IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, February 2025

Cyber Terrorism as a New Security Threat

Mansi Kad
Assistant Professor
Global Group of Institutes, Amritsar, Amritsar, Punjab,
Mansi_kad@yahoo.in

Abstract: *In the world of evolutionary developments in the field of information and technology, the cyber space is the new reality. The present day transactions of societal interactions are no alien to the fundamental world problems where terrorism stands atop. Similarly, the operational activities of terrorism which are correspondingly taking place in the cyber space, denoted as "cyber terrorism", has been a concern for the world since its very inception. The present paper is an attempt to explore the areas of cyber terrorism while understanding and analysis its true sense and meaning. The paper also elucidates upon the legal perspective of the first world countries like United States and United Kingdom on cyber terrorism and ultimately the paper explores the law enforcement in India on this issue. The paper also analysis the impact of cyber terrorism in several peculiar facets of worldly affairs. The paper also involves examples of cyber terrorism and cyber terrorism against traditional terrorism. After that various measures are discussed for the prevention and protection of cyber security. A detailed suggestive analysis will also be put forth through this paper to put an end to the curse of cyber terrorism. According to the U.S. Federal Bureau of Investigation, Cyber terrorism is any premeditated, politically motivated attack against information, computer systems, computers programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents..*

Keywords: Cyber Terrorism, Information Technology, Cyber Space

I. INTRODUCTION

The traditional concepts and methods of terrorism have taken new dimensions, which are very destructive in nature. In the era of internet and technology the terrorists use this combination of weapons and technology in a very expertise manner if there is no safeguard is taken then the damage would be almost irreversible and most catastrophic in nature. Cyber Terrorism includes a using information technology intentionally in a harmful manner to produces negative and dangerous effect to the property, whether tangible or intangible. The Cyber Terrorism includes two elements: cyber space and terrorism. Cyber space is also known as "virtual world" which means a place where computer programs function and data moves and "terrorism" means politically motivated violence against national groups. By
combining both the definitions "Cyber terrorism is the premeditated, politically motivated attack against information, computer programs which result in violence against noncombatant targets by sub national groups or clandestine agents. For example- Hacking of a computer system and then use that information for committing illegal and organized crime. Cyber terrorism is a kind of organized crime which is done by group of people for the purpose of causing threat and making money out of it. There are various laws regarding cyber terrorism in India and in other countries but there is no effective implementation of those laws. Cyber terrorism is committed by various terrorists by way of hacking computer systems, Introducing viruses to vulnerable networks, Website Defacing, Denial-of-service attacks, terrorist's threats via email, etc. Cyber terrorism result in creating difficulty to determine the identity of the initiators of cyber-attacks. These attacks are done from any part of the world thus leads to lack of boundaries. Cyber terrorism involves low cost of tools and a single attack by the terrorists leads to great damage. IP Snoofing, Password Cracking and Denial-of-service attacks are three common attack methods of cyber terrorism. There are various cyber terrorist attacks happen in India such as 9/11 Attack, Ahmedabad Bomb Blast and 26/11 Mumbai Attack.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, February 2025

Cyber Terrorism:
Cyber terrorism is a phrase used to describe the use of internet based attacks in terrorist activities, including acts of deliberate, large scale disruption of computer networks, especially of personal computers attached to the internet, by the means of tools such as computer viruses.1 "Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb".

Modes of Cyber Terrorism:
There are various modes of Cyber Crimes committed by terrorists which are as follows:
• Hacking of the systems and data owned by government of the target country.
• Hacking of sensitive information of national importance.
• Destroying the important data.
• Introducing of virus or malware into the system.
• Temporary causing disruption to the network of the government of the target nation and distracting the top officials so that they can pursue other means of terrorism.
• DDOS i.e. distributed denial of service attack , in this terrorist first infect the data by virus and then control the whole system after that the system is controlled by terrorists from any location.

Tackling Cyber Terrorism in India:
There are various legislation enacted by parliament which specifically address the cyber terrorism. These legislation are as follows:

IT Act : The Various provisions of Information Technology Act for preventing cyber terrorism are:
• Section 66F of the IT Act – section 66f of the IT Act defines cyber terrorism. This section is introduced by way of amendment to the act in 2008 after 26/11 Attack in India. This Attack made by way of using communication services. Under this section the person who commit or conspire to commit cyber terrorism shall be punished with the imprisonment which may extend to imprisonment for life.
• Section 69A of the IT Act- section 69A of the IT Act empowers the central government or its authority to direct any agency of the government to block any information from a computer resource in the interest of sovereignty and integrity of the nation.
• Section 70B of the IT Act- section 70B of the IT Act includes Computer Emergency Response Team (CERT-IN) which is setup for providing immediate alerts of incidents challenging cyber security and also lists emergency measures for handling incidents threatening cyber security of the nation.

