International Journal of Law and Legal Jurisprudence Studies : ISSN:2348-8212

Authors Name: Anuttama Ghose, Lahama Mazumdar

Institution: KIIT School of Law, KIIT University. Bhubaneshwar.

Year of Study: 3rd Year, 5th Semester.

E-Mail ID: (1) anuttama1993@gmail.com (2) lahamamazumdar@gmail.com

Cyber-terrorism: Weaponisation in the virtual world.

Abstract: In this study an endeavor will be made to examine about the concept of Cyber-terrorism. In the present world digital-terrorism is the stressing pattern in parallel to globalization. The new wave of globalization sponsored by present day innovations is confronting colossal feedback. Pessimists of globalization argue that globalization supported by tech savvy terrorists has enabled the terror organizations to exploit communication systems, information and funds etc. to further their activities.

Notable incidents are the Kosovo attack (1999), Internet Black Target on Sri Lanka(1997), Trade Center assault of 9/11 and so forth. India's first occurrence of cyber-terrorism was in 2008 serial blast in Varanasi it furthermore 26/11 in Mumbai.

This paper likewise interlinks cyber-terrorismwith domestic laws of INDIA, USA, UK. Indian Legislators however have given particular systematized statutes on digital terrorism (Sec 66, 66f of IT Act 2008) yet certain loopholes are available. Despite the fact that Section 66 talks about discipline on sending "grossly offensive messages" yet nowhere in the statute is a particular definition given for the term. We might additionally discuss about international conventions and regional conventions and the need of global system and national enactment fit for researching, arraigning and rebuffing for the wrongdoing.

Keywords – Cyber-terrorism, Globalization, Loopholes.

INTRODUCTION:

A long time after the September 11, 2001 assaults each youngster in the world knows about cyber terrorism. Consistently after this episode this date is grieved by every last national of America. Presently after 13 years, people know that to cause pulverization the terrorist weapon of decision may not so much be a 1,87,000 pound 767 plane stacked with fuel targeting New York city's 110 story iconic structures that fell taking , 2753 pure lives with it.[1] Today a computerized terrorist can result in a devastation secretly being furnished with a workstation and mouse sitting in his home. The word cyber terrorism as we all know was first time coined by the computer whiz Barry C Collin.

Terrorist have used computer space as a medium for communication as it is decentralised, difficult to control or restrict the information and it is accessible by all. Cyber weapon has been used as an indirect and direct tool to execute an attack. The different types of network that can be subjected to cyber terrorist attacks are military and civilian defence networks, other governmental networks (police, fire) , privately or publically owned networks used to control public utilities, public networks used by customers for business of communication education.[2]

In this paper we shall define cyber terrorism or digital terrorism as the following:

"Digital terrorism" implies unlawful danger or focused on assault to mischief machines, to take down confidential data and information on defense system of one or more nation which is done against government or public or creating fear in the minds of people for illicit political, social or religious goals.

Despite all the gloomy predictions of a cyber terrorism doomsday, no single instance of cyber terrorism has been recorded in the Indian journal of cases as of now. People might think that the prophecies of cyber terrorism has faced exaggeration, but it's not so.

INSTANCES OF CYBER CRIME:

Cyber terrorism has a short history. Only in the past decade have cyber security threat have surfaced worldwide. Obvious targets of cyber terrorism consist of infrastructures like transportation, electric power breach, telecommunication, financial institutions. Gulf war was the first time when Iraqi hackers have disrupted troop deployments embarking the start of cyber

[1] Scott Schober,*Cyber terrorism- The weapon of choice a decade after 9/11,* HOMELAND SECURITY NEWS WIRE, http://www.homelandsecuritynewswire.com/dr20111102-cyberterrorism-the-weapon-of-choice-a-decade-after-9-11(last accessed Aug 18th, 2014)

