CYBER TERRORISM: A THREAT TO FUTURE

***MD. BAHARUL ISLAM**

INTRODICTION

"For a warrior, nothing is higher than a war against evil The warrior confronted with such a war should be pleased. Arjuna, for it comes as an open gate to heaven. But if You do not participate in this battle against evil, you will incur sin, violating your Dharma and your honour."

BhagavadGita 2.31.

The expression cyber terrorism includes an intentional negative and harmful use of the information technology for producing destructive and harmful effects to the property, whether tangible or intangible, of others. For instance, hacking of a computer system and then deleting the useful and valuable business information of the rival competitor is a part and parcel of cyber terrorism. Cyber terrorism is a tempting occasion for terrorist group as they would require less people, money and fewer resources. Moreover, it enables the terrorist to remain anonymous, since it is being carried out far away from actual place. Also, it enables terrorists to conduct their operations with little or no physical risk to themselves.

Cyber terrorism is consisting of physical terrorism and cyber terrorism. Cyber terrorist is exploiting technology via the Internet to implement their terrorist purposes.[1] Cyber terrorism is a new and somewhat unclear concept. However, there are so many debates behind this vague term. The debates arise from the issue whether cyber terrorism is a separate phenomenon, or just a part of information warfare practiced by terrorists.[2]

Cyber terrorism is the vicarious form of cyber crime, severely threatens the security of the nation. Dorothy Denning defines "cyber terrorism as the convergence of terrorism and cyber

* Asst. Professor, Faculty of Law, The ICFAI University, Tripura, Email: baharulislam142@gmail.com

[1] L. Carlos et al, Cyber terrorism- a rising threaten in the western hemisphere, 2006, United States Army National Guard, p 3.

[2] Cyber terrorism and cyber operation, US Army Training and Doctrine Command, 3nd Edn, pp. 17. 2005.

space. It is understood to mean unlawful attack and threats of attack against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in the furtherance of political or social objectives"[3]. Mark Pollit also defines it as a "premeditated, politically motivated attack against information, computer systems, computer programmes and data which result in violence against non-combatant targets by sub national groups or clandestine agents"[4].

DEFINITION OF CYBER TERRORISM

'Cyber terrorism is the convergence of terrorism and cyber space. It is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and 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 reast 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 upon their impact. Attacks that disrupt non essential services or that are mainly a costly nuisance would not'[5].

Cyber terrorism has become a serious threat to national and international security, as cyber terrorists seek to advance religious or political agendas.[6] There is no single common definition of the term terrorism gained universal acceptance.

[3] Michael Chance (2012), The role of cyber terrorism in the future, forensic focus, Retrieved from: http://articles.forensicfocus.com/2012/06/01/the-role-of-cyber-terrorism-in-the-future/ (Accessed on: 12/07/2016.)

[4] Medha Surabhi (2012), Cyber warfare and cyber terrorism, Social science research net, Retrieved from: http://ssrn.com/abstract=2122633, (Accessed on: 10/07/2016).

[5]http://ids.nic.in/art_by_offids/Cyber%20security%20in%20india%20by%20Col%20SS%20Raghav.pdf (Accessed on 28/07/2016)

[6] K. Gable, 'Cyber-Apocalypse Now: Securing the Internet against Cyber terrorism and Using Universal Jurisdiction as a Deterrent' (2010) 43, The Vanderbilt University Law School Vanderbilt Journal of Transnational Law, p 2.

Likewise, no single definition of the term cyber terrorism has been universally accepted. As a matter of fact, scholars who are expert in this field define cyber terrorism with different focus.

The term cyber terrorism combines two greatest fears of this century: cyberspace and terrorism. It refers to 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. Furthermore, an attack should result in violence against persons or property, or at least cause enough harm to generate fear, to qualify as cyber terrorism. For instance, attacks that leads to death or bodily injury, explosions, or severe economic loss and serious attacks against critical infrastructures depending on impact. not put a heavy burden on government, it could not qualify as cyber terrorism.[7] More comprehensively, cyber terrorism refers to the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political and social objectives".[8]

In the Federal Government, the FBI describes cyber terrorism as: "Cyber-terrorism is a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda."[9]

CHARACTERISTICS OF CYBER TERRORISM

Cyber terrorism has several distinct characteristics. These characteristics help to better differentiate the fine line between a cyber-terror attack versus a cyber attack or activities of a hacker. Cyber terrorism will and may display the following signs:

[7]D.E.Denning, cyber terrorism, 2000, http://www.nautilus.org/archives/infopolicy/workshop/papers/denning.html (Accessed on: 18/05/2016).

