# A STUDY OF ACTS OF TERRORISM THROUGH CYBERSPACE IN INDIA: PREVENTION AND REMEDIES

# DEALING WITH CYBER AND TECHNOLOGY RELATED CRIMES

Shaily Jain & Shrishti Soumya[1]

## ABSTRACT

Cyber terrorism is a deadly menace imperilling the national security by offering a garb of anonymity to the perpetrators of terror. Malicious codes, viruses, worms and various new perils like electromagnetic pulse bombs and high-energy radio frequency weapons now create havoc in civilizations. India has been subjected relentlessly to this form of destruction since the past decade. From Mumbai's 26/11 attacks in 2008 to the Pathankot attack in 2016, the execution was primarily carried out through an aide in cyberspace. In numerous instances, China has hacked into the official networks of India allowing it to disable such networks during any conflicts. Inter-Service Intelligence (ISIS) and various Pakistani non-state Islamic terrorists have exponentially terrorized the citizens by influencing mindsets of individuals. Despite such threats, India lacks a comprehensive legislation to deal with cyber-terrorism.

The paper has been divided into two parts. Part – I discusses the rising incidents of Cyber Terrorism in India, the meaning and concept of the term, the motive and method behind an attack and the dangers involved. Part – II discusses the legal provisions on the national level, governance at the international level and how cyber terrorism might be a bigger menace and the future and how to fight it.

[1] Student, Institute of Law, Nirma University.

## INTRODUCTION

The third edition of the 'Global Terrorism Index 2015' ranked India as the 6th nation most distressed by terrorism out of 162 nations. Terrorism has plagued India since long back and various State and Non-State actors can be put to blame. However, significant changes in the trends of terrorism may be noted with the progression in technology and the increasing dependence of people on the same for all their activities. The use of internet in perpetrating terrorism in India can be traced back to the attack on the Indian Parliament in 2001 when the logo and a lot of other information pertaining to the Ministry of Home Affairs and the layout of the Indian Parliament were stolen with the help of information technology. Later, a laptop was seized through which the email system of the Indian Army was controlled through Pakistan's Internet Service Provider.[2]

Since 2006, the Chinese have been terrorizing the Indian government and private entities by unleashing cyber attacks consistently on their computer systems, and have been tracking the official networks, gaining access to the classified information on multiple occasions; which has empowered them not only to misuse such information, but also to disable any or all the networks during divergence on any subject matter and thus, get unfair advantage[3]. The Mumbai attack on 26/11/2008 is another instance when widespread horror and dread struck the nation by the way of information technology such as the use of Global Positioning Satellite systems, Voice over Internet Protocol, etc.[4] During the 2010 Commonwealth Games in India, the official websites of the Prime Minister's Office and multiple Government of India websites with the domain name 'nic.in' were hacked. The attack was possibly sourced by a state-actor, perhaps having Chinese origin, and had lasted for two months consequently leading to enormous data loss and more than 70 victims including multiple American government offices and business.[5] Majority of the attacks on India have so far been reported to stem from Pakistan, China, Bangladesh, Iran, Brazil, Turkey, Saudi Arabia, UAE, Algeria, Europe and the United States.[6] From 2001 to 2015, India has survived more than 57 terror attacks in which

[2] Ravi Kant, Prevention and Control of Cyber Terrorism, The Cyber Blog India, available at http://cyberblogindia.in/prevention-control-of-cyber-terrorism, last seen on 12/07/ 2016.

[3] Indrani Bagchi, China Mounts Cyber Attacks on Indian Sites, The Times of India (05/05/2008), available at http://timesofindia.indiatimes.com/india/China-mounts-cyber-attacks-on-Indian-sites/articleshow/3010288.cms, last seen on 15/07/2016.

[4] Khyati Jain, The SmeshApp Incident: Time to Take a Call on Cyber Terrorism, CSI Blog, available at http://www.cybersecureindia.in/the-smeshapp-incident-time-to-take-a-call-on-cyber-terrorism, last seen on 10/08/2016.

[5] Chinese Kept Hacking CWG Data for Two Months, The Times of India (12/08/2016), available at http://timesofindia.indiatimes.com/india/Chinese-kept-hacking-CWG-data-for-two months/articleshow/9521643.cms, last seen on 25/07/2016.

