HUMAN RIGHTS, CYBER TERRORISM & ROLE OF UNO: A CRITICAL ANALYSIS

Mr. GaneshappaDeshmane,
Asst. Prof. Law, School of Law,
SandipUniversity,
Nashik, Maharashtra, India.

Abstract: There is very close nexus between the cyber terrorism and Human Rights**.** In other word we can say that the result of the cyber terrorism is violation of the human rights. Human rights means the rights or situation which required every individual to live life with dignity. These rights are there irrespective of sex, caste, colour, religion, race, place or birth, age, language etc. etc.

In this paper author wants to high lights the issues raised by the cyber terrorism and its effects on human rights violation. Like the inadequacy of cyber laws available in India for cyber terrorism. The efforts taken by India at International level. The misuse of the Veto power by the permanent member of United Nation Security Council. There is a huge cry by the global leader that the veto power needs to be abolishing to establish the democratic environment in the United Nation which is the one of the apex international organisation[1]. Does this veto power possession members are playing political game at the cost of human right violation. Does the Counter-Terrorism Committee failed determine the strong strategy against terrorism? Is there any direct or indirect support from the develop country to the terrorist group?

*IndexTerms***:***Cyber Terrorism, Human Rights, Cyber Law, Veto Power. United Nation Security Council, Counter-Terrorism Committee, United Nations Organisation, etc.,*

1. Introduction:

There is very close nexus between the cyber terrorism and Human Rights**.**In other word we can say that the result of the cyber terrorism is violation of the human rights. Human rights mean the rights or situation which required every individual to live life with dignity. These rights are there irrespective of sex, caste, colour, religion, race, place or birth, age, language etc. etc.

In this paper author wants to high lights the issues raised by the cyber terrorism and its effects on human rights violation. The adequacy of Cyber laws available in India for cyber terrorism. The efforts taken by Indian in international level.The misuse of the Veto power by the permanent member of United Nation Security Council.There is a huge cry by the global leader that the veto power needs to be abolish to establish the democratic environment in the United Nation which is the one of the apex international organisation[2].

Concept of Crime: There is no universally accepted definition of the crime. Generally, the crime is defined as an unlawful act punishable by the state or any other controlling authority. If we see the ingredient of this definition it say that "an unlawful act" it means as per the definition if any act not cover by any law then it is not a crime. Means to determine crime law has to be there. On other hand

[1] http://www.jpost.com/International/World-leaders-call-for-end-of-United-Nations-veto-power-376443
[2] http://www.jpost.com/International/World-leaders-call-for-end-of-United-Nations-veto-power-376443

when we talk about the Human Rights we say that these are basic rights, fundamental rights, natural rights whether these are offered by any statutes or not it does not make any difference.

Another definition is that a crime/offence is an act harmful not only to some individual but also to a community, society or the state. Such acts are forbidden and punishable by law.

Element of Crime

*Actusreus*means the act and*mensrea*means the intention these two are the main essential of the most of the crime.For example if a person has an intention to kill another but he don’t do any act in furtherance of that then that is not the crime. Every criminal act violates the one or other human rights. Hence, it is imperative to understand the meaning of human rights.

2. Meaning of Human Rights:

Human rights are rights inherent to all human beings, whatever our nationality, place of residence, sex, national or ethnic origin, colour, religion, language, or any other status. We are all equally our human rights without discrimination. These rights are all interrelated, interdependent and indivisible entitled to. Most of the times below given human rights are getting violated through the cyber terrorism.

- **Universal Declaration of Human Rights, 1948**

The universal Declaration of the Human rights, 1948 is one of the important instrument on the human rights. Apart from this the International Covenant on Economic, Social and Cultural Rights and International Covenant on Civil and Political Rights two more instruments which talks about different human rights. However, in this article author has focused on the below given rights in the UDHR, 1948. All these are seems to be repeatedly violated through the cyber terrorism.

Article 1 states, all human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood. Cyber terrorism mainly act against the brotherhood as their intention is to provide the harm to the others.

Article 3states;everyone has the right to life, liberty and security of person. This article talks about the life, liberty and security however, cyber terrorism create the unsecure environment, threat to the life.

Article 27 states, we all have the right to our own way of life, and to enjoy the good things that science and learning bring.The terrorist group wants to compel the innocent person to follow their agenda.