[8] D. E. Denning, Cyber Terrorism, 2000.

[9] H. M. Hendershot, 'Cybercrime 2003 – Terrorists' Activity in Cyberspace' http://www.4law.co.il /L373 (Accessed on: 07/05/2016).

Attack is predefined and victims are specifically targeted[10].

i. Attack has an objective to destroy or damage specific targets such as political, economic, energy, civil and military infrastructures.

ii. Attack may even target specific opposing religious group's information infrastructures to insight religious pandemonium.

iii. The purpose of any attack is to create fear of the group's intentions and further their own political agenda or goals or gain fellowship by succeeding in their attacks.

iv. Destroy the enemy's capabilities to further operate or operate within their own arena.

v. Persuade others to believe that the victim or victims are vulnerable and their stability negligent.

vi. Create increased loyalty and pride within the group based on their successes.

WHO ARE CYBER TERRORIST

But who are the cyber terrorists, are they existing terrorist groups or are they new organizations. While there are some groups of cyber terrorists in operation in the world the main threat would seem to come from groups that have historically operated in the 'real' world. In this information age, terrorist organizations, which is generally get no access to television or radio communications, can easily broadcast via the internet[11]. They maintain their Exchanges, which are often perceived as a lynchpin of each nation's economy and hold something of an iconic status, have become seen as 'fair game' for attacks from almost every

[10] "Beyond Conventional Terrorism… The Cyber Assault" by Rajeev C. Puran. *SANS*, Available on https://www2.sans.org/reading-room/whitepapers/threats/conventional-terrorismthe-cyber-assault-931. (Accessed on: 12/03/2016)

[11] Alexander, Yonah Swetman, Michael S., *Cyber Terrorism and Information Warfare: Threats and Responses*, Transnational Publishers Inc., U.S., 2001.

type of cyber terrorist, according to experts. But who are the man behind the masks?[12] Experts distinguish cyber terrorists into four main categories, as below:

a) **Criminal Gangs**

Historically, hostile cyber activity in the financial services sector has involved criminal gangs targeting retail bank platforms in a bid to steal customer funds. Increasingly, these gangs have looked to target exchanges with a view to manipulating markets and profiting from wild swings in the price of securities.[13]. The target was an unnamed financial exchange platform, and the motive of the attack was market manipulation, according to a person close to Prolexic[14].

b) **Hackers**

Recent trends on the internet and attacks shows that politically motivated 'hactivists' such as anonymous have become more active. The protests they attempt largely take the form of disrupting online services. Exchanges have become seen as 'fair game' for attacks among these groups, according to Stephen Bonner, "Radical environmentalists or human rights groups tend to not target corporate, but the companies or infrastructure that support them, such as exchanges."[15]

c) **State-Sponsored Groups**

State-sponsored cyber terrorists are also known to be on the rise and are attacking 'iconic' pieces of market infrastructure such as exchanges. Last year, Israel's Tel Aviv Stock Exchange was attacked by pro-Palestinian computer hackers and this offensive disrupted the

[12] Tim Cave, "Cyber Terrorists: the Men Behind the Masks", *Financial News*, 30 July 2013, http://www.efinancialnews.com/story/2013-07-30/cyber-terrorists-the-men-behind-the-masks?ea9c8a2de0ee111045601ab04d673622, (Accessed on: 21/04/2016)

[13] *Ibid.*

[14] *Ibid.*

[15] *Ibid.*

exchange's website. Saudi Arabian hacking group "Nightmare" claimed responsibility for this cyber attack, it came during a period of heightened political tension in the region[16].