[2] Aviv Cohen, *CYBERTERRORISM : ARE WE LEGALLY READY?* , http://heinonline.org/HOL/Page?handle=hein.journals/jibla9&div=3&collection=journals&set_as_cursor=3&men_tab=srchresults&terms=cyberterrorism&type=matchall (last accessed Aug 18th ,2014)

terrorism. 1994 and 1997 were the other two years when instances of cyber terrorism were recorded. It could be seen that most of the youths were more influenced with the concept of tech savvy digital terrorism. The instance of a 16 years old boy who took down 100 US defence system in the year 1994. This fact substantiates the early statement used. 1997 saw 35 computer specialists had used hacking tools to shut down large segments of US power grid. They also silenced the command and control system of the pacific command in Honolulu. In 1998 another incident happened where Spanish protested bombarded the institute for global communication. The porters spammed IDC stiffs and members account and clogged their web pages, then IGC had relented and pulled the site because of male bombings. In 1998 the US military system were attacked electronically by 2 hackers based in California under the guidance of hacker in Israel. This was popularly known as solar sunrise attack where there was unauthorised accessing of computers available from the website of a university and collected user passwords by installing sniffer programs. The same year recorded the instance of another well known cyber attack by the internet black tiger group where they had attacked the email servers of Sri lanka's diplomatic account. [3]

The next year recorded the Kosovo conflict with NATO computers, blasted with email bombs and hit with denial of service attacks by hactivist protesting the NATO bombing. Highly qualitised viruses labelled emails were received by public organisation, academic institute and businesses.

11th September 2001 was one year when the whole world faced the major consequences of cyber terrorism. Not only was the cyber space but it devastated the physical space by taking away thousands of lives with it.

In April 2009 Chinese cyber spice hacked into the govt system using ghosnet in 103 countries which included the computer network that was used by Indian embassies abroad and the system of dalai lama. [4]

The Varanasi attack is also worth mention. The most recent incident of cyber terrorism in india is 26/11 in Mumbai.

APPEAL OF CYBERTERRORISM FOR CYBERTERRORISTS

Cyber terrorism is anonymous in nature. It's difficult to differentiate between common internet surfers and terrorists as they like others use nick names or log on to a website as a guest user making it hard for the security officials to identify them.[5] Moreover with the growing trend of cyber café to trace a person using a particular IP address is getting tough. Now cyber cafes are using protection measures for every users to access net as they ask for identity proof thereby following necessary measures, but this measure is not followed everywhere and they miss out on this scheme of protection which makes it easy for a offender to carry out his activities without the fear of getting caught. As we all know that there is no physical barrier and no check point in case of cyber world which it makes it easier to evade. Moreover the variety of targets in the cyber

[3]Rohas Nagpal, *Cyber terrorism in the context of globalization*, World Congress and Information law http://www.asianlaws.org/aboutus/spain.pdf (Aug 18, 2014)
[4] KARNIKA SETH , COMPUTER INTERNET AND NEW TECHNOLOGY LAWS 355(1st Edition 2012)
[5]Gabriel Weimann, *Cyberterrorism: The Sum of All Fears,* ROUTLEDGE TAYLOR AND FRANCIS GROUP, http://www.princeton.edu/~ppns/Docs/State%20Security/Cyberterrorism%20-%20sum%20of%20all%20fears.pdf(Aug 18, 2014)

world is enormous and cyber terrorism can be conducted remotely and it requires less training and lesser risk of morality which makes it more appealing.
Another distinctive feature of cyber terrorism is its relatively low cost. A terrorist attack in the physical space requires a lot of money including recruiting an executer, explosives or weapons, all the travelling expenses making sure that he can dodge all the security personals and checks on different locations. Whereas to threaten the world with cyber terrorism a person only has to have a computer and a certain hacking skill better than his opponent .[6]

EVIDENCES FOR CYBER TERRORISM:

Some scholars and military experts believe that "cyber terrorism" does not exist and is an exaggerated threat. This is probably due to a lack of empirical evidence. There is maybe some other (erroneous) suppositions which downplay the danger of cyber terrorism. Those assumptions are that terrorists will only use physical violence and they are ill equipped to use technology. But various research and findings have shown that cyber world can be used as a tool/tactic to enhance and create new forms of attacks that continue to carry out the same message.

