



International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)

www.iasir.net

Cyber Terrorism a Threat to National Security

Dr. Rishipal
Head and Professor AIBAS,
Amity University, Haryana, INDIA

Abstract: Every new technology brings both boons and crush for the humanity; same is the case with cyber technology. Cyber technology has helped humanity in solving very simple to complex problems of masses. On the one hand cyber technology has addressed the problems of day to day life related to the basic needs, comfort, luxury etc. on the other hand this technology has resulted in devastating consequence of cybercrimes and terrorism. This study will discuss the concept of cyber terrorism by taking the account of the existing plethora of knowledge. The objective of this research is to focus on the cyber-threat and cyber terrorism, and attempt to prove that all of the threats falling under the cyber technology cause highest degree of terror and loss of life through damage to critical infrastructure and present the largest danger to the national security.

Keywords: Terrorism, Cyber-terrorism, National security,

I. Main Text

A. Terrorism

Terrorism is one of the oldest destructive human activities existing here on this earth from the very beginning of human societies and it has escalated gradually over in the past years. Now a day, terrorism has engulfed the whole world in its clutches and has become one of the most serious socio-political and governance problems. As a result of advancement in technology, the terrorists have become more threatening and damaging and the executors of terroristic acts are becoming more indescribable. Terrorism is a dynamic process and exists in many forms but the motives of terrorism remain the same. Present day humanity faces various types of strange and new terroristic attacks which are executed by using different type of physical and virtual weapons. The whole world is united to fight against terrorism by using its national and international law and order maintenance system, intelligence & communication network, security measures, policies, programmes and other tactics. But all these agencies and paraphernalia involved in the process of terrorism combating and expected to safeguard the humanity, are not able to fight effectively against this destructive enemy. The policies, programmes, strategies, networks and infrastructure developed over the years by various national and international governance systems for combating terrorism are not sufficient and effective enough. Terrorists, no longer attacks only on the human beings, resources, infrastructure and facilities by using conventional weapons rather they have started involving in cyber-space and cyber-infrastructure for terrorism. This paper has studied the potential threat of cyber-terrorism on India's national security.

B. Cyber Terrorism

Cyber terrorist can easily have access into country's key facilities, resources, infrastructure and vital security issues through cyber-space to have control on them for causing serious damage to the living beings, infrastructure and economic system of a country. Such attacks are specifically executed to cause severe loss to information technology systems which may be vital for mass safety, transportation, communication, hospitals, emergency services and public works. The term cyber terrorism was first used 1980's by Senior Researcher at the Center for Strategic and International Studies (CSIS) Barry Collin as "the international abuse of digital information system, network, or component toward an end that supports or facilitates a terrorist campaign or action." Later on professionals from different field areas which are associated to fight against terrorism modified the definition. Cyber terrorism is a virtual criminal activity which involves disastrous computer involved attacks by terrorists or criminals on the data warehouse or information systems of a computer system to corrupt, change, hack of misuse it for the purpose of delinquency or personal gain. Cyber-terrorism is an activity of terrorism accomplished by using cyberspace for executing a terroristic act.

II. Cyber Terrorism and National Security

The threat of terrorism has caused an enormous challenge before the present governance systems. Terroristic activities in major cities, towns and public places across the globe have proved the insufficiency of the State mechanisms to face this challenge. Serious efforts have been made by States to address this challenge by scheming counter terrorism strategies and anti-terror machineries. However, most of these are planned in a conventional paradigm, which might be effective for conventional terror attacks only.

Information technology is exposing the cyber space user to an huge data bank of information concerning various field areas. However, it has also been exploited as a new tool for terrorism. Recent reports suggest that the terrorist groups are also acquiring and utilizing cyber space to execute terrorist attacks. The likelihood of such attacks in future cannot be denied. In the last few decades India has opened a niche for itself in IT. Most of the Indian banking industry and financial institutions have involved computers and IT for it's very significant business operations. According to various studies and international reports cyber-terrorism is mostly focused toward economic systems and financial resources of a country. Increasing dependence of the Indian transportation, railways, communication, financial and other organizations of utmost importance on computers and information technology may invite for the cyber-attacks and ultimately lead to a severe breakdown of normal functioning of these organizations. The most alarming issue is non-availability of standby arrangements or the absence of alternatives in case cyber system is not working. Detection of terrorist networks used in the recently executed terror attacks by the worldwide terrorists have proved the substantial use of cyber-tools and electronic gazettes based on the information technology like emails, cell phones, satellite phones, internet, whatsapp and other social media to communicate and conduct their terroristic activities. The matter of serious concern was the use of latest computers and other modern gadgets in association with lethal armaments like AK-47 and RDX based explosives to materialize their nefarious mental designs. The sole aim of terrorist bodies is to realize their potential and evil designs for disrupting purposes in minimum possible efforts and expenses, so they will depend maximum on latest technology.