d) **Disgruntled Insiders**

The downsizing of the financial sector can leave many former employees with an axe to grind, but for market infrastructure providers it can have dramatic consequences. Bonner said, "When exchange staff leaves, they take knowledge of risks and controls with them, as well as, potentially, software code." He recommended that exchanges review the e-mail history of all technology leavers in the period up to their departure. In November 2010, the London Stock Exchange issued a statement that a 127 minute trading outage on its Turquoise platform was caused by 'human error that may have occurred in suspicious circumstances'. However, following a full internal investigation, the incident was found to be just the result of human error.[17]

MODES OF CYBER TERRORISM

i. Cyber Terrorism is the Forerunner of Warfare

In the era of information and communication technology (ICT) one nation causes terrorist violence by using new technology against other nation or nations. These are not the conventional way of war rather cyber war or net war between two or more nations which are very much unpredictable. For e.g., net war between Israel and Pakistan, India and Pakistan, China and USA.

ii. International Cyber Terrorist Attack

When International Organizations of terrorists link or communicate between them through internet and attack any nation, it is called international cyber terrorist attack. For e.g. 11th

[16] Adrian Blomfield, "Hackers Disrupt Tel Aviv Stock Exchange and E1-A1." *The Telegraph*, Available on http://www.telegraph.co.uk/news/worldnews/middleeast/israel/9019204/Hackers-disrupt-Tel-Aviv-Stock-Exchange-and-El-Al.html (Accessed on: 03/07/2016)

[17] Tim Cave, "Cyber Terrorists: the Men Behind the Masks", *Financial News*, 30 July 2013, http://www.efinancialnews.com/story/2013-07-30/cyber-terrorists-the-men-behind-the-masks?ea9c8a2de0ee111045601ab04d673622 (Accessed on: 03/07/2016)

September 2001 attack on World Trade Centre and Pentagon; immediately after that 13th December 2001 attack at Indian Parliament.

iii. Use of Computer System and Internet Facilities

Use of computer system and Internet facilities by terrorists group to develop own websites and network to send messages to each other worldwide are effective mode of cyber terrorism117.

iv. Cyber Terrorists use Encryption Programme and Digital Signature

Cyber terrorists use encryption programme and digital signature to coordinate themselves using e-mail service which cannot be read by any one. Even the National Security Agency through their super computing system failed to crack terrorist group's code. The USA is fighting against these attacks since 1990s.

v. Terrorists Now Using Information and Communication Technology (ICT) Including Satellite Transmission

Terrorists now use ICT including satellite transmission, cell phones, wireless etc. to communicate with each other and organize for terrorist attack.

vi. Flowing Worm, Virus, Trojan Horse

Flowing worm, virus, Trojan horse etc. are used to collapse Government departments such as defence, intelligence, commerce, academic and health. Access to Global electronic network and information is one way which facilitates cyber terrorism.

MOTIVATION FOR CYBER TERRORISM

There are many different motivations for terrorists to deploy cyber terrorism as a mean to inflict damage or destruction to their targets. There are four main goals for such attacks to be carried out by terrorists:[18]

i. To destroy enemy's operational capabilities

The terrorists feel that the usage of cyber capabilities offers them a low cost and effective solution to severely damage or destroy their targets in order to force them to be unable to continue their normal operations.

[18] Axelrod, C. Warren. "Security Against Cyber Terrorism." 27 February2002. URL: http://www.sia.com/iuc2002/pdf/axelrod.pdf (Accessed on: 22/06/2016)

ii. To destroy or misrepresent the reputation of an organization, nation or alliance

Many organizations, nations and alliances are able to operate effectively and are highly respected and regarded because of their unmistakable and strong reputation. If this vital element is tarnished, it could severely impact the normal operations of the targeted entity.

iii. To persuade those attacked to change affiliation

Sometimes cyber terrorism is used in order to force the attacked entities to change their association or affiliation to certain parties. Even though this goal is much harder to be carried out, there has been cases where it has proved to be successful

iv. To demonstrate to their own followers that they are capable of inflicting significant harm on their targets

Cyber terrorists are also keen to carry out cyber attacks because they want to prove to their followers and the world that they have the capabilities of inflicting severe damages on its targets.