The US News & World Report has been digging into hundreds of pages of heavily redacted court documents and finds evidence that al-Qaeda has launched successful cyber attacks, including one against government computers in Israel. According to then papers, this is the first public acknowledgement of a terrorist group launching offensive cyber operations. A standout amongst the most early reported of the so called 'targeted orientated' cyber-terrorist attack was in 1997 when groups aligned with the Liberation Tigers of Tamil Eelam claimed responsibility for suicide email bombings against Sri Lankan embassies over a two week period.

Another more recent example is the Estonia conflict. In May 2007, Estonia was under attack for just about 3 weeks from programmers utilizing complex modes of engineering to mutilate and challenged person legislative and fiscal divisions. Taking after these occurrences the Stuxnet infection contaminated an Iranian force station and picked up control of the framework leaving the Iranian government's atomic program in turmoil. This was a complex and sophisticated attack on the Iranian industrial control systems in the Middle East. This is a clear demonstration of what a computer attack can look like. Additionally, the taking down of the Internet in different Arab nations in 2011 by different governments demonstrates the issues of foreswearing of administrations assaults.

From the various evidences which are noticed across the globe it can be clearly seen that cyber terrorism has become 'the new language of war'.

DEFENCES AGAINST CYBER TERRORISM

DOMESTIC LAWS

[6]Aviv Cohen, *Cyberterrorism: Are We Legally Ready?* , HEINONLINE, http://heinonline.org/HOL/Page?handle=hein.journals/jibla9&div=3&collection=journals&set_as_cursor=3&men_tab=srchresults&terms=cyberterrorism&type=matchall (last updated Aug 15th ,2014)

INDIA

Cyber terrorism in India is no more a new concept. Though attacks are quite common in Indian cyber space their detection is quite unnoticeable. There is an emerging need to amend cyber provisions in India. The IT Act 2008 has only one section -66F which provides punishment up to life sentence for cyber terrorism. Out of the few provisions Section 66F, Section 66F(1)(B) is worth mentioning. As we see threatening the security, integrity and to strike terror in people along with causing denial of access to any person to any computer without permission which can likely cause death or injury to the person, property of critical information infrastructure is included in the definition of this offence. So this clearly proves the merger of metaspace and cyber space in the definition of cyber terrorism. [7]

The scope and applicability of IT Act has increased with the amendment of 2008. The word communication devices has been inserted and it has a inclusive definition. Digital signature was replaced with electronic signature which covered a large ambit including biometrics etc. Moreover all the acts under section 66 are cognizable and non bailable offences and intension or mens rea is a major ingredient to bring any act under this section.[8] The Indian penal code and the Indian evidence act also have substantive statutes regarding the same. There are sections dealing with false entry and record thereby bringing electronic records within the ambit of Indian penal code .[9] As we all know now the electronic records are treated at par with the physical documents. [10]

Loopholes till now: ITA and ITAA have created a major change in the law, but still certain loopholes are yet to be dealt with. Territorial jurisdiction is a major issue which is not addressed sufficiently. Cyber Crime is mainly based on geography and is boundary less. So it needs to be look into. Moreover preservation of evidence is also a big issue as deleting stuff from a computer system is easy and leaves behind no trace. [11]For instance if the evidence lie in any intermediary computer or in the opponents computer, just a click can give rise to deletion of evidence. On looking through the definition clauses we can see a lot of important terms are not defined satisfactorily. For example Section 66A of IT Act is not defined properly making it easy for the offenders to slip in from their charges. Several other laws are there which have governed terrorism, e.g. The Unlawful activities prevention Act 1967, Terrorist and disruptive activities prevention Act 1987, Prevention of terrorism Act have already been there in India and extending their significance to the cyber world is only on the whims and fancies of the legislators of our countries which if done can solve a lot of problems.