Article 28 states, we have a right to peace and order so we can all enjoy rights and freedoms in our own country and all over the world. Here is the most violation of the human rights. The main agenda of the most of the terrorist is to create the unrest in the world.

Article 29- states, we have a duty to other people, and we should protect their rights and freedoms. Do terrorist act for the protection of the other rights? They are doing totally against it. Through the cyber terrorism they are violating one of the important human rights that is right to peace.

The next Article 30-says that,nobody can take away these rights and freedoms from us.[3] However, every move of the terrorist groups is to violate the various human rights granted by the different instruments.

[3] The human Rights of Universal Declaration 1948, https://www.amnesty.org.uk/files/udhr_simplified_0.pdf

3. Concept of Terrorism:

What is Terrorism?

Terrorism defined by Denning as “The unlawful use or threatened use of force or violence by a person or an organized group against people or property with the intention of intimidating or coercing societies or governments, often for ideological or political reasons.”

4. Concept of Cyber Terrorism:

Generally, the cybercrime means a crime in which computer or like devices used as tool to commit any offence. Cybercrime is a very broad term which include a number of crime like, hacking, cyber fraud, fishing, pornography, cyber stalking etc. Cyber terrorism is one of them still it is very different from the other crime as in other crime intention of the offender is personal gain. The intention in cyber terrorism is not the same. The cyber terrorism term was coined in the late 1980s, by Barry C. Collin.[4]

Another definition by The Centre for Strategic and International Studies (CSIS) has defined it as “the use of computer network tools to shut down critical national infrastructures (e.g., energy, transportation, government operations) or to coerce or intimidate a government or civilian population.[5]” Simply saying,if any incident in the cyber world can create terror, it may be called cyberterrorism.

There are around 11529 terrorist attacks are happen every year from 2006 to 2015 throughout the world[6]. The same is increasing day by day not only in number but also in atrociousness too.

- **What is Cyber terrorism?**

The below given are the few best definitions, of the cyber terrorism. There is no comprehensive definition of the terrorism as they are different agendas of them and they are changing the modus operenedi of the same day- by-day.

Ø “The premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub national groups or clandestine agents.” -Mark M. Pollitt.

Ø “[the] use of information technology and means by terrorist groups and agents.”-Serge Krasavin

Ø “Politically motivated hacking techniques used in an effort to cause grave harm, included but not limited to loss of life or serious economic damage.” -Larisa Paul[7]

- **Nature of Cyber terrorism:**

When we talk about the cyber terrorism we need to consider its main purposes. If we look at the nature then we can say that cyber terrorism is a species, as Cybercrime is a genus.

What make cyber terrorism different from other types of cybercrime is the aim or purpose of it. The aims of the cyber terrorism are as follows;

1. To create threat.
2. To get the confidential information of targeted government to damage the property.
3. To instigate/pursue and recruit the people to propagate their agenda as well as to execute their plan.
4. To keep updated and connected with other wrongdoer’s for the execution of their decided plan.
5. Use the digital communication technology to achieve their purpose.

- **Modus operandi of cyber terrorism**

[4] William L. Tafoya,Ph.D.,"Cyber Terror", FBI Law Enforcement Bulletin (FBI.gov), November 2011

[5] James Lewis, “Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats,” Center for Strategic and International Studies, http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf .

[6] https://www.statista.com/statistics/202864/number-of-terrorist-attacks-worldwide/

[7] [http://www.legalservicesindia.com/article/article/cyber-terrorism-quick-glance-1263-1.html]

Cyber terrorism itself includes various cybercrime to execute attack. Like, Identity theft, denial of services attack, to send the threating emails, to circulate the Jihad related material online and to instigate the targeted audience to join the terrorist group.

- **Issues posed by the cyber terrorism:**

Cyber terrorism has created various impediments before the investigating agencies as well as judiciary to hook the wrongdoers and punish them respectively. One of the major obstacles is insufficiency of the infrastructure. Easy method of the deletion of the available evidences in cyber space as well as to dilute the credibility and validity of the evidences. As per our law to punish the wrongdoer crime need to be proved beyond reasonable doubt. As the nature of the most of cyber terrorist activity is extraterritorial therefore issue of jurisdiction is there.