INTERNATIONAL EFFORT IN COMBATING CYBER TERRORISM

International cooperation in order to confront with cyber terrorism has different form of relationship among government and law enforcement agencies.

A. Effort from International and Global Organization

1) United Nation

United Nation is the lead organization which involves in the coordination and cooperation relating to the problem of international terrorism.[19] In their resolutions, they require the member states to promote the multi-lateral consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats. These resolutions have the same motive to improve the cyber security awareness at both the international and the national levels.[20]

[19] D. Yaman, the United Nation and Terrorism, legal aspect.

[20] L. Xingan "International action against cyber crime: networking legal systems in networked crime scene" webology, http://www.webology.ir/2007/v4n3/a45.html (Accessed on: 24/03/2016)

2) Interpol

Interpol has created an anti- terrorism section in September 2002 in the wake of alarming of international terrorist attack which is called Fusion Task Force (FTF). The primary objectives are to: identify active terrorist groups and their membership, solicit, collect and share information and intelligence, provide analytical support, enhance the capacity of member countries to address the threats of terrorism and organized crime.[21]

B. Effort from Multilateral and Multinational Organization

1) The Commonwealth Nations

Commonwealth nation main task is to harmonize their laws of its member states. It creates the Model Law on Computer and Computer Related Crime and had a great impact on the domestic legislation. It expands criminal liability including reckless liability for the offences of interfering with data, interfering with computer systems, and using illegal devices. Another task of the commonwealth is to consider the legal mutual legal assistant between commonwealth member and also between commonwealth member and non commonwealth.[22]

2) The Group of G 8

The group G8 is an informal forum and so it lacks an administrative structure compare with international organization. The leaders from the United States, United Kingdom, France, Germany, Japan, Canada, Italy, and Russia have been meeting annually since 1975 to discuss issues of importance, including crime and terrorism, and the information highway.[23]

3) Organization for Economic Cooperation and Development (OECD)

The OECD has been working for many years on a range of policy issues associated with the information society. These include infrastructure and services, consumer protection, privacy

[21] Fusion task force, http://www.interpol.int/Public/FusionTaskForce/default.asp (Accessed on: 03/05/2016)

[22] Legal and Constitutional Affairs Division Commonwealth Secretariat, Report on Law and Technology Workshop for the Caribbean 2003, Jamaica, 2004.

[23] What is the G8, http://www.g7.utoronto.ca/ (Accessed on: 25/04/2016).

and security, through to broader issues surrounding ICT and economic growth.[24] The OECD adopted Guidelines for the Security of Information Systems and Networks in July 2002, calling on member governments to establish a heightened priority for security planning and management and to promote a culture of security among all participants as a means of protecting information systems and networks.[25] The aim of this guideline is to aim to develop a global culture of security through advice on policies and measures to address internal and external threats such as cyber-terrorism, computer viruses or hacking in a globally interconnected society, while preserving important societal values such as privacy and individual freedom.

C. Effort from Regional Organization

1) European Union

On December, 2004 European council calls on member state to ratify the convention on the mutual assistance in criminal matters, its protocol and the three protocols to Europol convention. Also, their framework implement in other aspect such as, traffic data by service provider, cross- border pursuit, exchange of information on conviction for terrorist offences and etc. the council adopted necessary measures for council regulation to identify new and applicable function for the Schengen information system (SIS).[26]

2) Council of Europe

The main task of council of Europe since 1949 was to maintenance human rights, the rule of law and pluralist democracy, and is determined to combat terrorism which combats with

[24] http://www.intgovforum.org/brief.htm (Accessed on: 05/-4/2016).

[25] http://www.intgovforum.org/brief.htm (Accessed on: 07/06/2016).