[6] Cyber Attacks on India Mostly from Pakistan, China: Government, The Economic Times (07/08/2015), available at http://economictimes.indiatimes.com/news/defence/cyber-attacks-on-india-mostly-from-pakistan-china-government/articleshow/48392113.cms, last seen on 26/07/ 2016.

cyberspace was the chief playing field including the 26/11 Mumbai carnage and the Pathankot strike for which critical information was scythed with the help of fake Facebook profiles.[7]

Another looming threat is from the Islamic State (ISIS) who have currently been focussing on communicating their messages tactically to the people across the world and gather ardent devotees by indoctrinating their ideologies about religion, politics, etc. In 2015, a 16 year old girl form Pune, Maharashtra was arrested by the Anti-Terror Squad who was brainwashed into leaving the country to join the Islamic State of Iraq and al-Sham (ISIS) by Sirajuddin, an ISIS recruiter, working at the Indian Oil Corporation, who was also arrested at Jaipur, Rajasthan.[8] The teenager had been in contact with around 200 IS followers through cyberspace and revealed their plans of expansion outside Syria and a massive attack on the Indian sub-continent by the year 2020.[9] The girl was an innocent young adolescent who was an exceptional student being educated in a convent school. However, swayed by the ISIS, she totally changed her way of living and espoused wearing burqa and was manipulated to join them as a suicide bomber.[10] Another incident involves a 'jihadi suspect', Mehdi Masoor Biswas who was a supporter of the IS activities and posted them on his Twitter account, "@ShamiWitness" putting the question before the Indian courts that whether 'open ideological support' would amount to terrorism.[11] The most recent attack on the Indian Defence Personnel was launched allegedly, by the Pakistan Intelligence Agencies by tricking them into downloading an application on their phones, called "SmeshApp".[12] The application is enabled to gather all the information including phone logs, text messages, e-mails and location through the GPS and possibly photographs can covertly be taken from the corrupted phone.[13] The application is considered to have possibly aided the Pathankot attack in January 2016.

The increasing numbers of aggressive attacks in the cyberspace clearly indicate that terrorism is no longer restricted to the traditional methods of suicide bombings, explosives and mass destruction. Along with the advancement of technology and increasing reliance of the people all over the world on the internet, even terrorism has evolved with new perilous aspects. These cases evidently illustrate that the terrorists have

[7] Jayadev Parida, Need to Beef up India's Cyber Security Policies and Mechanisms, available at http://www.orfonline.org/research/need-to-beef-up-indias-cyber-security-policies-and-mechanisms/, last seen on 30/07/2016.

[8] Pune Girl Who Wanted to Join ISIS Arrested, India Today (18/12/2015), available at http://indiatoday.intoday.in/story/pune-girl-who-wanted-to-join-isis-arrested/1/550103.html, last seen on 05/08/2016.

[9] Kiran Tare, 'Radicalized' Pune Girl Revealed ISIS Grand Plan to Attack India, The Indian Express (19/12/2015), available at http://www.newindianexpress.com/nation/Radicalised-Pune-Girl-Revealed-ISIS-Grand-Plan-to-Attack-India/2015/12/19/article3185052.ece, last seen on 06/08/2016.

[10] Ibid.

[11] Bharadwaj and Veeraraghav, Terror on Twitter: The Life and Crimes of Mehdi, The Hindu (28/12/2014) , available at http://www.thehindu.com/sunday-anchor/terror-on-twitter-the-life-and-crimes-of-mehdi/article6731135.ece , last seen on 10/08/2016.

[12] Supra4.

[13] SmeshApp: Cyber Terrorism is Real, but What Is It and What Can We Do about It, Tech 2, available at http://tech.firstpost.com/news-analysis/smeshapp-cyberterrorism-is-real-but-what-is-it-and-what-can-we-do-about-it-304701.html, last seen on 15/08/2016.

found the worst possible use for the most advanced technologies. These acts of perpetration of terrorism in the cyberspace that often result in actual destruction of life and property can be termed as 'cyber terrorism'.

## THE CONCEPT OF CYBER TERRORISM

Every researcher comprehends different ideas about cyber terrorism. However, the most accepted understanding of the concept is the use of internet for carrying out terrorist activities. According to Dorothy Denning, a leading expert in the field, cyber terrorism can be referred to the "unlawful attacks or threats of attacks against computers, networks, and information stored therein, when done with the intention to intimidate or coerce a government or its people, or in furtherance of political or social objectives"[14]. The definition focuses on the unauthorized users who gain access to information by different ways of cyber attacks with the intention to threaten and cause harm to the government and the society, and achieve political and social objectives. Such attacks may be made inside or outside the organization by use of internal or external networks.[15] Various definitions by different researchers focus upon varied aspects such as source and target of the attack, intention of the terrorists, means used thereby and the consequences of the attack.[16] The Federal Bureau of Investigation provides an understanding as, "the intimidation of civilian enterprise through the use of high technology to bring about political, religious, or ideological aims, actions that result in disabling or deleting critical infrastructure data or information."[17]

The provision for the offence of cyber terrorism in India has been provided under Section 66F of the Information Technology Act, 2002 prescribing imprisonment extending to life as punishment for the same. It defines the act of cyber terrorism as:

"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 authorization or exceeding authorized access; or
> (iii) introducing or causing to introduce any computer contaminant,

[14] Amar Singh, Spectre of Cyber-terrorism: A Potential Threat to India's National Security, 5 Paripex Indian Journal of Research (2016), available at http://worldwidejournals.com/paripex/file.php?val=March_2016_1459421461__05.pdf , last seen on 15/08/2016.