5. **Incidences of cyber terrorism attack.**

a. The Mumbai Attack:

The Mumbai police have registered a case of ‘cyber terrorism’—the first in the state since an amendment to the Information Technology Act—where a threat email was sent to the BSE and NSE on Monday. The MRA Marg police and the Cyber Crime Investigation Cell are jointly probing the case. The suspect has been detained in this case.

Status: The MRA Marg police have registered forgery for purpose of cheating, criminal intimidation cases under the IPC and a cyber-terrorism case under the IT Act[8].

b. ISIS supporter gets 20 years for cyber terrorism[9]: a case of combination of terrorism and hacking,

A 20 year-old from Kosovo has been arrested and sentenced to 20 years in prison for leaking confidential US military information to the Islamic State of Iraq and the Levant, announced the US Department of Justice. ArditFerizi hacked a US retailer and collected the data from tens of thousands of customers. He then used it to compile a hit-list of some 1,300 military and government personnel.

The ISIS supporter announced on Twitter that he had gained access to the personally identifiable information, which ISIL intended to use as a hit list. After sharing the document with JunaidHussain, a recruiter for ISIL, a link to the document was published on Twitter.

Farizi was captured in Malyasia and extradited to the US. Then He pleaded guilty.

c. Parbhani ISIS Cell Arrested, Used Black Tape on Cell phone Camera for Antisurveillance. ISIS operative planning to execute 'major operation' arrested in Parbhani.

Recently, Officer from Maharashtra Anti-Terrorism Squad (ATS) yesterday arrested a 31-year-old ISIS operative from Parbhani — radicalised by a Syria-based ISIS handler — who was preparing to carry out a ‘major operation’ soon. The operative was identified as Nazir Bin YafaiChausa middle-class family in Parbhani.

An officer said they received a tip-off about a man named Nazir who was using various platforms on the Internet to contact ISIS handler Faruq in Syria, following which they started monitoring his online activities.

Nazir and Faruq have been booked under relevant sections of Indian Penal Code (IPC) and the Unlawful Activities Prevention Act (UAPA) for acts of terrorism, recruiting members for terrorist activities, conspiracy, being member and supporting a terrorist organisation.

d. **Mumbai to Syria: More men from Malwani have joined ISIS[10].**

[8] [http://niiconsulting.com/checkmate/2014/06/it-act-2000-penalties-offences-with-case-studies/]

[9] https://hotforsecurity.bitdefender.com/blog/isis-supporter-gets-20-years-for-cyber-terrorism-16738.html

[10] http://www.mid-day.com/articles/mumbai-to-syria-more-men-from-malwani-have-joined-isis/16792193

Three Malwani-based youth are missing since October 30 and their families believe they left home to join the ISIS.
"The same day Mohsin and Wajid left home, more men from the group also went missing," said an ATS officer, All of them were in constant contact on WhatsApp and Facebook.

e. **Eight from Tamil Nadu, one from Telangana joined Islamic State in Syria: NIA[11]**
HYDERABAD: In a major blow to India's premier security agencies, nine persons -- eight from Tamil Nadu and one from Telangana -- are believed to have joined the Islamic State in 2016. The National Investigation Agency booked a fresh case to probe the matter on January 26, 2017.

The NIA learnt about the module of nine that was based in Chennai from central security agency inputs. The central agencies had interrogated three persons deported from Abu Dhabi for recruiting Indian youngsters for ISIS.

The agency's probe had recently revealed that the Chennai-based module of nine persons, including one from Telangana and eight from Tamil Nadu, all reportedly under the age of 30 had managed to join IS in Syria.

The NIA has registered a fresh case (Suomoto) following the directions of Ministry of Home Affairs under sections 120 B (criminal conspiracy) of the IPC, and Unlawful Activities (Prevention) Act, 1967.

f. **Kalyan youth, suspected to have joined ISIS, returns to Mumbai[12].**
KALYAN: ArifMajeed, one of four youths from Kalyan who had gone to Iraq and is reported to have joined the Islamic State, returned to India and was being interrogated by the NIA.
In May, four youths from Kalyan — Arif, FahadShaikh, SaheemTanki and AmaanTandel — went to Iraq to join the terror group ISIS. Later, however, they expressed a wish to be rescued and to return home.

g. **Revealed, the first NHS doctor to join ISIS: Hormone expert abandoned his hospital job and his wife and children to fight with jihadists[13].**
The first British NHS doctor to join ISIS in Syria has been revealed thanks to leaked ISIS recruitment papers.IssamAbuanza, 37, allegedly left his wife and two children behind in Sheffield when he fled the UK in 2014. Shocking images posted on social media appear to show Abuanza wearing an army uniform and clutching an AK-47 while reading the Koran.