[26] Declaration on Combating Terrorism, pp. 7. http://www.tmmm.tsk.tr/regulations_en.htm (Accessed on: 03/07/2016).

these values. It tried to fight against cyber terrorism by strengthening legal action against terrorism, safeguarding fundamental values, and addressing the causes of terrorism.[27]

The Council of Europe set its focus area on cyber terrorism and the subject of CODEXTER (the Committee of Expert against Terrorism) is about cyber terrorism. It has been surveying the situation in member states to evaluate whether existing international instrument are sufficient to respond cyber threat or not.[28]

3) Convention on Cybercrime

The Convention put into effect in July 2004, which is the first and only international treaty to deal with breaches of law over the Internet or other information networks. This convention has not only been ratified by all European Union member states, but also it does not specifically address cyber terrorism. The Convention requires participating countries to update and synchronize their criminal laws against hacking, infringements on copyrights, computer facilitated fraud, child pornography, and other unlawful cyber activities.[29] Indirectly, it can be applicable for cyber terrorism as well. Although the convention on cyber crime does not define the term cyber crime and cyber terrorism specifically, Article 2 to 6 mention various forms of criminal activity that are prohibited which may include cyber terrorism activities.

4) Council of Europe: Convention on the Prevention of Terrorism

The Council of Europe has adopted the Convention on the prevention of terrorism to increase the effectiveness of existing international texts on the fight against terrorism. The aim of the convention is to strengthen member states' efforts to prevent terrorism and sets out two ways to achieve this objective: first, establish a certain acts of criminal offences, and second, it reinforces the cooperation on prevention both internally (national prevention policies), and

[27] Council of Europe, human right and legal affairs, http://www.coe.int/t/e/legal_affairs/legal_cooperation/fight_against_terrorism/1_General/ (Accessed on: 08/-3/2016).

[28] Council of Europe, human right and legal affairs, http://www.coe.int/t/e/legal_affairs/legal_cooperation/fight_against_terrorism/4_Theme_Files/ (Accessed on: 16/06/2016).

[29] C.wilson, Botnet, Cyber Crime, Cyber Terrorism: Vulnerabilities And Policy Issues For Congress, congressional research service.CRS report for congress, 2008.

internationally (modification of existing extradition and mutual assistance arrangements and additional means). In other words, the Convention contains a provision on the protection and compensation of victims of terrorism.

5) Asia Pacific Economic Cooperation (APEC)

APEC is a regional forum which was established in 1989 for facilitating economic growth and its goal is to strengthening the Asia- pacific community. APEC has 21 members and it has not obliged their members and decisions made within (APEC) are reached by consensus. After September terrorist attack on United States, APEC issued a statement on counter-terrorism and condemns these attack and effort to collaborate to fight against terrorism.

6) North Atlantic Treaty Organization (NATO)

NATO was founded in 1949 on the basis principle of collective defense. The parties are following the basic principle of the Charter of the United Nations. This cooperation and commitment to security continues among the members nations today. However, the Internet, cyber space and cyber crime were not in existence at the time that NATO was established. Nevertheless, NATO has changed their political and technical requirement and improved their capabilities in the area of cyber defense. NATO has also to address new challenges and posed by terrorists and the threats to computer information systems (CIS).[30]

7) International Multilateral Partnership against Cyber Terrorism (IMPACT)

The International Multilateral Partnership Against Cyber Threats (IMPACT), backed by the United Nations (UN) International Telecommunication Union (ITU) and International Criminal Police Organization (Interpol), which is known as the world's first comprehensive global public private partnership between governments, industry leaders and cyber security experts to enhance the global community's capacity to prevent, defend and respond to cyber threats. It has launched its global headquarters in Malaysia on 20th March 2009. It will act as a centralized anti-cyber-terrorism intelligence centre which allows its 191 member countries

[30] http://www.impact-alliance.org/ (Accessed on: 12/04/2016)

to be alerted on cyber terrorism threats such as attacks against the global financial system, power grids, nuclear plants, air traffic control systems and others.

THE INFORMATION TECHNOLOGY ACT, 2000

So far as India is concerned in order to combat cyber terrorism through law, the Information Technology (Amendment) Act, 2008 has been enacted to include the same within the meaning of offences and therefore, is made punishable. Though, cyber terrorism has not been defined, but sec. 66(f) of the Information Technology (Amendment) Act, 2008 prescribes as to when cyber terrorism is said to have been committed. Sec. 66(f) of the said Act reads as to the following effect-

"Whoever:- (A) With the 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) By 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;

And by means of such conduct causes or is likely to cause death or injuries to persons or to damage to or destruction of property or disrupts or knowing that it is like 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 for the security of the state or foreign relations, or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used

to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the state, friendly relations with foreign states, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, Commits the offence of cyber terrorism.