[15] Ali Mazari & E. Nyakwende, Cyber terrorism taxonomies: Definition, targets, patterns and mitigation strategies, 6 International Journal of Cyber Warfare and Terrorism (2015) available at https://www.researchgate.net/publication/282985438, last seen on 05/08/2016.

[16] Ibid.

[17] FBI Law Enforcement Bulletin, The Federal Bueau of Investigation, available at https://leb.fbi.gov/2011/november/cyber-terror, last seen on 06/08/2016.

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 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 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, 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."

The scope and extent of the concept in the Indian statute has been elaborated upon in the second part of the paper. However, it can be deduced that cyber terrorism entails attacks made through computer systems and networks against the government or citizens of the nation, with certain social, ideological or political reasons and the motive to threaten, intimidate or cause physical destruction to life and property and perpetrate terror and violence in the society which may result in explosions, destruction of life and property and critical financial losses.

## THE MOTIVE AND METHOD BEHIND AN ATTACK

The 'cyber terrorists' may have multiple agendas behind cyber attacks such as to send out their message to the government and the society, recruit supporters or brainwash the innocent, raise funds for their unlawful activities, demand ransom, gather critical information so as to enable them in further acts of terrorism, preparation for physical attacks, destruction of critical or classified information so as to disable the government to take measures or actions against them or harm the governance system, peace and order in the nation. The most vulnerable targets to cyber terrorism includes the government, military, critical national infrastructures, social and national identity and private entities.[18]

Cyber terrorism can take distinctive forms. In December 24, 2008, the official website of the Indian Eastern Railways was hacked into by Whackerz-Pakistan.[19] The website displayed unusual and offensive notes including threats for future cyber attacks and 'to save the motherland from turning into pieces.'[20] The visitors to the website were also attacked by the Trojan virus and it had taken nearly three hours to secure the site. Such a method of cyber attack is often used by 'hacktivists' who hack into the websites or database

[18] Supra2.

[19] Rohit Khanna, Pak Hacker Attacks E Rlys Site, Threatens Cyber War on India, The Financial Express (26/12/2008), available at http://www.financialexpress.com/archive/pak-hacker-attacks-e-rlys-site-threatens-cyber-war-on-india/402609/ , last seen on 7/08/2016.

[20] Ibid.

of multinational corporations or government as a hostile response to their actions and make political statements, threats or demands or sometimes for the purposes of fraud, identity theft or to steal information.[21] The attacker often vandalizes the authorized content displayed on the official website and puts on view the messages he wants to convey. Such an act amounts to 'website defacement'. Besides hacking into a system or a website, an attacker might remotely control programs installed on a system through 'bots' and gain control over a large number of computers which, after gaining control over them, are called 'zombies'.[22] The Indian metros across various cities including Mumbai, Delhi, Bangalore, Cochin, Hyderabad and Pune have reported an alarming rate of 65% of infection. In 2014, India ranked as 16th most bot-infected country in the world.[23] Another mode of attack may involve use of a software program, such as key logger, which observes and registers the keystrokes of a user and passes the classified information to the accessed data such as passwords, to the attacker.[24] In January 2015, the American chain of Hyatt Hotels Corporation were attacked worldwide with a malware to collect details of the payment card of its customers, including 20 out of the 23 hotels in India.[25] This is an instance of a cyber attack through malwares or viruses whereby the invader infects the network by means of e-mails, attachments, or even a Wi-Fi connection. Another mode of attack may involve Denial of Service (DoS) or Distributed Denial of Service (DDoS) whereby the attacker floods the targeted system with traffic, junk data etc, so as to prevent the access to the targeted website or computer which usually crashes down and is rendered inoperative for effective communication.

Usually, the attack originates from multiple sources and it becomes difficult to detect the legitimate user traffic making it impossible to obstruct the overwhelming requests to the targeted system by blocking the IP address.[26] In April 2015, the Telecom Regulatory Authority of India (TRAI) had released a consultation paper for the citizens to assert their opinions on the debate of net neutrality. Over 1 million of the names email addresses of people who posted their views on the debate were leaked by the TRAI. Subsequent to that, a group called 'AnonOpsIndia' brought the website down and disclosed that they launched a DDoS attack as revenge for leaking the details and making those people vulnerable to hackers and spammers.[27] These attacks are no longer restricted to websites or computer systems anymore. The threat has reached to

[21] Aparna Viswanathan, Cyber Law: Indian and International Perspectives, Lexis Nexis, 13 (1st ed., 2012).

[22] Ibid.

23India is the 16th most bot-infected country worldwide: Symantec, News 18 (23/04/2015), available at http://www.news18.com/news/tech/india-is-the-16th-most-bot-infected-country-worldwide-symantec-983542.html last seen on 12/08/2016.

[24] Supra7.

[25] Divya Sathyanarayanan, Hyatt's India Properties Hit by Malware Too, Economic Times (18/01/2016), available at http://economictimes.indiatimes.com/industry/services/hotels-/-restaurants/hyatts-india-properties-hit-by-malware-too/articleshow/50618887.cms, last seen on 13/08/2016.