III. Type of Cyber Terroristic Attacks

Computer viruses and worms are the frequently used weapons for cyber terrorism. That is why in some cases of cyber terrorism is also called 'computer terrorism'. The cyber-terroristic attacks can be classified into three different groups:

(a) Damaging Computers Hardware: Use of conventional armaments like bombs, bullets and fire etc. to damage the physical computer infrastructure.

(b) Syntactic Attack: Computer worms, viruses and Trojans are used in this type of attack. Computer infrastructure works with the help of combined functioning of inbuilt hardware and installed software. If computer software is corrupted by inducing worms, Trojans and viruses in it then it will either delay or not execute the desired function which will further deteriorate the major function like communication or transportation system for which it was under use.

(c) Semantic Attack: In this type of cyber-terroristic attack, the information stored in the computer system for a specific purpose is modified, changed or deleted during accessing or exiting the system without the knowledge of the owner of system.

Cyber terrorism is not only the tool to cripple the computer network system but also it is used to help the traditional terrorism like suicide bombings of computers, Internet and information gateways . Internet and emails have become an easy mode for organizing a terrorist attack. Most common use of Internet for cyber-terrorism is developing and designing the fake websites for misleading publicity. This type of activities are categorized as psychological warfare.

IV. Weapons Used for Cyber Terrorism

Different type of physical and virtual cyber tools, equipment, gazettes, and methods are being used by the Cyber terrorists to terrorize the humanity for the achievement of their ulterior and evil mottos. A brief description of some of such weapons is given hereunder:

(a) Password Hacking: Any type of illegal or unethical access into a computer system or a network of computers by someone who is not authorized is called hacking. Hacking is one of the most frequently used method of cyber terrorism used by the terrorists to cause harm and terror among people, organizations and governments. The basic technologies used for such purposes are password cracking, packet sniffing tempest attack and buffer outflow facilitates hacking.

(b) Trojans: Trojans are the computer software Programmes which can be injected in the computer system or computer networks without the knowledge of the user(s). These programmes shows that they are made for a specific useful purpose whereas in reality are designed and induced in the computers for damaging or harming their software/ hardware. Some of them are popularly known as the wooden Trojan Horse of the 12th Century BC.

(c) Computer Viruses: These are again a type of computer programmes. Cyber-criminals or terrorists can forcefully inject these programmes with the support of some useful programme, without the knowledge of user. These programmes can infect the computer system and its useful programmes by modifying and deteriorating the software's working. These viruses spread very quickly from one computer system to other.

(d) Computer Worms: Computer worm is the self-contained type of computer programme(s) which can spread its functional copies or it's subdivisions to other computer systems or networks generally via network systems.

(e) **Malware:** It is one of the mischievous software which is induced in a computer system by a host programme to disrupt the functioning of a computer system or network. Malware cripples the operations of a computer system to gather sensitive information against the desire of the user. Malware is a comprehensive term which includes different type of hazardous and damaging software like browser hijacker, rogue security software, keyloggers, worms, viruses, Horses, Trojan, spyware, Ransomware, backdoors, rootkit, scareware, adware etc.

(f) **E-Mail used as host programme for viruses and worms:** Worms and viruses need a host programme to have access in the desired computer systems. Emails can effectively perform the role of the host programme. E-mails may also be used for dissemination of terrorizing type of information, threats and offensive matter.

(g) **Refusal of Services:** These are the cyber-crimes executed willfully when an authorized user of a cyber-space is not allowed have access to a computer or computer network.