A Palestinian doctor with British citizenship, Abuanza is said to have filled in ISIS registration forms when he crossed into Syria to join them on July 26 2014.

6. Information Technology Act and Cyber Terrorism:

Cyber terrorism denotes unlawful attacks and threats of attack against computers, networks and information stored therein to intimidate or coerce a government or its people for propagating hidden political or unlawful social and religious agendas. These attacks result in violence against persons or property or cause public unrest. Few examples could be explosions, plane crashes and

[11] http://defenceforumindia.com/forum/threads/eight-from-tamil-nadu-one-from-telangana-joined-islamic-state-in-syria-nia.78404/
[12] http://timesofindia.indiatimes.com/india/Kalyan-youth-suspected-to-have-joined-ISIS-returns-to-Mumbai/articleshow/45307316.cms
[13] http://www.dailymail.co.uk/news/article-3607249/First-case-British-NHS-doctor-going-Syria-join-ISIS-said-wanted-soldier-terror-group-s-entry-form.html

severe losses. Terrorists are known to use internet to prepare the schemes, raise funds and spread cyber terrorism. For instance, RazmiYousef who was a key person behind World Trade Centre attack had details schemes to destroy United States airliners encrypted files in his laptop computer[14].

- **Section 66F Punishment for cyber terrorism:**

(1) Whoever,-

(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 –

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

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorized access; or

(iii) introducing or causing to introduce any Computer Contaminant and by means ofsuch conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it 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

(B) knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computerdatabase, 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, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

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

The above section in the Information Technology Act deals with the cybercrimes including cyber terrorism which is again not comprehensive.

69 Power to issue directions for interception or monitoring or decryption of any information through any computer resource. -

(1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

(2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

[14] [http://www.legalservicesindia.com/article/article/cyber-terrorism-quick-glance-1263-1.html]

(3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to-

(a) Provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

(b) Intercept, monitor, or decrypt the information, as the case may be; or

(c) Provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.

Section 75 of the Information technology Act talks about the Extra-territorial jurisdiction, but it is not much helpful in absence of the extradition treaty.

Section 75 also extend to the ‘long arm jurisdiction’ available to catch the wrong doers in case of damages to the tangible as well as intangible property. Again, as far as cyber terrorism is concerned the long arm jurisdiction principle is also not of so much use as it is very difficult to trace the property of the terrorist group, file claim and recover damages.

7. International perspective: The Role of United NationOrganization

After the 2nd world war United NationsOrganisation has played very important role in maintaining peace at international level. After 2005 the UNO has started rigorously working against the terrorist activities. It has constituted different committees, prepared different plans, released various review report, determine various strategies and plans, The Security Council and General Assembly has passed several resolutions against the terrorist activities. The counter terrorism committee is continuously working on it. There are several documents available on the website of UNO. The Counter-Terrorism Committee Executive Directorate (CTED) by Security Council has taken more pro-active policy on human rights. Still the numbers of terrorist activities are increasing. Is it not the failure of UNO to stop the terrorism and protect the human rights internationally? If answer to the above question is yes, then we seriously need to look at it and find the reasons for the same. I find below reasons;

1. All Members of the UNO are not interested to stop the terrorism genuinely.
2. The dominant members of the UNO are indirectly supporting Terrorism.

   Out of the above two 2nd reason, I personally fill is very important, that some dominant countries and acting diplomatically on the issue of terrorism. For their personal agendas and interest they are directly or indirectly supporting the terrorism. They want to protect their interest at the cost of violation of human rights or rather we can say at the cost of the lives of people. The permanent members of the Security Council are misusing the Veto power for their personal gain. The recent example, the China has blocked the India’s bid at United Nation to ban the Jaish-e- Mohammadchief MasoodAzahar. This has again given rise to the few questions on Veto power.

   1. Does China playing the power politics?
   2. Does veto power is against the democratic values?
   3. Dose the concept of veto power needs to be relooked?
   4. What is the purpose of the veto power?
   5. Can veto power possessing country use the veto power for their agendas or gain at the cost of violation of human rights?