[26] V. Beal, DDoS Attack – Distributed Denial of Service, Webopedia Blog, available at http://www.webopedia.com/TERM/D/DDoS_attack.html, last seen 14/08/2016.

[27] Swati Khandelwal, TRAI Leaked over Million Email Addresses: Anonymous India Takes Revenge, The Hacker News (27/04/2015), available at http://thehackernews.com/2015/04/net-neutrality-trai-emails.html, last seen 14/08/2016.

the 'Internet of Things (IoT) or internet connected devices' including smart TVs, refrigerators, printers, etc. Very recently, 25,000 CCTV cameras were usurped to jeopardize other services 'from 105 countries with an aggregate of 25,513 unique IP addresses within a few hours'. The researchers claimed it to be a massive 'Layer 7 DDoS attack that overwhelmed Web servers, occupying their resources and crashing websites'.[28]

## THE MENACE OF CYBER TERRORISM

Reliance upon the technology and dependence upon the internet has provided the terrorists with a new platform to attack and cause large-scale destruction in a very easy manner, low costs and at a high speed. The option of attacking the national security of a country online would seem more feasible since an attacker is enabled to operate from anywhere in the world with a garb of anonymity and it would be nearly impossible to detect him. Breach in the computer security can go undetected unless there is very strong protection software denying unauthorized access to the critical information.[29]

Cyber terrorism can not only cause destruction on computers or the internet but can cause large scale devastation, cost thousands of lives and demolition of property which may lead to grave damage to the financial state of a nation and complete breakdown of the nation's critical infrastructure denoting "all those assets or parts thereof which are essential for the maintenance of critical societal functions, including the supply chain, health, safety, security, economic or social well-being of people whose importance is such that any entire or significant loss or impairment of function could cause serious damage to human welfare, serious damage to the environment, serious damage to the national security or serious negative impact on the national economy."[30]

However, there is another view to the problem which raises the question if cyber terrorism is a real and indisputable menace, causing not only disorder but actual destruction. It is debated that the most essential element of terrorism is that 'the violence has a dramatic purpose: to provoke fear, dread and terror in a wider audience, an audience extending beyond the immediate victims of the attack'[31] and that so far there has scarcely been any incident where a cyber attack has resulted in massive violence and immense fear among the general public necessary to constitute 'terrorism'. Many would argue that distributed denial of service or web defacement or hacking may crash the system or the website, bringing about frustration to the user due to unavailability or display of offensive content, however, none of these instigate dread or alarm or physical terror that is the consequence of actual terrorism. Many critics also argue that the conception of cyber

[28] Swati Khandelwal, IoT Botnet – 25,000 CCTV Cameras Hacked to Launch DDoS Attack, The Hacker News (28/06/2016), available at http://thehackernews.com/2016/06/cctv-camera-hacking.html, last seen on 14/08/2016.

[29] Dr. Gupta and Agarwal, Cyber Laws, 369 (1st ed., 2008).

[30] Clive Walker, Governance of the Critical National Infrastructure, P.L. 2008, Sum, Pg. 323-352.

[31] Michael Kenney, Cyber-Terrorism in a Post Stuxnet World, available at http://connection.ebscohost.com/c/articles/100082206/cyber-terrorism-post-stuxnet-world , 59 Orbis 111 (2015), last seen on 14/08/2016.

terrorism is deficient and defective. According to their views, cyber terrorism should include any use of the internet by the terrorists in any execution of their plans including, “posting videos of attacks online, and building websites to attract supporters, raise funds or research targets.”[32] However, one may reasonably argue that terrorists also use various other devices to facilitate themselves in their activities such as cell phones. But one may not term the consistent use of cell phones as ‘cell phone terrorism’.[33] The view holds that cell phones, internet etc are mere ‘instruments’ that assist them to hit their targets and any speculations on the subject would be moot deliberations.

Nevertheless, cyber-terrorism is not entirely a conjecture of mind. Even if it is believed that terrorists have not caused an attack of a large magnitude so far so as to completely breakdown a nation and terrorize the citizens to their core, it cannot be guaranteed that it is entirely impossible in the distant future. Cyberspace, has so far, proven to be an effective weapon for physically demolishing national critical infrastructure with high casualty rate or to threaten a government to extort ransom or meet any demand on any stipulation by the terrorists. Since cyberspace has a lot of potential of causing massive destruction without the risk of exposure at costs significantly low than the actual terrorism, terrorists can invest to build new and deadly ‘cyber weapons’ with the advancing technologies. The government cannot put its feet up believing that the terrorists are not likely to pursue cyber terrorism as a means to strike and should allocate resources to develop measures to stymie the possibilities of cyber attacks of any kind.