Unlawful Activities Prevention Act, 1967: This Act includes punishment for terrorist activities. This Act also includes punishment for person who recruiting other person for terrorist activities and for organizing terrorist camps. Use of cyber space is also punishable under this Act.

Indian Penal Code, 1860: The term "property" under this Act relate with the punishment of theft and other such crimes which further extended to cover data and results in ambit the crime of data theft.
R.K. Dalmia vs Delhi Administration : Under this case supreme court held that word
"property" is used in a wider sense . Any information stolen by the terrorists used against the sovereignty and integrity of nation is punishable under IPC.2

Cyber Security Policy, 2013: In 2013, for the first time in history, India introduce its National Level cyber security policy for protecting the cyber space security. The main aim of this security is to create a broad umbrella of cyber security framework so that Indian cyber space is secure and free from any kind of terrorists attack. This initiative is taken to protect the dignity of the nation.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, February 2025

Tackling Cyber Terrorism at the International Level:

International Telegraph Union-Unites Nations : ITU agency is a specialized agency of united states whose responsibility is to protect the information and communication technologies. Other basic role of ITU is to build cyber security in all its Members countries and also ensure international cooperation. In 2007, an agenda called global cyber security agenda was launched by ITU which is followed by all the member nations.

Who partakes in the act of cyber terrorism?

Budapest Convention: The issue of Cyber Crime and terrorism was first deal with an international convention called Budapest Convention whose main aim is to promote international cooperation among nations. It includes common policy which control Cyber Crime and cyber terrorism and also deals with the issues relating to security of data on cyber space. Two countries India and Brazil have not become party to this convention.

North Atlantic Treaty Organization: This organization also plays a vital role to protect the cyber terrorism. For achieving this objective, Cyber Defense Management Authority is created for ensuring cyber security and prevent cyber terrorism. Moreover, A Rapid Reaction Team is created to stand against the Cyber Attacks.3

Impact of Cyber Terrorism:

Cyber Terrorism is an act done by terrorists by way of using internet and computers. This leads a negative impact over world or society and also leads to affect the future. Impact of cyber terrorism are as follows:

- Cyber Terrorism leads to control over the air traffic i.e. airlines infrastructure could be hacked.
- This leads to violation of banking systems i.e. all the money could be stolen.
- Various Bombs and other explosives could be set off by the remotes.
- Important information's whether of business, governmental or hospital lose by way of cyber terrorism.
- Various secret plan of government also get exploited by cyber terrorism.
- This also leads to tempering of water system.
- Cyber terrorism leads to personal insecurity.
- Cyber terrorism lays economic as well as psychological effects over the society.
- Cyber terrorism leads to lose of money by way of hacking etc.

Cyber War- Black Out Day:

On 14th august, 2003 at "New York" Cyber War was the first war which is continued for 3 days. In this war Hackers attack on power lines and thus 100 power points are shut down and that effects lies on whole traffic, airlines power, water system and nuclear reactor. This caused by introducing virus called "Blaster". After the incident New York government struggle for 3 months to find the accused i.e. Russian Government.4

Examples of Cyber Terrorism:

- 9/11 Twin Towers Attack : Al-Qaeda laptop was found in Afghanistan. The name of the website is "Sabotage Handbook". Al-Qaeda actively researched publicity available information concerning critical infrastructures posted on web sites.
- Ahmedabad Bomb Blast (26/07/2008) : Person named Kenneth Haywood's unsecured WIFI routed in his house was being misused by terrorists. A Mail was being sent by a group of terrorists through ID named as alarbi_gujrat@yahoo.com.
- 26/11 Mumbai Attack : The accused communicated to terrorists with an email id Kharak_telco@yahoo.com which was accessed from 10 different IP addresses. Terrorists communicated with handlers in Pakistan through Callphonex using VOIP (voice over internet protocol).5

Cyber terrorism against traditional terrorism:

In the future, Due to Perceived anonymity, low risk of detection, low investment, cyber terrorism become a feasible option to traditional physical acts of violence.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, February 2025

Attack Methods of cyber terrorism:

There are mainly 3 common attack methods of cyber terrorism which are as follows:

• IP Spoofing: This refers to creation of IP packets with forged source IP address with the purpose of concealing the identity of sender. IP Snooping mostly used in Denial-of- service attacks. IP Snooping is mostly effective in corporate networks where users can login without a username or password.

• Password Cracking: password cracking can be implemented using a brute-force attacks. Password attacks usually refer to repeated attempts to identify a user account or password, these repeated attempts are called Brute-force attacks. For example-weak encryption used by Microsoft windows XP, can easily be attacked.

• Denial-of-service attacks: These attacks focus on making a service unavailable to intended users. There are two forms of DOS attacks i.e. those that crash services and those that flood services.

Prevention and Protection:

For preventing cyber terrorism and protecting cyber security a lot of preventions and cautions are needed which are as follows:

• Caution is needed while opening email attachments to protect the cyber security.
• There is a need of complete software updates.
• There must be a creation of difficult passwords for preventing Cyber Crimes.
• There must be downloading of Anti-Virus software.
• The unused applications or services must be uninstalled.
• There must be maintenance of high alert and vigilance.
• Regular updating of OS and applications
• There must be installment of ANTI-VIRUS software.

