INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 2 | Issue 1

2020

A Critical Study on Cyber Terrorism and Its Interrelationship with Cyber Security

NAVDHA MAHESHWARI[1]

ABSTRACT

There have been various occasions of Cyber Terrorism in the previous decade. The activities of cyber Terrorism involve destruction to the protected critical computer system which has sensitive information that of the national interest, etc., which are controlled by operating computer systems. In regard to the expanding number and victory of cyber-attacks, cyber security is the cornerstone of national security. The rapidly increasing growth in digital payments in our country and the thrust towards a cashless economy has resumed center of attention on the necessity to strengthen and boost financial cyber security. The most strenuous dare in cyber security is the constantly expanding nature of security threats. Cyber terrorists can deteriorate the economy of the nation by castigating the critical infrastructure in the advanced and big towns, such as electricity and water supply. It is necessary for India to take certain steps to counter the menace of cyber terrorism. Violations of cyber security have become a day-to-day affair. As violations and contraventions start to directly affect the bottom line and is becoming common with every passing day, cyber security has come out as a serious concern. By introducing sections 66F, 70, 70A and 70B, the legislators have applied-in the most important missing links in the legislative machinery. Cyber terrorism is actuality and so is the case with cyber security. If cyber terrorism is to be defeated, one requires the latter. However, the absence of comprehensiveness in law needs to be resolved with utmost importance.

I. INTRODUCTION

India has been confronting terrorists for the previous two decades. Throughout this time, various types of terrorism have been unfolded, the recent being cyber terrorism. This high-tech configuration can lead to harm to various critical infrastructures, without even firing a bullet. Our intelligence organizations have been reprimanding about it. Cyber Terrorism refers to unlawful attacks to convict harm to computer systems or network, critical systems information with connection to one or more nations which are targeted at terrorizing its government and the people or causing distress and terror in the society for unlawful, political,

[1] Author is a student at MBA Law (1st year), NMIMS Mumbai, India.

 [ISSN 2581-9453]

social or religious goals.[2] These threats can route ruthlessness, both physical as well as virtual which leads to direct destruction to country's people and belongings or results in disturbances.

The activities of cyber Terrorism involve destruction to the protected critical computer system which has sensitive information that of the national interest, etc., which are controlled by operating computer systems. In 2007, in Estonia, various websites of the country were castigated endangering its critical infrastructure.[3] Also, it has been learnt that the cyber terrorists have discovered the process to hack the computer system of a plane, which can result in a plane crash.

There have been various occasions of Cyber Terrorism in the previous decade. US airlines encrypted files were destructed by Ramzi Yousuf, who damaged the US World Trade Centre. One other example of cyber terrorist associations is the websites named as 'Muslim Hackers' Clubs.' The said website explains the method to hack the Pentagon. When NATO started with Serbia, Serbian hacker organizations, 'The Black Hand' had condemned NATO internet infrastructures, called as the Kosovo attack. One other example of cyber warfare includes that of the Internet Black Tiger group that castigated in 1998.

On November 26, 2008, the terrorist attacks on Mumbai made it indisputably understandable that the Internet era transfigured human communications as well as the mode of waging war to execute the attacks, updated technology has been used by the terrorists.[4] The terrorists came from Mumbai through sea, by the help of Global Positioning Satellite(GPS) system. Remailer service was used by the terrorists in order to send e-mails, while sustaining anonymity which disclosed the advanced technologies employed by the terrorists to execute their attacks.[5] Eventually, it was uncovered that every call was made by the application of the Voice over the Internet Protocol (VOIP), in order to plan and execute the attacks.[6]

With the country watching Mumbai burn over number of days, there could be no uncertainty that cyberspace was one more sphere of warfare besides the Mumbai attack by land and sea. Various cyber-attacks have been there by Pakistan against India. The Kendriya Vidyalaya of Ralam, The Center for transportation Research and Management have been hacked by the Pakistan Cyber Army. The Indian Eastern Railways Portal was also hacked in the year 2008.

[2] Karnika Seth, *Computers, Internet and New Technology Laws* 360 (Lexis Nexis, 2013).
[3] Editorial, *"It is time for countries to start talking about arms control on the Internet,"* The Economist, July 3, 2010.
[4] Aparna Vishwanathan, *Cyber Law- Indian and International Perspectives,* 1 (Lexis Nexis, 2012).
[5]Kamlesh Bajaj, *Tweaking the law to deal with Cyber Terrorism*, (Feb.28,2019), http://www.lawmint.com/2009/01/-15222108/Tweaking-the-law-to-deal-with.html
[6]*Cyber Challenge*, (Mar. 1, 2019), http://www.upiasia.com/Security/indias_cyber_challenge/6678/.