## PART – 2

## INDIAN GOVERNMENT INITIATIVE TO COUNTER CYBER TERRORISM

The Government of India has, time and again, proved that it is not at leisure with the ongoing attacks in the cyberspace and has been constantly dealing with the consequent shock and panic among the general public and the threat to the national security. However, the appropriate time, mode, impact and efficacy of such governmental action remain a major concern and calls for preventive measures on part of individuals, firms and corporations.

### Information Technology Act, 2000

One of the most indispensable features of a proficient legal system is that it should keep pace with the changes in the society. Promulgation of Information Technology Act, 2000 was aimed at catering to such changes which were transforming the world at large. But, this act proved to be deficient as its provisions

[32] Ibid.

[33] Ibid.

aimed at holstering the e-commerce, whereas, cyber crimes were not given much thought.[34] The act barely contained ten sections which dealt with cyber crime. The legislators could not fathom the unbridled speed at which technology could outrun this law. By 2008, when "The Information Technology Amendment Bill 2008" was passed the world had drastically changed and the line between real world and the virtual world was blurring. By then, cyber –terrorism had already reared its ugly head in the country. Introducing provision related to this menace was indeed a need of the hour. In fact, this amendment was a knee-jerk reaction to the 26/11 terror attacks that shook the whole nation in 2008.[35] The main focus of this Act was on the aspects related to cyber-crime and cyber-terrorism.[36] Section 66F was introduced through this amendment which talks about Cyber Terrorism and punishment for the same. This section includes all such acts in cyber-terrorism, which are threat to the unity, integrity, sovereignty and security of the nation or strike terror in minds of people through disrupting the authorised access to a computer resource or getting access to a computer resource through unauthorised means or causing damage to computer network.[37] If these acts cause injuries to persons, cause death of any person, damage or destruct any property, causes disruption of essential supplies or services, or negatively affect the critical information structure, they become punishable in nature. The punishment for this offence is from three years up to imprisonment for life depending upon the gravity of the act. However, while this section attempts to define cyber-terrorism, it is almost impossible for one section to include all acts that might amount to cyber-terrorism. The world has not even come to a consensus regarding the definition of terrorism itself. When we come to 26/11 attacks, the terrorists just used communication services to provide an aide to the terrorists who had invaded the Taj Hotel. This communication aide does not come within the ambit of this section.[38] Even though Section 66F does not talk about communicational aspect, Section 69 talks about issuing directions regarding interception, decryption or monitoring of information using a computer resource. Section 69A talks about blocking public access to any information, whereas Section 69B takes into account monitoring and collecting traffic data for Cyber Security. Hence, the act has taken into consideration communicational aspect, although it has failed to do so when it comes to Section 66F. The challenge here is to include the aspect of communication aide to the propagation of terror in this Section so that this becomes an effective tool for combating cyber-terrorism.

[34] Dr. Maneela, Cyber Crimes: The Indian Legal Scenario, 11 US-China Law Review 570, 573 (2014).

[35] N. S. Nappinai, Cyber Crime Law in India: Has Law Kept Pace with Emerging Trends, 5 Journal of International Commercial Law and Technology (2010), available at http://www.jiclt.com/index.php/jiclt/article/viewFile/97/96, last seen on 20/08/2016.

[36] Ibid. See Section 66F, Information Technology Act, 2000.

[37] F Cassim, Addressing The Spectre of Cyber Terrorism: A Comparative Perspective, 15 Potchefstroom Electronic Law Journal (2012), available at http://www.saflii.org/za/journals/PER/2012/27.pdf, last seen on 22/08/2016.

[38] Debarati Haldar, Information Technology Act and Cyber Terrorism: A Critical Review, Social Science Research Network, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1964261, last seen on 25/08/2016.

## Cyber Security Policy, 2013

India lacked a proper Cyber Security Policy before 2013, and this status quo would have remained intact for a while had it not been for Edward Snowden, the whistleblower who leaked National Security Agency's documents. [39]This leak bared before the world the vulnerabilities that the cyber space was susceptible to. Department of Information Technology (DIT) released the National Cyber Security Policy in 2013, setting high goals and covering plethora of initiatives from capacity building to a proper framework for emergency response. But this policy has faced a lot of flak for not being at par with the policies of cyber mature nations. First of all, India still does not have an adequate national security doctrine and even the strategy that is being practiced is inadequate.[40] A legislative lacuna that this policy faces is that it did not go through public evaluation being just a policy, and cyber agencies ignore it on the pretext of this policy being neither binding nor enforceable. Moreover, with advent of new technologies like cloud computing and ever-increasing customer base for smart phones, the shift of miscreants has shifted towards these mediums while the policy does not take these into consideration.[41]

Recently, adhering to the cyber security policy, government of India has undertaken various initiatives to counter cyber-terrorism and various organisations have been formed to manage India's cyber community. National Informatics Centre is responsible for e-governance and assists Central Government bodies, State Government bodies, District level and other government bodies.[42] It provides decentralised government services, communication network throughout the country and other information technology services.