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

RECOMMENDATIONS:

Prevention is always better than cure. It is always better to take certain precaution while operating the net. Some other suggestions to prevent and reduce the incidence of cyber terrorism at domestic level are as follows:

1) Statistics indicates that instead of hacking by outsiders, maximum security breaches are the consequences of insider misconduct it may be ignorance of the users. Users must take reasonable precautions to secure files and data on their computers, e.g., back up important files, use an updated virus scanner, regularly monitor for download and install security patches from the vendors of the software, use a strong secure password for network access controls, and ensure permissions are set properly on files that can be accessed by others.
2) Individuals generally reveal their personal information while transacting online. In this process their personal information becomes available for unwanted cybercriminals. A self-regulatory approach is the best way for protecting privacy on the Net is worthwhile both in itself and as a way to avoid government regulation. Self-regulation may be suggested as one of the practicable solution to reduce the incidence of cyber crime.

3) Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. This process protect the information from unauthorized persons and it can be used only when it decrypt by the authorized person. Therefore, encryption technology shall be made mandatory at all levels of government, semi-government and non-government organizations and commercial organizations which are depended on the computer technology and having critical infrastructure.

4) The centralized management of intrusion-based security technologies can be used as preventive strategy called as the 'intrusion management'. It can be used for testing, detection and investigation of cyber crime. Intrusion management technology is highly recommended for the entities which are dealing in the information critical infrastructure.
5) The law enforcement agencies must perform their tasks without any fear or pressure. All laws related to search, seizure and arrest of cybercriminals shall be liberalized and the investigating agencies need more teeth, in the form of training and powers.
6) Biometric techniques can be the best tool identifying the real perpetrator of cyber crime. Biometrics involves electronic analysis of attributes arising from a person's physical characteristics that are unique to that person.
7) The cyber criminal laws of various countries including cyber law should be universalized so as to extend adequate protection to citizens, institutions, organizations, government and nongovernment agencies and society as a whole against the menace of cyber terrorism.
8) It is highly suggested for the effective implementation of law to have extradition treaties with the other countries. Extradition treaty will solve the problem and cyber terrorists and criminals can be brought to India and *vice-versa* for trial and prosecution in accordance with the established principles of international law.
9) In the age of internet India is not an exception, it is on way to computerization of all data. All the networks relating to the government are controlled and managed by the National Informatics Centre (NIC). The history of cyber attacks shows that the cyber terrorists always prefer to attack the primary source of network. So, it is high time to reconstruct National Informatics Centre for the better cyber security.
10) Mass level awareness programme must be conducted, where the cyber experts provide the information and cyber security issues to all the entities, dealing in critical information infrastructure particularly.
11) Every set of persons involved in investigating or combating cyber crimes, in various states of a countries or even in other countries across the world must worked in a networked environment if the nature of case demands. Technical experts from various countries can share their knowledge and help solving complex cyber crimes.
12) Special courts should be set up for the trial of cyber crimes and its presiding judges should be properly and technically trained to evaluate evidence technologically.

EXAMPLES OF CYBER TERRORISM[31]

Some attacks are conducted in furtherance of political and social objectives, as the following examples illustrate:

i. In 2000, a Japanese Investigation revealed that the government was using software developed by computer companies affiliated with Aum Shinrikyo, the doomsday sect responsible for the sarin gas attack on the Tokyo subway system in 1995. "The government found 100 types of software programs used by at least 10 Japanese government agencies, including the Defense Ministry, and more than 80 major Japanese companies, including Nippon Telegraph and Telephone."[32] Following the discovery, the Japanese government suspended use of Aum-developed programs out of concern that Aum-related companies may have compromised security by breaching firewalls. gaining access to sensitive systems or information, allowing invasion by outsiders, planting viruses that could be set off later, or planting malicious code that could cripple computer systems and key data system.[33]

ii. In March 2013, the New York Times reported on a pattern of cyber attacks against U.S. financial institutions believed to be instigated by Iran as well as incidents affecting South Korean financial institutions that originate with the North Korean government.[34]

[31] https://en.wikipedia.org/wiki/Cyberterrorism (Accessed on 28/07/2016)

[32] Maryann Cusimano Love, Public-Private Partnerships and Global Problems: Y2K and Cybercrime. Paper Presented at the International Studies Association, Hong Kong, July 2001

[33] Calvin Sims, "Japan Software Suppliers Linked to Sect," The New York Times (March 2, 2000): A6.