CONSTITUTIONAL INTERPRETATION:

[7] KARNIKA SETH , COMPUTER INTERNET AND NEW TECHNOLOGY LAWS 356(1st Edition 2012)
[8] UNIVERSAL'S Information Technology Act, 2000 along with Rules & Regulations , Universal Law Publishing Co. Pvt. Ltd.(2000)
[9] UNIVERSAL'S Criminal Manual, Indian Penal Code(45 of 1860) As Amended By The Criminal Law Amendment Act , 2013, PG NO.- 467, 471, Universal Law Publishing Co. Pvt. Ltd.(2013)
[10]Rohit K. Gupta, India: An Overview Of Cyber Laws vs. Cyber Crimes: In Indian Perspective, MONDAQ, http://www.mondaq.com/india/x/257328/Data+Protection+Privacy/An+Overview+Of+Cyber+Laws+vs+Cyber+Crimes+In+Indian+Perspective(Aug 18, 2014)
[11] id

The constitution of any country says that its governance is controlled by the three branches or organs of the country by which we mean the legislative , the executive and the judiciary. So for controlling any sort of activity that has its branches within the country these three bodies have the upper hand. As we all know constitution is the main document which provides all the power to the people of country or its representatives, its interpretation is the most necessary so here we discuss how the three organs can work for combating cyber terrorism in a country.

The danger of cyber terrorism could be viably controlled, even if not totally disposed of, if the three sovereign organs of the Constitution work on the whole and in concordance with one another regarding dealing with this issue. Further, a vigilant citizenry can supplement the dedication of end of digital terrorism.

Legislative Commitment:

The governing body can give its support to the favorable goal of end of digital terrorism by ordering proper statutes managing cyber terrorism. It must be noted that to give effect to the provisions of Information Technology Act, 2000 appropriate amendments have been made in the I.P.C, 1860, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934. On the same lines another section managing "Cyber terrorism" could be added to the effectively existing criminal statues to make them good with cutting edge manifestations of terrorism. Additionally, another section managing digital terrorism could be consolidated in the Information Technology Act, 2000 by method for its correction to bring harmonization among different laws. The exclusion of POTA and its likely to replace the previous law with a new ordinance which shall be more effective and useful to fight against cyber terrorism.

Executive concern:

The central and state government can make new set of rules and regulations regarding the execution of various new laws or contribute towards effective implementation of the IT Act to deal with the problem of cyber terrorism as per the changing needs of the society. *For instance, the [12]Karnataka government made new set of rules and strict implementation of the rules regarding the running of a [13]"cyber café" in order to ensure security and restricting unlawful or terrorist activities through disclosure of proper photo identity, record of time of use and other details of users. It also says about the Cyber Police authorities may on complaint inspect Cyber Cafes at all reasonable time to ensure compliance of these rules.* The government can also block certain website which they want in order to curb cyber terrorism. There is no unequivocal procurement in the IT Act, 2000 for obstructing of sites. In fact, blocking is considered to be censorship hence it can be challenged if it restricts the freedom of speech and expression. But websites promoting hate, contempt, slander or defamation of others, promoting gambling, promoting racism, violence and terrorism can be blocked under the reasonable restriction so that one cannot claim the breach Fundamental Right of free speech and expression. Otherwise if the blocking occurs due to unreasonable grounds or irrelevant materials, then it would be vulnerable to the attack of unconstitutionality, being in violation of Articles 14, 19 and 21 of the Constitution of India.

[12] Information Technology (Karnataka) Rules 2004

[13] Rule 4, 5 and 6 of the Information Technology (Karnataka) Rules 2004

Judicial response:

The judiciary can assume its part by receiving a stringent methodology towards the threat of cyber terrorism. But problems may arise in order to deal with this issue due to lack of specific jurisdiction. The nonattendance of geological limits may offer ascent to a circumstance where the demonstration lawful in one nation where it is carried out may disregard the laws of an alternate nation. This methodology further made confused because of the nonappearance of an uniform and orchestrated law overseeing the jurisdictional parts of debate emerging by the utilization of Internet. But there are laws by virtue of which the judiciary can still to some extend try to cease the terrorist activities through computers. Like, it must be noted that by uprightness of section1 (2) read with section 75 of the Information Technology Act, 2000 the courts in India have "long arm jurisdiction" to manage cyber terrorism.

