CYBER TERRORISM: THE DANGER IS REAL, AND THE COUNTRY MUST READY TO CURB

Dr. Deepak Kumar Srivastava* & Ankit Awasthi**

INTRODUCTION

There are two issues over which individuals are having common apprehensions as they recognize them as threat for nation viz. corruption and terrorism, but the threat which is more dangerous in 21st century specifically in Indian scenario is cyber terrorism. Cyber space is regarded as the meeting place for criminal groups.[1] Cyber space has recently emerged as the latest battleground in this digital age.[2] The convergence of the physical and virtual worlds has resulted in the creation of a "new threat" called cyber terrorism.[3] At this juncture it is pertinent to note that the threat of cyber terrorism with respect to India's infrastructure is real and immediate. Computers and servers, especially those belonging to the Governments, are the most aggressively targeted information systems in the world, with attacks increasing in severity, frequency, and sophistication each year.[4]

India is one of the most developing economies in the world which based on service sector specifically information technology but it is having threat (attack) at both internal and external level. These attacks can threaten our nation's economy, public utility works, power generation systems, communication systems, computer networks and cripple them for a longer duration, if not protected properly and immediately.[5] In this respect it would be apt to quote the observations of EC Council President and CEO Jay Bavisi as he said that, *"India's response to cyber terrorism is dis-jointed. To begin with, there is no central cyber command and there is a non-existent cyber-security training programme."*[6] Further he said that, *"India is not prepared to handle a sophisticated cyber-attack as it also faces a serious shortage of trained professionals. There is a lot of talk, but things need to be figured out. There is an understanding that data is important, but nothing substantial is being done,"*[7]

* Assistant Professor of Law, Hidayatullah National Law University, Naya Raipur, C.G.
** Faculty Member, Hidayatullah National Law University, Naya Raipur, C.G.

[1] *Tushabe and Baryamureeba, 2005,* World Academy of Science, Engineering and Technology, *66.*

[2] *Veerasamy,* 4th International Conference on Information Warfare and Security, *26-27 ,March,2009.*

[3] It should be noted that the physical world refers to the place where we live and function, whilst the virtual world refers to the place in which computer programmes function

[4] Addressing the Threat: Cyber terrorism Defense Initiative (CDI); Criminal Justice Institute University of Arkansas System; available at http://cyberterrorismcenter.org/Documents/CDI%20Cyber%20Classes%20(v.3).pdf

[5] R. Ramamurthy, Chairman, Cyber Security & Privacy Foundation available at http://issuu.com/mcci200/docs/mcci-july2k12

[6] India not prepared to handle cyber terrorism threat: EC Council, PTI Feb 19, 2014, 06.28PM IST, EC Council President and CEO Jay Bavisi, The Economic Times Feb 19, 2014, available at http://articles.economictimes.indiatimes.com/2014-02-19/news/47489884_1_cyber-ddos-participants

[7] id.

In this backdrop the aim of this article is to envisage an understanding of the nature and undesirable impact of Cyber Terrorism and making an exertion to study and analyze the steps taken by India to address this issue and anticipate what more can be done in this regard but before we do that it is highly required to conceptualize the concept with the help of definitions.

DEFINING CYBER TERRORISM

"Cyber Terrorism" is the combination of two terms viz. Cyber and Terrorism. According to American Heritage Science Dictionary the term Cyber or Cyberspace means *"the electronic medium in which online communication takes place."*[8] In other word it denotes a virtual world in which computer programs function and data moves from one source to another. Other part of the mentioned term is *"Terrorism"* which is a much used term both at national as well as international level, with many definitions but again universally accepted definition is not a single one because of its nature and scope. For the purposes of this understanding in the light of present paper, we will use the definitions observed by some departments of United States. These are as follows:

According to The United States Federal Bureau of Investigation terrorism means, *"The unlawful use of force or violence, committed by a group(s) of two or more individuals, against persons or property, to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."*[9]

According to The United States Department of Defense terrorism means, *"The unlawful use of or threatened use of force or violence against individuals or property, to coerce and intimidate governments or societies, often to achieve political, religious or ideological objectives."*[10] The United States Department of State defines it as, *"premeditated, politically motivated violence perpetrated against noncombatant targets by sub national groups or clandestine agents"*[11]