(h) **Cryptology:** When encryption and high frequency encrypted voice/data is accessed by the unauthorized user is called cryptology. It is very tedious and intricate job to decrypt the data, terrorists transport data by using encryption.

V. Cyber Terrorism Challenges for Indian National Security

India is successfully moving towards digital India and this has become possible because of India's reliance on computer and information technology. Besides this, India is struggling very hard for effective governance, to achieve this goal; e-governance is one of the effective tools. E-governance is possible with the help of application of computer and information technology. For achievement of this goal India has already started implementing the e-governance among it's major sectors like railways, aviation, communication, travel, transportation, income tax, land registration, banking, police, passport, judiciary, and visa etc. and rest of other sectors to follow. Besides this the newly emerged sectors of e-commerce, social media, e-banking and stock markets etc. are also solely dependent on the computer and IT. To terrorize the country, all these cyber-sectors are an open invitation to target and paralyze various national and international services by using cyber terrorism weapons. These types of cyber-terroristic attacks can ultimately results as a severe challenge to the national security and also economic & financial losses. The damage caused by these attacks may happen to be disastrous and irrecoverable.

VI. Impact of Cyber Terrorism on India

Use of Internet is a boon for individual, community, society, organizations state and government for their purposes might be involved in constructive and positive activities or in destructive and negative (like terrorism). Internet has penetrated in all the walks of life by involving all the spheres of working. Nearly the whole world is under influence of internet including terrorist

groups Al Qaeda one of the most deadliest groups of terrorists used internet in one of its most damaging terrorist attacks of 9/11 on the United States, specifically for planning, funding, messaging, recruitment, and execution. Not only AL Qaeda, other terrorist groups like Islamic State are also using cyberspace for terroristic activities.

According to Global Cyber Security Market Assessment, 2014 conducted by Frost & Sullivan, cyber-crime is costing much more than the trafficking of illegal drugs. This report reveals that cyber-crime victim in every three Internet users.

Multiple networking of computers and other similar electronics gazettes like notebooks, mobile phones and tablets has created lot of possibilities for executing terroristic activities by unauthorized and illegal access to critical data of vital importance of national security.

Indian governance system was taken aback by the detection of the IS twitter account user from Bengaluru. He was involved in the enrollment of IS volunteers for the last many years. As per one of the national security advisor hundreds of Indians are involved in such type of activities. When Twitter India was questioned for all this, it could not respond properly because of security and privacy reasons and could provide review report only. Not only this, another case of Whatsapp message sent by an officer of Indian defence services about terrorist attack on army camp in Uri in the year 2014 was also intended at creating rebellion in the army.

Some of the Cyber terrorists groups have also acquired the ability to develop and use proxy servers and complex code for communicating by opening e-mail accounts which can disappear if not accessed within 24 hours.

Terrorist groups working at international level are generally running hi-tech centres to connect with terror cells in different countries. One of such centre run by Indian Mujahadeen was found working at Karachi in Pakistan and this centre is having connections with its sub-centres at India, Nepal, Maldives, Sri Lanka and Bangladesh.

A video message released by Al Qaeda, showing about the cyber-attacks on the US government computer networks and crucial infrastructure like electric grid etc. All of the above incidences can clearly explain the impact of cyber terrorism on national security.

VII. Steps Taken by Indian Government to Curb Cyber-terrorism

The horrifying effect of cyber terrorism has forced Indian and other state's governance systems to formulate new legislations to address the newly emerged devastating cyber terrorism for the protection of critical computer networks and information technology which is necessary for the protection of national and economic security.

India has also developed and installed 'Lawful Intercept and Monitoring' systems to check and control the Internet based activities of the country people. These systems have been deployed to monitor internet transmission and communication through Web browsing, e-mails, Skype and other Internet activities. The Lawful Intercept and Monitoring systems are installed between the edge router and core network for complete indiscriminate access to the online activity of the country's users. Indian government has also appointed a coordinator to control over the new inter-agency structure of cyber security. This new system developed by the government of India is overseeing the various interconnected government organizations of key departments like the defence, National Technical Research Organization, and different ministries, whereas CERT will function as authority to control cyber protection.

The growing threat of different terrorist groups such as ISIS and Al Qaeda etc. has forced the countries to take a non-governmental step to implement a Counter Extremism Project which was launched in the US with Israeli assistance to face the alarming threat from the terrorist groups.

