cyber terrorism need to be more elaborately detailed, whether in the Information Technology Act,2000. Or by means of secondary legislation which can help provide the platform for expeditious trial of cyber terror related cases. Also, there is need for creating secondary legislation with regard to practices and procedures to be followed. Lastly as times passes by, as more and more cases pertaining to cyber terrorism are likely to occur, there would be need for distinct cyber terror courts which would need to be duly trained in this regard and who can provide far more effective expeditious platform for expeditious trial of cyber related cases. 32

## CONCLUSION

Currently world is facing heat on account of online hate speech and cyber terrorism. In fact, both of these concepts are part of the same coin. Often hate speech gives rise to terrorist activities if it is directed against a particular race or community. Both the problems can't be dealt with effectively by one State or administrative unit. Since the reach of the Worldwide Web, as the name suggests, is the whole world, the domain of stakeholders is not limited to a single country. So, the cooperation among the world community is needed to deal with the twin

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extent to imprisonment for life."

\_

<sup>&</sup>lt;sup>32</sup> Pawan Duggal, Cyber Law, Universal Law Publishing Co., New Delhi, 2014, p.199-203.

problems. Further, we have to strive hard to reach a consensus in defining "hate speech" and "terrorism". Presently, we are not in a position to define 'terrorism' and regarding hate speech too, there is no unanimity of approach amongst the nations. Without doing so, it will not be possible to fight with these scourges. Moreover, it should be understood in most clear terms that use of force is not the ultimate solution to contain these cantankerous issues. We will have to resort to other means also, like educating the masses, social and political cohesion of the people living in a society and so on. Private actors like social media platforms owe an onerous duty in this regard. They will have to ensure that no such material which disturbs the existing structure of society is propagated through their sites for onward consumption. The state's role in keeping strict vigil continuously on such sites is imperative. The erring sites need to be punished accordingly. Last but not the least, the awareness of citizens play a key role in smooth functioning of a democracy. "Aware citizenry" is the most powerful deterrent for fighting such online aberrations which are very dangerous for the survival of humanity.

# **BIBLIOGRAPHY**

### **Books**

- Boghosian, Heidi, Spying On Democracy, Open Media Series, City Light Books, San Francisco, 2013.
- Wacks, Raymond; Privacy, A Very Short Introduction, Oxford University Press, New York, 2010.
- Duggal, Pawan; Cyber Law, Universal Publishing Company, New Delhi, 2014.
- Ash, Timothy Garton; Free Speech, Ten Principles for a Connected World, Atlantic Books, London, 2016

## **Articles**

- Countering Online Hate Speech; UNESCO SERIES ON INTERNET FREEDOM, UNESCO, 2015 available at http://unesdoc.unesco.org/images/0023/002332/233231e.pdf, accessed on 18.1.2018.
- K. JaiShankar, Cyber Hate: Antisocial networking in the Internet, Editorial, Open Access, July- December, Vol. 2 (2), 16-20, 2008, available at http://www.cybercrimejournal.com/editorialijcc july2008.pdf, accessed on 18.1.2018.

- Responding To Cyberhate, Progress and Trends, March 2016, available at https://www.adl.org/sites/default/files/documents/assets/pdf/combating-hate/2016-ADL-Responding-to-Cyberhate-Progress-and-Trends.pdf, accessed on 18.1.2018.
- Ezekiel Rediker, The Incitement of Terrorism on the Internet: Legal Standards, Enforcement, and the Role of the European Union, Michigan Journal of International Law, vol. 36/ Issue 2, available at https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1077&context=mjil, accessed on 18.1.2018.
- Pete Burnap and Matthew L. Williams, Cyber Hate Speech on Twitter: An Application of Machine classification and Statistical Modeling for Policy and Decision Making, Policy and Internet, available at http://onlinelibrary.wiley.com/doi/10.1002/poi3.85/epdf, accessed on 18.01.2018.
- Pete Burnap and Matthew L. Williams, Us and them: Identifying Cyber hate on Twitter across multiple protected characteristics, EPJ Data Science, available at https://link.springer.com/content/pdf/10.1140%2Fepjds%2Fs13688-016-0072-6.pdf, accessed on 18.01.2018.
- Matthew L. Williams and Pete Burnap, Cyberhate on social media in the aftermath of Woolwich: A case study in Computational Criminology And Big Data, Brit. J. Criminal(2016) 56. 211-238, available at https://academic.oup.com/bjc/article-pdf/56/2/211/7451319/azv059.pdf, accessed on 18.1.2018.
- Krishnadas Rajagopal, Redefining hate speech, The Hindu, 15.12.2017.
- Seema Chishti, Change Law to punish hate speech online, The Indian Express, 6.10.2017.
- Sami Zeidan, Desperately Seeking Definition: The International community's quest for Identifying the Specter of Terrorism, available at https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=1530&context=cilj, accessed on 23.1.2018.