Again if we talk about the *"Cyber Terrorism"* it also doesn't have any common universally accepted definition. According to Sarah Gordon, *"The term cyber terrorism is becoming increasingly common in the popular culture, yet a solid definition of the word seems hard to come by. While the phrase is loosely defined, there is a large amount of subjectivity in what exactly constitutes cyber terrorism"*[12] The most widely cited paper on the issue of Cyber terrorism is Dorothy E. Denning's CYBERTERRORISM Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives,

[8] Published by Houghton Mifflin, available at http://dictionary.reference.com/browse/cyber-

[9] The United States Federal Bureau of Investigation (FBI-2002); available at https://www.fbi.gov/stats-services/publications/terrorism-2002-2005

[10] The United States Department of Defense (DOD-2002); for details refer Gus Martin, Understanding Terrorism, pg. no. 38, 4th edition, Sage Publications Ltd. (2013)

[11] Id. for details refer The United States Department of State (DOS-2002)

[12] Sarah Gordon and Richard Ford, Cyberterrorism? Available at https://www.symantec.com/avcenter/reference/cyberterrorism.pdf

in which at the outset he mentioned and researchers quote that, *"Cyber Terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as Cyber Terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of Cyber Terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not."*[13]

As per researchers understanding this is one of the most comprehensive definitions of cyber terrorism. But even this has a limitation as observed by Col. S.S. Raghav that, *"it states that for an attack to qualify as a cyber-attack it should lead to violence. This is more conventional. Terrorist may direct attack only to disrupt key services. If they create panic by attacking critical systems/infrastructure there is no need for it to lead to violence. In fact such attacks can be more dangerous."*[14]

Now after conceptualization it would be relevant to have some idea about the Cyber Terrorist's weapons, Methods and Techniques.

CYBER TERRORIST'S WEAPONS, METHODS AND TECHNIQUES

According to Col. S. S. Raghav as he mentioned in his article titled, *"Cyber Security in India's Counter Terrorism Strategy,"* that, "the most popular weapon in cyber terrorism is the use of computer viruses and worms. That is why in some cases of cyber terrorism is also called 'computer terrorism'."[15] Further he discussed the weapons or methods on the computer infrastructure which can be classified into following categories[16]:

- **Physical Attack:** In Physical Attack generally computer infrastructure is damaged by using conventional methods like bombs, fire etc.
- **Syntactic Attack:** In Syntactic Attack unlike Physical Attack computer infrastructure is damaged by modifying the logic of the system in order to introduce delay or make the system unpredictable. Generally Viruses, Trojans etc. are used in such attacks.
- **Semantic Attack:** In comparison to Physical and Syntactic attacks, Semantic Attack is more treacherous as it exploits the confidence of the user in the system. During the attack the information keyed in the system during entering and exiting the system is

[13] Dorothy E. Denning's CYBERTERRORISM Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, available at http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf

[14] Col. S.S. Raghav, CYBER SECURITY IN INDIA'S COUNTER TERRORISM STRATEGY, pg. no. 2, available at http://ids.nic.in/art_by_offids/Cyber%20security%20in%20india%20by%20Col%20SS%20Raghav.pdf

[15] id

[16] id

modified without the user's knowledge in order to induce errors which may cause disastrous effects.

After discussing the Methods of Attacks he mentioned that, *"Cyber terrorism is not only limited to paralyzing computer infrastructures but it has gone far beyond that. It is also the use of computers, Internet and information gateways to support the traditional forms of terrorism like suicide bombings. Internet and email can be used for organizing a terrorist attack also. Most common usage of Internet is by designing and uploading websites on which false propaganda can be pasted. This comes under the category of using technology for psychological warfare."*[17]

TECHNIQUES OF CYBER TERRORISM

There are various types of techniques used by Cyber terrorists to give a free rein to terrorism.[18] These are Hacking[19], Trojans[20], Computer Viruses[21], Computer Worms[22], Unauthorized Intrusions[23], E-Mail Related Crime[24], Domain Name Service (DNS) Attacks[25],

[17] id

[18] Id at pg. no. 3. Infra no. 21, 22, 23, 24, 26, 29 and 30 are also cited from the same source that is available at http://ids.nic.in/art_by_offids/Cyber%20security%20in%20india%20by%20Col%20SS%20Raghav.pdf

[19] The most popular method used by a terrorist, it is a generic term used for any kind of unauthorized access to a computer or a network of computers. Some ingredient technologies like packet sniffing, tempest attack, password cracking and buffer outflow facilitates hacking.