Protection of only state bodies from the cyber terroristic activities is not enough, as now a day, the private sector is also involved in production of vital goods and services at mass level with the support of computer and information technology. If the cyber space of these private sector organizations is attacked by the terrorist groups it may cause lot of damage to the organizations and hardship for the common man in the form of non-availability of goods and services. So participation of public, private and government sector is necessary to face the problem effectively.

India should also take similar steps as taken by China on the issue of national security from cyber terrorism. One of the Chinese information technology company established in 1998 has been ranked 4th among 100 top Internet provider companies by Forbes magazine. This company offers similar facilities and cyber services as Facebook, Skype, Amazon, Twitter, Microchat, Wizard, Gaming, Google, etc.

Hundred percent securities against cyber-attacks is something which is totally impossible but we can moderate these threats upto appreciable level by developing a mechanism to effectively oversee the use of IT in the country, a national level system for proactive protection of computer systems/ network and information technology.

VIII. Organizations which can support to Check Cyber Terrorism

National Informatics Centre (NIC)

NIC is one of the premier government organizations which is providing operative support to develop national and international level networking for Central & State Governments, Union Territories, Districts and other Governments bodies for effective e-governance. NIC delivers extensive range of information through well-developed computer and communication technology. NIC also provides national level communication network for government services for nationwide transparency in the deliverance at national and local level.

Indian Computer Emergency Response Team (Cert-In)

Cert-In is another key body working for the Indians cyber space. This cyber body is catering its services to ensure nationwide security to the cyber space by developing the security for communications system and infrastructure for IT, through effective collaboration to ensure flawless security.

National Information Security Assurance Programme (NISAP)

National Information Security Assurance Programme (NISAP) is working for Government to manage and protect critical cyber infrastructures, details of its objectives are as under:

- (a) Cert-In should form a panel of auditors for effective implementation of IT security.
- (b) Cert-In should regularly be reported for security policy observance on a specified interval basis by all the organizations.
- (c) Government should develop effective policies, programmes, optimum infrastructures and a point of contact for the security of country's cyber space and IT.
- (d) Every organization should implement security control policy and system and also report the problem faced in the security to Cert-In.
- (e) NISAP should involve in a third party audit of all the organizations using cyber space.

Indo-US Cyber Security Forum (IUSCSF)

The Indo-US Cyber Security Forum (IUSCSF) was constituted in the year 2001 by involving high power delegations from both side and objective of this Forum was to take several initiatives and mat the followings:

- (a) Setting up of India Information Sharing and Analysis Centre (ISAC) for effective cooperation and taking anti-hacking measures.
- (b) Setting up of India Anti Bot Alliance to spread awareness about upcoming threats from cyberspace from Confederation of Indian Industry (CII).
- (c) Creating maximum cooperation among India's Standardization Testing and Quality Certification (STQC) and the US National Institute of Standards and Technology (NIST).
- (d) The R&D group of IUSCSF will work on the complex and intricate problems of cyber security like Cyber forensics and anti-spasm.

(e) To Chalk-out the methods and procedures for strengthening the bilateral ties between the two countries for cooperation to control cybercrime.

IX. Recommendations

There is urgent need to sensitize the citizens about the dangers of cyber terrorism. Cert-in should involve academic institutions network to develop and observe an aggressive strategy for this purpose.

All the organizations public sector, private sector, government agencies, defence forces, NGOs and others should jointly work by involving qualified & skilled personnel for effective and wholesome implementation of corrective measures for cyber security.

All the organizations from different sectors, dealing in cyber security should be support for everything necessary to execute effective and foolproof security plan without giving much importance to the issue of dominance.

Agreements signed in respect of cyber space and cyber security should be given ample importance to check and control the cyber-crimes and terrorism.

Development of professionals and more financial investments is need of the hour.

Indian agencies involved in cyber security should keep a close watch on the cyber-activities of IT sector to monitor and control adversaries.

Government should come up with a comprehensive and Overarching Cyber Strategy and define clear cut roles for various governmental, nongovernmental and other agencies to generate effectiveness in cyber security implementation, maintenance and accountability.