   If this is going to be the seen then we will not be able to control the terrorism and violation of human rights.

8. Conclusion :

The modus operandi of the Terrorism got changed due to the use of information Technology. From the above incidences we can see that how the terrorist groups through information technology are attracting the youth of the globe to join their organisation. Few local from different location are also getting attracted toward their assertion and motivating others to join this catastrophic path.

It is seen that the member of the United Nation Security Council are misusing the veto power for their personal gain at the cost of violation of human rights as well as life of the innocent people. On other hand on international level it has also been seen few countries are promoting terrorism for their personal gain and agendas. Even the veto power possessing members in united nation Security Council are also not behind in this. The recent case of AzaharMasood against whom the India had bit the UNSC relating to the declaration or Jaish E- Mohammad and MasoodAzhar.

Again, The Ministry of Home Affairs of India in its annual report has release how digital technology misused in the 26/11 Mumbai terrorist attack by extremist.

The Information Technology (Amendment) 2008 had incorporated though not in direct spirit but indirectly few provision are there which can cover the crime like cyber terrorism, however, considering the human rights violation life imprisonment is not the sufficient punishment for the cyber criminals. Therefore, I personally fill that, IT Act, 2000 is not a comprehensive statutes to eliminate the cyber terrorism completely and hence new statute is required.

At international level also we all need to come together to fight with terrorism as well as for the protection of the human rights globally.

9. Suggestions:

After the discussion of the above below are the few suggestions to control the cyber terrorism and prevention of human rights violation.

- ❖ Separate Act needs to be enacted focussing on the cyber terrorist activity as it is different cybercrime than other and considering the incidences.
- ❖ The cyber terrorism needs to be defined with the open ending definition to enable judiciary to keep pace with the changing Information Technology.
- ❖ Special provisions needs to be added into the Indian Evidence Act to dilute the test of "Crimes needs to be proved beyond reasonable doubt" if, we apply these test to cyber terrorism, chances are more that such offender get acquitted on the ground of non-proven of the cyber terrorist activity beyond reasonable doubt as the effect of the cyber terrorism is prima facie seen.
- ❖ Capital punishment should be impose on cyber terrorist without showing any sympathy to them as their intentions is very clear to break down the economy, damage the property, damage the communication system, to create the threat among the civilian and ruined the human rights.
- ❖ A separate body at international level needs to be constituted who will ban the terrorist groups throughout the world at the genuine request of any country.
- ❖ It has been seen that the veto power is misused by certain countries for their personal gain at the cost of huge violation of human rights throughout the globe. Therefore, guidelines need

to be prepare for the use of veto power. Like, if 2/3 countries possessing the veto power are agreed with something then disagreement of ¼ will not be consider.

Other References:

1. Information Technology Act, 2000
2. "Cyber Terrorism And Its Solutions: An Indian Perspective" By Praveen Dalal
3. Indian Penal Code, 1860
4. Unlawful Activities (Prevention) Act, 1967
5. "Cyber Terrorism: A New Dimension in Battlespace" by- Major J P I A G CHARVAT, SO2 Course Director Centre of Excellence Defence Against Terrorism.
6. "Putting Cyber Terrorism Into Context" By ZahriYunos, CyberSecurity Malaysia.
7. Journal of Information Technology Education Volume 3, 2004 Editor: Lynn Hunt Janet, "Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks" by- J. Prichard and Laurie E. MacDonald, Bryant University, Smithfield, RI, USA.
8. "Overview and Analysis on Cyber Terrorism", Steve Saint-Claire MSc and candidate to PhD in Computing Technology by the Department of Engineering and Technology of the School of Doctoral Studies of the EU.
9. Andrew M. Colarik, 'Cyber Terrorism: Political and Economic Implications' 2006 edition.
10. by Brian Blakemore,"Policing Cyber Hate, Cyber Threats and Cyber Terrorism" 2012 edition.
11. 'Cyberterrorism: Understanding, Assessment, and Response' Editors, Thomas M. Chen, Lee Jarvis, Stuart Keith Macdonald, Publisher Springer, 2014 ISBN 1493909630, 9781493909636.
12. https://www.un.org/sc/ctc/
13. http://www.un.org/en/sc/ctc/aboutus.html
14. https://en.wikipedia.org/wiki/Cyberterrorism
15. https://en.wikipedia.org/wiki/Human_rights

===