[20] Programmes which pretend to do one thing while actually they are meant for toeing something different, like the wooden Trojan Horse of the 12 Century BC

[21] It is a computer programme, which infects other computer, programmes by modifying them. They spread very fast

[22] The term 'worm' in relation to computers is a self contained programme or a set of programmes that is able to spread functional copies of itself or its segments to other computer systems usually via network connections

[23] It means viewing private accounts, messages, files or resources when one has not been given permission from the owner to do so. Available at http://www.businessdictionary.com/definition/unauthorizedaccess.html#ixzz3vbzXTUzL

[24] Usually worms and viruses have to attach themselves to a host programme to be injected. Certain emails are used as host by viruses and worms. E-mails are also used for spreading disinformation, threats and defamatory stuff

[25] According to Steve Saint-Claire, *"Computers connected to the Internet communicate with one another using numerical IP addresses. Domain name servers (DNS) are the .Yellow Pages. that computers consult in order to obtain the mapping between the name of a system (or website) and the numerical address of that system. If the DNS server supply an erroneous numerical address for the web site, the user's system would connect to the incorrect server. Making matters worse, this fake connection would likely be completed without arousing the user's doubt. The result would be that the user is offered a web page that he believes is on the desired web server but, in reality, is on the attacker's server. An attacker could distribute fake information with a triumphant attack on a select DNS server (or group of servers), bypassing the need to break into the actual web servers themselves. Moreover, a DNS attack would prevent access to the original web site, depriving the site of traffic."* As he mentioned in his article titled, "Overview and Analysis on Cyber Terrorism." Available at http://www.iiuedu.eu/press/journals/sds/SDS_2011/DET_Article2.pdf

Distributed Denial of Service (DDoS) Attacks[26] or Denial of Service in general[27], Cryptology[28] etc.

CYBER TERRORISM IN INDIA

India is one among the prime victim of cyber-crime across the world. The report of the Security and Defence Agenda (SDA), a leading defence and security think tank in Brussels and McAfee ranked India as the fifth country in the world severely harmed by cyber-crimes.[29] The rose of cyber-crimes from 2012 to 2013 is 2876 to 4356 cyber-crime cases were registered under the Information Technology Act, 2000 and 601 to 1337 cases were registered under the Indian Penal Code, 1860 reported by National crime record bureau evident the far reaching growth of cyber-crimes in India.[30] In this context the then Home Minister of India has stated cyber space as fifth domain after land, sea, air and space where much of country's critical infrastructure lies and challenged with terrorist threats.[31]

In this context it would be helpful to quote the observation of James Lewis, *"it is the use of computer network tools to shut down critical national infrastructures or to coerce or intimidate a government or civilian population'.*[32] As discussed earlier under Techniques of Cyber Terrorism such attacks in the forms of viruses and other means to disrupt the system, hacking and theft of data and denial of services by damaging networks etc., create harm especially in the government as well as essential service sectors. Several government and security establishment sites in the country were constantly targeted by such attacks. The IT Minister on November 30, 2011 in Lok Sabha stated that many government web sites has been defaced by various hacker groups in the year 2008, 2009, 2010 and January- October 2011.[33] This statement shows the position and helplessness of India in such matters.

It was observed by S. Sreejith in his article titled, *"Varying Faces of Cyber Terrorism in India,"* that, "The terrorist had also uses the cyber field for facilitating their activities as communication, banking, financial fraud etc. The investigation of David Hardly in US revealed that the hardly team used Mail service for communicating each other by saving

[26] id. as he observed DDoS Attacks means, "DDoS attacks utilize armies of .zombie machines taken over and controlled by a single master to overpower the resources of victims with floods of packets. These."

[27] These attacks are aimed at denying authorized persons access to a computer or computer network.

[28] Terrorists have started using encryption, high frequency encrypted voice/data links etc. It would be a Herculean task to decrypt the information terrorist is sending by using a 512 bit symmetric encryption

[29] Sanchitha Bhattacharya (2012), Cyber terrorism: the fifth domain, South Asian Intelligence Review, Vol. 10 (48), Retrieved from: http://www.satp.org/satporgtp/sair/Archives/sair10/10_48.html, Accessed on: 14/02/2015.