II. CONCLUSION

Information and Technology gives as many good things along with those good things it also gives us bad things that is harmful for the Nation and against the cyber security. Cyber terrorism is the one of the scary concept which arise out of technology and internet. Cyber terrorism is the organized crime done by group of people for attaining profit by illegal means. Nowadays criminals use easy ways to commit the crime. They use internet and technology to hack the systems to attain knowledge and data which they further use to commit a Cyber Attack. Various necessary facilities must be established in various parts of the country so that the cyber-crime in the world can be controlled. The information technology field is very dynamic in nature so that law enforcement authorities need to amend the act as per the changes. The preamble of Information Technology Act, 2000 provides that the act was passed with the objective to give legal recognition for transaction carried out by means of electronic data interchange and other means of e-commerce further the act also made amendments to the Indian panel code 1860, Indian evidence act 1872 and the reserve bank of India for fascinating legal reorganization and regulation of commercial activities, moreover the law should be made flexible so that it can easily adjust to the needs of society and the technology development. The cyber terrorism is a huge problem facing by the whole world, this is the crime against humanity, crime against and above all crime against civilization, the countries all over the world are trying their best to eliminate this problem cannot be effectively solved without the support of popular public and judiciary. The problem of cyber terrorism is multilateral having varied facets and dimensions. It must be noted that law is always seven steps behind the technology it is because we only used to make laws when the problems reaches at its zenith. When the problem is reach at its last stage then it is difficult to deal with that problem. This occur mainly in the cases of offences and violation involving information technology. It must be appreciated that “something is better than nothing”. The solution to any problem can be found by making check over the preventive measures of that problem. Thus, till a law dealing expressly with cyber terrorism is enacted, we must not feel shy and hesitate to use the existing provisions. In summoning up, in the field of communication and information technology, it is highly important to check the emergence and growing menace of cyber terrorism.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, February 2025

Suggestions:

The Judiciary can play a vital role in implementation of cyber law only if it is high-tech equipped. A new mechanism of administration of justice to be adopt which is called as E- Justice. E-Justice result in speedy trails which convict terrorists without any delay. Electronic records are not in permanent nature as compare to other records, so it is suggested that parliament should pass Electronic Code of Criminal Procedure for e-courts for expeditious trail.

It is suggested that scope of existing law may be extended to cover the other aspects of cyber- crime but the enforcement of those laws must not be ignored. As we heard that "Prevention is better than Cure", so various preventive measures must be taken to protect the cyber security and to prevent the cyber terrorism. These preventive measures are as follows:

• There is a need of some provisions along with the definition of "cyber terrorism", which means that the cyber terrorism is the use of computer as tool or target to cause unpredictable violence and threat in the mind of general people about safety, national security, safety and interest etc.

• International standard of security measures must be needed to protect the cyber terrorism.

• For International Communications, Local Area Network (LAN) must socially chosen by governmental agencies.

• There must be adoption of own communication, secret and confidential fiber method and they must delete important information after use to fight against virus, worm, hacking, hijacking, net-war, cyber terrorism.

• There must be regular updating of anti-virus software, changing password, updating system etc. for the prevention of cyber terrorism.

• There is a great need of awareness of IT education and training to governmental agencies as well as the general public.

• Infrastructure of law enforcing agencies also need to get improved.

• Judiciary should also get some training in this field.

• Investigating agencies must be empowered to deface terrorist's websites and network to make prevent and control over net warfare.

• Cyber terrorism may be controlled by investigating suspected wireless, mobile phones and service providers like history in the computer and through menu in the cell phone.

• Network services must be attached or connected with each other to share or exchange information to alert others for sudden attacks.

• The provisions of IT Act, 2000, IPC, 1860 must be followed to protect the cyber security.

• It is the responsibility of website owner to adopt some policy for the protection of cyber security as internet users are increasing day by day.

• Security programs must be used to control the information on the sites.

• Legislation has to enact strict laws for the prevention of cyber-crime and for the protection of citizens of the nation.

• IT Department should also provide some strict provisions regarding the use of internet and technology and some punishment which is given to the offenders.

• Victims of cyber-crime must get compensation and compulsory remedy and offenders get rigorous imprisonments as per the laws.

• Email attachments must be open carefully

• No one gives the cell phone number to the unknown person through internet or email.

• Email filters must be used to delete unnecessary emails.

• To secure the data and for the prevention of cyber terrorism, there must be a frequent change of password and also frequently checking of virus in computers.

All these measures must be followed to prevent the cyber terrorism and to make control over the cyber security. Also these measures must be followed to protect the citizens of country from cyber-crimes, which are usually done by group of people in a very organized way to earn profit by using Technology and Internet.