USA

In U.S cyber command (USCYBERCOM) was established to address national defence and security in cyber space. Besides the Homeland Security Act of 2002 (HSA), The USA PATRIOT ACT of 2001 , was enacted after the terrorist attack of 11th September 2001 and substantial changes were made therein in 2005. by adding support mechanisms to law enforcements to combat terrorism , including strengthening law enforcement's surveillance power. [14] Section 814 of the Patriot Act speaks about detterance and prevention of cyber terrorism. It mainly talks about the intention of any person to unauthorisely access a protected computer and cause loss to one or more person causing physical injury or cause damage to national defence and justice.

UK(UNITED KINGDOM)

As per *The Terrorism Act, 2000*, the term "terrorism" includes the use or threat of action that is

i. designed seriously to interfere with or seriously to disrupt an electronic system
ii. designed to influence the government or to intimidate the public or a section of the public, and
iii. made for the purpose of advancing a political, religious or ideological cause.[15]

INTERNATIONAL EFFORTS IN COMBATING CYBER TERORISM

When the term international effort in combating cyber terrorism come s to our mind or we can first think of is United Nations and its policies to generate cooperation. The UN has to act as a catalyst and must facilitate the states to have an agreement now. Several agencies under UN, like International Atomic Energy agency is working for a legal framework on cyber security events. There are still countries who are acting as antagonists in opting for a cyber terrorism free space.

[14] KARNIKA SETH , COMPUTER INTERNET AND NEW TECHNOLOGY LAWS 356(1st Edition 2012)
[15] Rohas Nagpal, *Cyber Terrorism In The Context Of Globalisation* , II World Congress on Informatics and Law Madrid, http://www.asianlaws.org/aboutus/spain.pdf (Aug 18, 2014)

Some of these countries are United States, South Korea, France, Germany, China, Taiwan, Canada, Italy, Great Britain[16]- this is what the Symantec Corporation suggest.

We already know that cyber terrorist have used computer either as a target or as a weapon. Conventions like Montreal and Hague convention has gone talk about disrupted activities that occur on account of using computer as am medium of weapon but they have not specifically pointed out so. As we see Montreal Convention, deals with aviation and areal navigation acts of terrorism but no where is a computer usage being motioned. Already existing conventions like the Bombing Convention, the Convention for the suppression of terrorist bombings are not that specific in nature but its applicability can be extended. August 2000, was the year when experts from Stanford University had published "A proposal for an International Convention on Cyber crime and terrorism", this was named the Stanford Draft. I dealt specifically with the correspondence between terrorism and Computer Communication based infrastructure. This was the Sectoral Convention.

Now that we already have a glimse of various international efforts. We further try to categorize the efforts of International Organisations, Multinational Organisations and regional organisations.

Efforts of GLOBAL ORGANISATIONS:

United Nations: United Nation is the lead association whose determination is to make the part states push the multi-parallel attention of existing and potential dangers in the field of data security, and also conceivable measures to farthest point the dangers. These resolutions have the intention to enhance the digital security mindfulness at both the universal and the national levels. After the awfulness of 11th September the Security Council resolution 1373 makes headway to battle against terrorism. The point of this determination is to counter terrorism exertion.[17] This resolution provides an internationally recognized definition of terror for the first time which seems to provide an inclusive ban on all forms of violence that international target civilian, regardless of the motive, as well as calls on countries to prosecute terrorists.