[30] National crime record bureau (2013), The Crime- 2013 statistics, New Delhi. Available at http://ncrb.nic.in/CD-CII2011/cii-2011/Chapter%2018.pdf, Accessed on: 1/03/2015.

[31] Supra no.31

[32] James Lewis (2010), "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," Center for Strategic and International Studies, Available at http://csis.org/files/media/csis/pubs/021101_ risks_of_cyberterror.pdf, Accessed on: 28/2/ 2015.

[33] Staff reporter (2012), 112 govt. Website hacked in three months, Economic times, Retrieved from: http://articles.economictimes.indiatimes.com/2012-03-15/news/31197171_1_ government-websites-internet-frauds-sachin-pilot, Accessed on: 23/02/2015. For more details see http://pib.nic.in/newsite/PrintRelease.aspx?relid=77958

messages in the draft and members visited the mail by using same passwords without sending each other. Terrorist in several attacks in India such as Ahmadabad (2008), Jaipur (2008), Delhi (2005) Varanasi (2010) and Delhi High court (2011) etc., have used the internet and mail services to further their attacks in Indian soil. Mumbai 26/11 operation reveals the extensive use of internet, mobile and satellite phones to communicate the directions from the planners and perpetrators in different spots."[34] Further he mentioned that, *"Terrorist groups also use the web bases to recruit, train and motivate the followers for the jihad. Al Qaida, Laksher e Taiba, Indian Mujahedeen etc., is having their own IT wings which carry terrorist activities in the cyber field. The extensive arrests of IT professionals in terrorism related activities in the country in the immediate past give more weight for the claim of cyber terrorism in the country. Ronald Nobel, former Head of United States Secret Service who is the secretary general of the Interpol says in an interview that the internet is giving terrorists new ways to plot mass murders."*[35]

TRENDS IN INDIAN CONTEXT

According to R K Ragavan, *"A number of cases of hacking of Indian internet sites have been traced to Pakistan but it would be difficult to nail them."*[36] Reason of this problem was mentioned by the President of India's National Association of Software and Service Companies (NASSCOM), Dewang Mehta as, *"Indian companies on an average spent only 0.8 percent of their technology budgets on security, against a global average of 5.5 percent."*[37] Recently some computer experts managed to break into the high security computer network of Bhabha Atomic Research Center but were luckily detected.[38] *"GForce,"* a group of anonymous hackers, whose members write slogans critical of India and its claim over Kashmir, have owned up to several instances of hacking of Indian sites run by the Indian government, private companies or scientific organizations.[39]

As mentioned by Lidia Mariam Benoji in her article titled, '*Cyber Terrorism- Quick Glance'* that, *"as tensions between the neighboring regions of India and Pakistan over Kashmir grew over time, Pro- Pakistan cyber-terrorists and recruited hackers began to target India's Internet Community. Just prior to and after the September 11th attacks, it is believed that the sympathizers of Pakistan (which also included members of the Al Qaeda Organization) began their spread of propaganda and attacks against Indian Internet based communities. Groups such as G- Force and Doctor Nuker have defaced or disrupted service to several major entities in India such as the Zee TV Network, The India Institute of Science and the Bhabha*

[34] S. Sreejith, *Varying Faces of Cyber Terrorism in India, Volume : 1 | Issue : 5 | Nov 2012 ISSN No 2277 – 8160; available at* http://worldwidejournals.com/gra/file.php?val=November_2012_1353498262_2f441_40.pdf

[35] id

[36] INDIAN WEBSITES ARE NEW TARGET OF HACKERS; available at http://www.cyberlawsindia.net/cases2.html

[37] id

[38] id

[39] id

Atomic Research Centre which all have political ties.”[40] These instances are enough to say observed by the then CBI Director, R K Ragavan that, “Cyber Crime is the crime of the future.”