Under the Department of Information Technology (DIT), there is a Computer Emergency Response Team (Cert-in), formed in 2004, which assists the law enforcing agencies in their combat efforts.[43] This team works to maintain the security of the cyber space through, as specified in its mandate, "enhancing the security communications and information infrastructure, through proactive action and effective collaboration aimed at security incident prevention and response and security assurance".[44]

[39] A. Verma and A. Sharma, Cyber Security Issues and Recommendations, 4 International Journal of Advanced Research in Computer Science and Software Engineering (2014), available at http://www.ijarcsse.com/docs/papers/Volume_4/4_April2014/V4I4-0448.pdf , last seen on 17/08/2016.

[40] Time for a National Security Doctrine, The Hindu (05/01/2016), available at http://www.thehindu.com/opinion/editorial/editorial-time-for-a-national-security-doctrine/article8065314.ece, last seen 27/08/2016.

[41] Captain S. Chhabra, India's National Cyber Security Policy (NCSP) and Organization- A Critical Assessment, Naval War College Journal, available at http://www.indiannavy.nic.in/sites/default/themes/indiannavy/images/pdf/resources/article_6.pdf, last seen on 15/08/2016.

[42] Col. SS. Raghav, Cyber Security in India, available at http://ids.nic.in/art_by_offids/Cyber%20security%20in%20india%20by%20Col%20SS%20Raghav.pdf, last seen on 20/08/2016.

[43] Supra33.

[44] Supra38.

Cert-in also manages National Information Security Assurance Programme (NISAP) which calls for security policy for government and other critical infrastructure. It makes it mandatory for organizations to have a proper cyber security control and report any suspicious incidents to Cert-in. This programme also allows Cert-in to create a panel of auditors who will audit the organizations once a year. The organizations are required to keep Cert-in updated about their security compliance on a periodic basis.[45]

In 2011, National Critical Information Infrastructure Protection Centre (NCIIPC) was created as a sub-division to Cert-in to avert crisis when it comes to critical Infrastructure such as defence, energy, space, telecom, banking and so on. National Technical Research Organization is also responsible for maintaining the critical infrastructure of the nation. But experts believe that these organizations have not really been successful in maintaining their objectives.[46]

## COMBATING CYBER TERRORISM AT INTERNATIONAL LEVEL

At international level, the perils of cyber-terrorism have been acknowledged and potential measures are being gravely considered. United Nations is the biggest platform at the international level which has given importance to a need to fortify the world against cyber-terrorism. The major objective of the United Nation is to maintain the equilibrium of peace and security. Generally the UN works through legal instruments like conventions or other legal framework for the suppression of terrorism acts. UN already follows various resolutions to combat terrorism and has also established a Counter Terrorism Committee. A few relevant resolutions when it comes to cyberspace are – Resolution 56/121 (2001) which is on "Combating the Misuse of Information Technology" and Resolution A/RES/2321 adapted by UN General Assembly which focuses on cyber terrorism, public awareness and mentions standard penalisations in case of different types of attacks. General Assembly also adapted another resolution in 2010 on "creation of a global culture of cyber security and taking stock of national efforts to protect critical information infrastructures".[47] These resolutions guide the member states to develop their legal framework and policies keeping in mind the work done by Commission on Crime Prevention and Criminal Justice, and also the international and regional organizations which are working for restraining cybercrimes.[48] These resolutions also advocate the need for

[45] Ibid.

[46] Supra41.

[47] P. Tehrani, N. Manap and H. Taji, Cyber Terrorism Challenge: The need for a global response to a multi-jurisdictional crime, Computer Law & Security Review (2013), available at https://www.researchgate.net/publication/257101606, last seen on 27/08/2016.

[48] Judy R. Westby, International Guide to Cyber Security, American Bar Association (2004), available at https://books.google.co.in/books?id=zjFrE0DvdgkC&pg=PA1&lpg=PA1&dq=judy+westby+international+guide+to+cyber+security&source=bl&ots=OPQKV7k0bH&sig=-dE9UMyOUymTIuz2K6kt4lWkgKU&hl=en&sa=X&ved=0ahUKEwiw3ZKd0-

multilateral cooperation amongst the member states and encourage them to adopt measures to combat and limit the potential threats.

UN is playing a vital role in fighting against cyber terrorism by evolving sound and coordinated strategies. Howsoever, it is also true that the UN has to be dynamic and hence requires conceptual adaptation and structural changes to meet the changing dimensions of cyber terrorism.