Interpol:

Interpol has always tried on curbing international crime even when there is no diplomatic relation between countries. They have declared public safety and terrorism as priority crime area. It works on the gap between the legal framework and criminal phenomena. "Fusion task force"

[16] Mark Higgins,*Attack Trends For Q3 and Q4 2002*, SYMANTEC INTERNET SECURITY AND THREAT REPORTS, http://eval.symantec.com/mktginfo/enterprise/white_papers/b whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf(Aug. 18, 2014)

[17]Mitko BOGDANOSKI & Drage PETRESKI, *Cyber Terrorism – Global Security Threat*, SECURITY AND PEACE JOURNAL , http://eprints.ugd.edu.mk/6849/1/CYBER%20TERRORISM%E2%80%93%20GLOBAL%20SECURITY%20THREAT%20-%20Mitko%20Bogdanoski.pdf (Aug. 18, 2014)

is a creation of INTERPOL which seems to be an alarm for international terrorist attacks , its objectives are to distinguish terrorist branches , their participation, gather and offer data sagacity , give expository help , upgrade the limit of past nations to areas of danger of terrorism and sorted out wrongdoing. [18]

MULTINATIONAL ORGANISATIONS

Commonwealth Nations

They have created Model law on computer related crimes which has had a great impact on domestic legislations. It has specified criminal liability for offences like interfering with data and computer systems and using illegal devices. It also covers the problem of territorial jurisdiction when a person sitting in one country plans on an attack on a different country. A principle of dual criminality is thereby defined at this stage by the Commonwealth Nations.

G8 group

It is an informal forum with an non binding obligation with just 8 member to it who have discussed issues of importance, including Crime and terrorism and information highway.

OECD (Organisation for Economic Cooperation and Development)

This is a forum where government of 30 countries join together to address the economic, social and environmental challenges of globalisation. In the year 2002 it adopted certain guidelines for the security of information system and network . The aim of this guideline is to develop a culture on policies and measures to have a take upon threats such as cyber terrorism.

REGIONAL ORGANISATION :

EUROPEAN UNION AND COUNCIL OF EUROPE**:**

After the devastating damage to Madrid through cyber weapon the European union pledge to put forward effective legislation to deal with every aspect of cyber terrorism. On December 2004 , all the member state of the council assembled to deal with criminal activities and rectify previous conventions in order to regulate more strict laws on cyber terrorism. Various laws regarding data trafficking through servers cross border exchange of digital information , curbing terrorist activities etc were discussed and revised here.[19]

Other legal instruments passed by European council are:

1. The cyber crime convention : This convention was signed in the year 2004 on cyber crime against hacking , infringement of copyrights , child pornography but not about cyber terrorism in much details. Article 2 to Article 6 touches only the outline of the subject cyber terrorism .[20]

[18]Nazura Abdul Manap & Pardis Moslemzadeh Tehrani, *Cyber terrorism: Issues in its Interpretation & Enforcement*, INTERNATIONAL JOURNAL OF INFORMATICS AND ELECTRONIC ENGINEERING , http://www.ijiee.org/papers/126-I149.pdf (Aug 18, 2014)
[19] id

2. Council of Europe: Convention on prevention of terrorism , 2005 : This convention was marked keeping in mind the end goals to manage the different overall outcomes confronted by individuals as an after effect of terrorism [21]. This meeting aimed towards combating terrorism through a cooperative actions of the society by modifying and strict implementation of both national and international policies against terrorism along with providing compensation to the victim of terrorism and gift them a terror free life.

3.Committee of Experts on Terrorism(CODEXTER) : Harmful effect of Terrorism also damage social security and human rights so CODEXTER was founded in the year 2006 in order to discuss detail information on the matters of evaluation on international instruments , spreading worldwide awareness on such crimes and variation in the use of IT System as a weapon and mode of communication [22]

ASIA PACIFIC ECONOMIC CORPORATION (APEC)

This forum was formed in 1989 in order to overcome economic hurdles and achieving growth and development along the 21 Asia pacific member countries. Different work and exertion of this forum got to be more dynamic and productive after the 9/11 attack.

NORTH ATLANTIC TREATY ORGANISATION(NATO)

The fundamental guideline of NATO (1949) was aggregate resistance against crimes , composed according to the centre principle plans of UN charter, yet cyber crime and cyber terrorism issues were not in presence amid its foundation. Anyhow in the present year NATO has changed their political and specialized necessities and enhanced their ranges on digital defence by curbing terrorist activities through cyber weapon .

INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER TERRORISM (IMPACT)

This organisation is the first comprehensive global private public partnership between nation industrialists and other experts to eradicate cyber terrorism . This organisation was supported by united nation (UN) , international telecommunication union (ITU) and international criminal police organisation(Interpol). It looks into the matter of cyber terrorism upon financial system , politics , areal control etc. It tries to merge domestic and International aspects together to fight against the menace of cyber terrorism.

CRITICAL ANALYSIS OF LEGAL SCENARIO:

In this study we have already gone through the domestic legislations of India and also laws at certain national and international level. In a report of Economic Times, al leading newspaper of India it was notified that a CBI judge Talwant Singh, New Delhi had stated that "Till date, we do not have a single treaty with any other country to extradite a cyber criminal to be bought in

[21] Murat Dogrul & Adil Aslan & Eyyup Celik , *Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism* , Turkish Air War College , http://www.ccdcoe.org/publications/2011proceedings/DevelopingAnInternationalCooperation...-M.%20Dogrul-Aslan-Celik.pdf (last updated Aug 18, 2014)

[22] id

India".[23] Facts have already made it clear that the need of a treaty is indeed there. After 26/11 terror attacks of Mumbai, Indian Legislators had realised the importance of framing a statute but all they did was of little use. In the year 2013, the findings of National Crimes Record Bureau indicated the rise of cyber crime incidents in India as reported by The Times of India. [24]Just after that another leading newspaper, NDTV Gadgets reported about Chinese hackers breaching the computers of India's top military organisations, Defence Research in Development Organisation (DRDO) which seems to be the biggest security breaches till date. [25]

Now the question rises why isn't India or any other country signing a convention on cyber terrorism. According to our point of view, the reason might lie in the status of each country. The developing and the developed countries are mainly differentiated by their economic status and as we all know that the economy of most of the country can be stolen with just a click of a finger. So why will a developing country sign a pact with a developed country. When the facts are compared it can be easily inferred from the facts that never have two developed countries come into conflict due to cyber terrorism. With the growth of technology our dependence on technology is also increasing. Referring the metro projects running throughout India which is all running via computer, if this comes under a cyber attack nobody is there to shut it down.[26] India's laziness in this field can lead to loss of thousands of life. But even after so many incidents and sufferings of common man no such international binding laws has been there. As a crimes committed in cyber space do not have a territorial boundary, a binding international law is a must and time has come that steps need to be taken in this field. Though a small problem, it is rising at a very contagious rate. Cyber terrorism as a crime has already invoked universal consensus and should be either comprehensively included in the UN Convention against transnational organised crime or a new convention should be paved away by now to provide an effective international legal framework to combat terrorism.[27]

[23] *Cyber crimes : India yet to sign treaty with other countries* , The Economic Times, http://articles.economictimes.indiatimes.com/2012-10-05/news/34279945_1_cyber-terrorism-cyber-crimes-cyber-law (Last updated Aug 18, 2014)
[24] Cyber crimes rise sharply, The Times Of India, http://timesofindia.indiatimes.com/city/bhubaneswar/Cyber-crimes-rise-sharply/articleshow/37952914.cms (Last updated Aug 18, 2014)
[25] *India must wake up to cyber terrorism* , NDTV Gadgets, http://gadgets.ndtv.com/internet/news/india-must-wake-up-to-cyber-terrorism-349274 (Last updated Aug 18, 2014)
[26] *Cyber crimes : India yet to sign treaty with other countries* , The Economic Times, http://articles.economictimes.indiatimes.com/2012-10-05/news/34279945_1_cyber-terrorism-cyber-crimes-cyber-law (Last updated Aug 18, 2014)
[27] KARNIKA SETH , COMPUTER INTERNET AND NEW TECHNOLOGY LAWS 357(1st Edition 2012)