LEGAL RESPONSE TO CYBER TERRORISM IN INDIA

According to Rohit K. Gupta, *“There was no statute in India for governing Cyber Laws involving privacy issues, jurisdiction issues; intellectual property rights issues and a number of other legal questions. With the tendency of misusing of technology, there arisen a need of strict statutory laws to regulate the criminal activities in the cyber world and to protect the true sense of technology the Information Technology Act, 2000 (IT Act, 2000) was enacted by Parliament of India to protect the field of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cyber-crimes. The above Act was further amended in 2008 in the form of IT Amendment Act, 2008.”*[41] So we can say that the cyber law of India received a fatal blow in the form of Information Technology Act 2008 (IT Act, 2008).[42]

It is pertinent to mention here that Information Technology Act, 2000 was planned to regulate the use of internet only. But it is because of 2008 amendment government got power to block websites if they come within the purview of section 69A[43], 69B[44] and for such activities 66F[45] shall be applicable. In addition to the amendment Government of India[46] also notified Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, the information Technology (Electronic Service Delivery) Rules, 2011, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Information Technology (Procedure and safeguards for blocking for access of information by public) Rules, 2009, The Digital Signature (End entity) Rules, 2015, The Electronic Signature or Electronic Authentication Technique and Procedure (Amendment) Rules, 2015, The Information Technology (Security Procedure) Rules, 2004, The Information Technology (Other Powers of Civil Court vested in cyber appellate tribunal) Rules, 2003, the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003 and Information Technology (Certifying Authorities) Rules, 2000 etc.

[40] Lidia Mariam Benoji, *Cyber Terrorism- Quick Glance; available at http://www.legalservicesindia.com/article/article/cyber-terrorism-quick-glance-1263-1.html*

[41] Rohit K. Gupta, India: An Overview Of Cyber Laws vs. Cyber Crimes: In Indian Perspective; available at http://www.mondaq.com/india/x/257328/Data+Protection+Privacy/An+Overview+Of+Cyber+Laws+vs+Cyber+Crimes+In+Indian+Perspective

[42] ICT TRENDS IN INDIA 2009 BY PERRY4LAW AND PTLB; available at http://hrpic.blogspot.in/2009/12/ict-trends-in-india-2009-by-perry4law.html

[43] Power to issue directions for blocking for public access of any information through any computer resource.

[44] Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security

[45] Punishment for cyber terrorism

[46] In exercise of the powers conferred by clause (ob) of subsection (2) of section 87 read with section 43A of the Information Technology Act, 2000 (21 of 2000), the Central Government has power to make rules. Available at http://deity.gov.in/content/notifications

Apart from abovementioned legislative steps 2nd July, 2013 Department of Electronics and Information Technology (Deity) under the Ministry of Communication and Information Technology notified first of its kind, National Cyber Security Policy – 2013 (NCSP - 2013).[47] According to Sanjiv Tomar, *"The Cyber Security Policy aims at protection of information infrastructure in cyberspace, reduce vulnerabilities, build capabilities to prevent and respond to cyber threats and minimize damage from cyber incidents through a combination of institutional structures, people, process, technology and cooperation."*[48]

CONCLUSION

In concluding remark researchers would like to cite the observation of National Research Council that, "*Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb,"*[49] as observed by Frank Cilluffo that, *"While bin Laden may have his finger on the trigger, his grandchildren may have their fingers on the computer mouse."*[50] In such circumstances government has to develop workable strategy and invest more and more on research activities to find out the solution for such attacks, if they happen. Apart from this mere enactment of a plethora of statutes is not a solution per-se but we have to give emphasis on proper implementation. Judicial and quasi-judicial bodies have to take active steps in interpretation and enforcement of existing laws. At last researcher would like to say that apart from state and non-state actors it's the duty and responsibility of common individuals to think in this respect and always ready to defend and defeat the so called threat.

[47] National Cyber Security Policy – 2013; available at http://deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf

[48] Sanjiv Tomar, National Cyber Security Policy 2013: An Assessment; available at http://www.idsa.in/idsacomments/NationalCyberSecurityPolicy2013_stomar_260813

[49] GABRIEL WEIMANN, Cyberterrorism: The Sum of All Fears? *Studies in Conflict & Terrorism*, 28:129–149, 2005; Routledge Taylor & Francis Inc. available at https://www.princeton.edu/~ppns/Docs/State%20Security/Cyberterrorism%20-%20sum%20of%20all%20fears.pdf

[50] id at pg. no. 146