The Council of Europe created a Convention on Cyber Crime through its "Committee of Experts on Cyber Crime". It has even non-European states as its member. Its main focus is on controlling cybercrimes at an international level. This convention divided criminal offences into four categories – "offences against confidentiality, integrity, and availability; computer-related offences; content-related offences; and offences against infringements and related rights."[49] It attempts to establish a common criminal policy at a global level to curb cyber-crime and cyber terrorism through international co-operation and managing computer network through globalised action. It also tries to deal with issues such as disclosing traffic data, intercepting the content, search and seizure of computer data and so on. It also allows for a trans-border access to the member states to stored computer data and establishing a network for speedy assistance between signatory nations. This convention does not directly address the issue of cyber terrorism, although Article 14(2) sub-clause (b) and (c) of the convention include criminal offences committed through the means of computer and collection of evidences in electronic form, hence, can facilitate in addressing the issue of cyber-terrorism. But this convention has not yet been able to harmonize cybercrime laws of signatory states; rather, it is just a potential tool for creating hegemony in cyberspace against cybercrimes.[50] Many important nations have not yet signed the convention, India being one of such nations. The main concern of such nations is that the Convention might violate the sovereignty of the nations and also that the Convention's intellectual property related crime provisions are not compatible with their developing markets.[51]India has raised concern that since it has not been included in negotiations regarding this convention, its priorities are not reflected in this convention.[52]

POAhVJRI8KHeygC00Q6AEIKjAA#v=onepage&q=judy%20westby%20international%20guide%20to%20cyber%20security&f=false, last seen on 27/08/2016.

[49] C. Ernest, Cyber Crime: New Threat and Global Response Expert Group on Cyber Crime, Department on New Challenges and Threats (2011), available at https://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Presentations/Russia_1_Cybercrime_EGMJan2011.pdf, last seen on 24/08/2016.

[50] A. M. Weber, The Council of Europe's Convention on Cybercrime, Berkeley Technology Law Journal (2003), available at http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1416&context=btlj, last seen on 26/08/2016.

[51] A. Kovacs, India and the Budapest Convention: To sign or not? Considerations for Indian Stakeholders, Internet Democracy Project, available at https://internetdemocracy.in/reports/india-and-the-budapest-convention-to-sign-or-not-considerations-for-indian-stakeholders/, last seen on 26/08/2016.

[52] Ibid.

There are other platforms also like Europol which manages "Check the Web", where the police officials of the member countries share data on terrorist organizations and terrorists.[53] Germany has also established "Joint Internet Centre", which assimilates information on suspicious activities in cyberspace.[54] "Monitoring Assessment and Partners" (MAP) was launched in 2009 by Interpol to monitor activities on suspicious websites, uncover relevant information and disseminate it to the police forces of nations all over the globe.[55]

## GEARING UP FOR FUTURE: SUGGESTIONS

Internet being a far-reaching medium, gives the terrorists an opportunity to target remote areas while sitting at one place. These cyber attacks are not always contained to the virtual world, but have the ability to cause havoc in the real world also. In future, as the critical infrastructure and governance become more and more technology reliant, cyber terrorism might even surpass the threats of terrorism. Terrorists would be able to shut down the whole functioning of a country by targeting the technologies which are running that nation. Cyber terrorism, being a global menace, can be said to be an international crime.[56] Thus, it calls for an international response. Universal jurisdiction can be applied to the acts of cyber-terrorism through international community and states.[57] Treaty regimes and customary international law can help build a strong system of universal jurisdiction. Multilateral co-operation between nations is very important to combat this evil. Currently, Council of Europe Convention on Cybercrime is the only treaty against cybercrime at the global level.[58] But since this Convention has not been signed by many important nations, there is a need to either make some reformations to this or form a new treaty after a dialogue between the nations at international platform such as United Nations.

The most successful formula ever, "divide and rule", has been used by terror propagating agencies since time immemorial. One of the best ways to combat cyber-terrorism would be by harmonizing the cyber laws all over the globe through international treaties. This might seem like a herculean task, but initiation can be made by adopting measures like liberal sharing of data on terrorists and attacks, sharing new technologies,

[53] Supra46.

[54] Ibid.

[55] Countering the Use of Internet for Terrorist Purpose, Counter-Terrorism Implementation Task Force Working Group Compendium (2011), available at http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf, last seen on 23/08/ 2016.

[56] Supra47.

[57] S Wilske and T Schiller, International Jurisdiction in Cyberspace: Which States May Regulate the Internet, Federal Communications Law Journal (1997), available at http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1148&context=fclj, last seen on 19/08/2016.

[58] Supra14.

responding quickly to bilateral requests and references made by Interpol and other international intelligence agencies, conducting cross-country training exchange programs.[59]

On the domestic level, a national cyber security doctrine needs to be developed and the definition of cyber terrorism in Information Technology Act, 2000 must be stretched to cover cyber communication which aids the terrorists in achieving success in their terror inducing missions. Formulation of a National Security Policy by the Cabinet Council on Security which should be duly endorsed by the Prime Minister Office can help to make an enforceable legislation in this field.[60] Cyber Security Policy can be made a subset of this policy. In addition to this policy, a national cyber security doctrine and Cyber Security strategy by respective ministries can help establish a tier-based "policy-doctrine-strategy" regime which would ensure a better security of the whole nation when it comes to cyber-terrorism.[61]

Moreover, an apex body needs to be created to look over the cyber security mechanism of the country. It should have the power to look over for policy formulation, budget allocation and implementation of the cyber security measures all over the nation. Cert-in does not have any enforcement powers, so, it should be shifted under Ministry of Home Affairs from Ministry of Communication and Information Technology.[62] It would lead to a simple line of reporting and Cert-in will have the accountability over enforcement and vulnerability assessment.