For increasing cyber resilience governments should necessarily involve civilians as stakeholders in the cyber space security.

International code of conduct and norms for regulation, governance and penalization on the cyber space development and functioning should be decided.

References

- [1]. Albanesius, Chloe. "Surprise Vote on Internet Issues Rattles ITU Conference." PCMAG. N.p., 13 Dec. 2012. Web.
- [2]. Alexander, Yonah Swetman, Michael S. (2001). *Cyber Terrorism and Information Warfare: Threats and Responses*. Transnational Publishers Inc., U.S.
- [3]. Bibi van Ginkel, "The Internet as Hiding Place of Jihadi Extremists" (International Centre for Counter-Terrorism - The Hague, 2012)
- [4]. Blau, John (November 2004). "The battle against cyber-terror", *Network World*, Retrieved March 20, 2005
- [5]. Blumenthal, Daniel. "How to Win a Cyberwar with China," *Foreign Policy*, N.p., 28 Feb. 2013. Web.
- [6]. Carter, Chelsea J. "Official: Cyber-attacks, N. Korea, Jihadist Groups Top U.S. Threats." CNN. Cable News Network, 01 Jan. 1970. Web. 25 Apr. 2013.
- [7]. Colarik, Andrew M. (2006). *Cyber Terrorism: Political and Economic Implications*. Idea Group, U.S.
- [8]. Collin, B. C. (1997). The future of cyberterrorism: Where the physical and virtual worlds converge. *Crime and Justice International*, 13(2), 14-18.
- [9]. Conway, M. (2002), 'Reality Bytes: Cyber terrorism and Terrorist "Use" of the Internet', *First Monday* 7(11).
- [10]. Corbin, Kenneth. "Iran Is a More Volatile Cyber Threat to U.S. than China or Russia." CIO. N.p., 21 Mar. 2013. Web.
- [11]. Costigan, Sean (2012). *Cyberspaces and Global Affairs*. Ashgate.
- [12]. Goldman, David. "The Real Iranian Threat: Cyber-attacks." CNN Money, Cable News Network, 05 Nov. 2012. Web.
- [13]. Gross, Grant (Nov 2003). "Cyber terrorist attack would be more sophisticated than past worms, expert says". *Computer World*, Retrieved March 17, 2005
- [14]. Himma, Kenneth Einar. "A View of Cyber terrorism Five Years Later." *Internet Security: Hacking, Counterhacking, and Society*. Sudbury, MA: Jones and Bartlett, 2007.
- [15]. Jacqueline Ching (2010). *Cyber-terrorism*. Rosen Pub Group.
- [16]. Maras, Marie-Helen, "Cybercrime Laws: Which Statute for Which Crimes." *Computer Forensics: Cybercriminals, Laws, and Evidence*. Sudbury, MA: Jones & Bartlett Learning, 2012. 104-06. Print
- [17]. McAfee, and CSIS. *In the Dark: Crucial Industries Confront Cyber Attacks*. Issue brief. N.p.: n.p., 2011. Print.
- [18]. Meserve, Jeanne. "Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid." CNN. Panetta, Leon E. "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City." *Defense.gov*. N.p., 11 Oct. 2012.
- [19]. Poulsen, Kevin (March 17, 2005). "South Pole 'cyber terrorist' hack wasn't the first". *SecurityFocus News*.
- [20]. Rollins, John. *Terrorist Capabilities for Cyber-attack: Overview of Policy Issues*. Rep. no. RL33123. N.p.: Congressional Research Service, 2007. Print.
- [21]. Rolón, Darío N., (2013) Control, vigilancia y respuesta penal en el ciberespacio, *Latinamerican's new security thinking*, Clacso
- [22]. Schlachtenhaufen, Mark. "Officials: If You See Something, Say Something » Local News » The Edmond Sun." *Local News ATOM*. N.p., n.d. Web. 25 Apr. 2013.
- [23]. Singer, Peter W. "The Cyber Terror Bogeyman." *The Brookings Institution*, N.p., Nov. 2012.
- [24]. Thevenet, Cédric (November 2005). "Cyber terrorisme, mythe ou réalité?" (PDF) (in French). *terrorisme.net*.
- [25]. U.S. GAO – Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented." N.p., 14 Feb. 2013.