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

iii. In August 2013, media companies including the New York Times, Twitter and the Huffington Post lost control of some of their websites Tuesday after hackers supporting the Syrian government breached the Australian Internet company that manages many major site addresses. The Syrian Electronic Army, a hacker group that has previously attacked media organisations that it considers hostile to the regime of Syrian president Bashar al-Assad, claimed credit for the Twitter and Huffington Post hacks in a series of Twitter messages. Electronic records showed that NYTimes.com, the only site with an hours-long outage, redirected visitors to a server controlled by the Syrian group before it went dark.[35]

iv. Pakistani Cyber Army is the name taken by a group of hackers who are known for their defacement of websites, particularly Indian, Chinese, and Israeli companies and governmental organizations, claiming to represent Pakistani nationalist and Islamic interests.[36] The group is thought to have been active since at least 2008,[37] and maintains an active presence on social media, especially Facebook. Its members have claimed responsibility for the hijacking of websites belonging to Acer,[38] BSNL[39], India's CBI, Central Bank, and the State Government of Kerala[40].

---

[35] http://www.thedailystar.net/beta2/news/new-york-times-twitter-hacked-by-syrian-group/ (Accessed on 28/07/2016)

[36] *"Pakistan Cyber Army (PCA) – Hacking Indian Websites, Promoting Pakistani Interests In Cyber Space And Nurturing Pakistani Hackers | The Cyber & Jihad Lab". cjlab.memri.org.*(Accessed on: 23/07/2016)

[37] *"Debugging the Pakistan Cyber Army: From Pakbugs to Bitterbugs - ThreatConnect | Enterprise Threat Intelligence Platform". Threat Connect | Enterprise Threat Intelligence Platform.* (Accessed on: 22/04/2016)

[38] *India; Censorship; China; Japan; Apple; Reg man says to Honkers, ponders Asia's future role in tech world; month, Acer founder Shih to step down for second time next; themselves, Script fools n00b hackers into hacking. "Pakistan Cyber Army declares war on Chinese, Bangladeshi sites".* (Accessed on: 29/04/2016)

[39] *Saxena, Anupam (2011-07-28). "BSNL Website Hacked By Pakistan Cyber Army: Report". Media Nama.* (Accessed on: 22/04/2016).

[40] *"Hacked by 'Pakistan cyber army', CBI website still not restored". NDTV.com. Retrieved 2016-05-28. 'Indian websites are more vulnerable to cyber attacks from Pakistan-based hackers on major events' | Latest Tech News, Video & Photo Reviews at BGR India". www.bgr.in.* (Accessed on: 25/04/2016).

CONCLUSION

In conclusion, it can be said that the traditional concepts and methods of terrorism have taken new dimensions, which are more destructive and deadly in nature. In the age of information technology the terrorists have acquired an expertise to produce the most deadly combination of weapons and technology, which if not properly safeguarded in due course of time, will take its own toll. The damage so produced would be almost irreversible and most catastrophic in nature. In short, world is facing the worst form of terrorism, popularly known as cyber terrorism.

The law dealing with cyber terrorism is, however, not adequate to meet the precarious intentions of these cyber terrorists and requires a rejuvenation in the light and context of the latest developments all over the world. The laws have to take care of the problems originating at the international level because the Internet, through which these terrorist activities are carried out, recognizes no boundaries. Thus, a cyber terrorist can collapse the economic structure of a country from a place with which a country may not have any reciprocal arrangements, including an 'extradition treaty'. The only safeguard in such a situation is to use the latest technology to counter these problems. Thus, a good combination of the latest security technology and a law dealing with cyber terrorism is the need of the hour.