The system administrators and the government need to remain highly alert for any warning they receive for cyber attacks at any point of time. Systematic and routine risk assessment of critical information infrastructures should be regularly conducted and given priority for proper risk management.[63] . A proper cyber warfare and encryption policy needs to be developed. E-governance services are needed to be given more cyber security. A cyber security agency can be created which acts as a bridge between government agencies and civil agencies to improve the country's resilience against serious electronic attacks, and enhance the security. Maintaining the systems should be given utmost importance by keeping operating system, software and anti-virus programs up to date; "locking down" the system; disabling all unnecessary services and enforcing strong password protected systems. Active defence measures should also be adopted such as finding the source of attacks and imposing serious risk and penalty, and counter attacks.[64] With every attack, its after-effects should be studied and proper measures should be taken to ensure such attacks do not pose any threat in future. Defective entities should be removed, a damage assessment should be done,

[59] Supra33.
[60] Supra 41.
[61] Supra41.
[62] Ibid.
[63] Christopher Beggs and Matthew Butler, Developing New Strategies to Combat Terrorism, Innovations Through Information Technology,, available at http://www.irma-international.org/viewtitle/32381/, last seen on 23/08/2016.
[64] S.E. Goodman, Cyberterrorism and Security Measures, Science and Technology to Counter Terrorism (2007), available at http://www.nap.edu/read/11848/chapter/6, last seen on 25/08/2016.

the undamaged residue should be rationed and reallocated, reconstitution of functions should be done as per their importance and pre-attack status should be reached without destroying evidences.[65]

Government organisations as well as other organisations should create and enforce user policies which cover legitimate usage, security issues and promote vigilance. The user policies should be known to all employees and strictly adhered to. The employees of such organisations should be provided with proper training regarding cyber security and a general awareness among the mass also needs to be generated. Since technology is an ever changing entity, the policies and strategies need to be analysed and updated at regular intervals. Communication between various organisations should also be smooth so that proper warnings can be given at the time when it really matters. A forewarning about their vulnerabilities can help them to establish strong preventive measures. The main weapon of cyber terrorists is their garb of anonymity, cyber cafes and other public service platforms which provide internet facility provide a platform to maintain this garb. Hence, it is necessary to follow security procedures like identity check of customers, maintaining proper records to keep a check on cyber terrorism.

One major hindrance in strengthening the cyber security in India is the negligence that is shown to it when it comes to funding. While the internet companies all over the world spend an average of 5% of its funds on cyber security, Indian internet companies spend less than 1% of their funds on security.[66] Adequate funding should be provided in the field of cyber security and private sector should also contribute in such funding. Moreover, India should try to make its laws and policies complementary to the international agencies and conventions, building up strong multilateral connections with the nations all over the world so that there is an international cooperation in dire circumstances. A comprehensive analysis should be done by the government of its concerns and all the stakeholder groups need to participate in this analysis and then form foreign policy objectives regarding this matter.

Media, being the disseminator of information throughout the world, needs to engage the public in a conversation and make them aware regarding such threats.[67] Academicians and scholars can also help in this matter by providing their expertise on technical, psychological and ethical issues involved in this form of terrorism. Internet Literacy needs to be increased and evolved at individual level so that people can maintain cyber security at individual level. Moreover, there is a dire need for people to maintain good inter-personal relationship to ensure that members of family or friends do not become susceptible to the influence of terror propagating organizations such as ISIS. Young minds are most impressionable and hence parental control

[65] Ibid.

[66] Supra33.

[67] Kostas Mavropalias, Cybercrime & Cyberterrorism: Inducing anxiety & fear on individuals, Cyberpsychology, available at http://iconof.com/blog/cybercrime-cyberterrorism-inducing-anxiety-fear-on-individuals/, last seen on 24/08/2016.

and parental guidance at proper time can save them from falling prey to the acts of brainwashing by the terrorist organizations.

## CONCLUSION

In general parlance, cyber terrorism is better understood as instigating terror through the medium of cyberspace. In light of the incessant series of events that have alarmed the nations all over the world, one may fairly conclude that cyber terrorism, cyber warfare and cyber crimes, irrespective of the futile categorization, are a grave concern, constantly growing with the advancement of science and technology. As the cyber world reaches to a level of being ubiquitous and transgresses itself all over the world, it amasses the potential to become a lethal medium of propagation of terror. It is vital that the government of each and every nation as well as the international community pays heed to the threat of cyber-terrorism and takes all possible measures to curb this menace. Although, national and international agencies are working towards building a secure cyberspace, the dynamic nature of the cyber-world requires a constant scrutiny and change in measures so as to match the pace of technological development.