In 2007, Chinese hackers damaged around 143 Indian websites.[7] Innumerable cyber attacks have taken place against Indian websites, before Commonwealth Games of October 2010. As per data and various reports, the loss of huge amount of data has been the outcome of such attacks.[8]

Some years back, a security company namely Mc Afee reported the outcome of a 5-year scrutinization known as Operation Shady ROT which investigated attacks against several nations, comprising the attacks against the Indian government, beginning in September 2010, that employed the Remote Access Tools (RAT) to attain control of systems from distant location. The Mc Afee Report, therefore comprises the attacks in opposition to the Indian Government, preceding the Commonwealth Games in Delhi in the year 2010. The said scrutinization and observation did not mention the hackers name but stipulated that the attacks arose in China.

In regard to the expanding number and victory of cyber-attacks, cyber security is the cornerstone of national security. Among all, India accounts on the 4th number for having highest volume of web users in the world. It has observed substantial increase in the cyber crimes taking place in the cyber space. In March 2010, Indian websites nearly amounting to 901 were damaged. Furthermore, the figure of 901 websites damaged was the apex for the 1st six months of the year 2010. In contrary, in the year 2011, nearly 1000 websites were disfigured and damaged on the months of April, May and June with the digits reaching around 2000 in May 2011.[9] There has been a substantial rise in cyber -crime in the nation since the year 2006.

II. CYBER SECURITY

The rapidly increasing growth in digital payments in our country and the thrust towards a cashless economy has resumed center of attention on the necessity to strengthen and boost financial cyber security. Banks and other financial institutions are outstandingly vulnerable to several forms of cyber attacks as well as online frauds. Cyber security is a method and technology to protect networks, computer system, data or any other device from unlawful, attack, unauthorized access through the way of internet or any other cyber means. In other words, Cyber security is a body of practices, techniques and technologies outlined to save networks, programmes, various devices and information from attack, destruction or unauthorized access. Another term namely, Information Technology Security may also be

[7] Kounteya Sinha, *"Hacking on overdrive:wreck 143 sites in October,"* The Times of India, Nov.16, 2007.
[8] Editorial, *"Chinese kept hacking CWG data for 2 months,"* The Times of India, Aug. 8, 2011.
[9] Aparna Vishwanathan, *Cyber Law- Indian and International Perspectives* 4(Lexis Nexis, 2012).

used sometimes, in place of Cyber security.

Cyber security has been defined under the IT Act, 2000.[10] It is the safety of internet-connected systems, incorporating software, hardware and data from various cyber attacks. Tortuous and dynamic security challenges are being faced by India, along its borders, which poses a threat to the country's internal stability and territorial integrity.[11]

In the reference of use of computers, security consists of two elements, i.e., Cyber security and physical security. Both of these are employed by enterprises and various organizations to safeguard against unlicensed or unauthorised access to various data centres and computerized systems. Information security, outlined to regulate the righteousness, confidentiality, privacy and availability of data and information is a part of cyber security.

Assuring cyber security needs the cooperation of endeavours in every phase and part of information system which involves application security, operational security, network and information security etc. One of the most troublesome components of cyber security is the persistently extending nature of security threats. The traditional outlook has been to lay focus resources on constituents of crucial system and safeguard against the biggest menace which are known to be existent in today's world, which implies leaving components unsecured and not shielding the systems against less risky threats.

To tackle with the present environment, advisory groups are furthering a more dynamic and adaptive strategy, for e.g. - The National Institute of Standards and Technology lately furnished updated regulations in its risk evaluation framework that suggests a shift towards constant monitoring and real time evaluations.

The usage of cyber security can aid in stopping cyber attacks, identity theft, privacy violations etc., and can help in risk management also.[12] A well-built network security of an organisation helps to prevent and lessen these attacks. Cyber security or information technology are the methods of safeguarding computer networks, information programs and data from unlicensed access which have an objective for destruction.[13] Various fields under cyber security are-

- *Information Security*- It safeguards data and information from unauthorized access to prevent identity theft and shield privacy. Several methods employed under this includes cryptography, identification, authorization and authentication of user, etc.

[10] The Information Technology Act,2000 (Act 21 of 2000), s.2(1)(nb).
[11] Editorial, *"India facing complex security challenges,"* The Times of India, Jan1, 2019.
[12]Margeret Rouse, *Cyber Security*,(Mar.2,2019), https://searchsecuritytechtarget.com/definition/cybersecurity.
[13] Editorial, *"Definition of Cyber Security,"* The Economic Times, Feb. 21, 2016.

- *Application Security*- It comprises steps which are implemented during the development life-cycle to safeguard applications from obstacles and various menaces that can come by the means of drawbacks in the application design, progress, utilization, enhancement or maintenance. Some core practices employed for application security include input parameter validation, session management, auditing and logging, etc.
- *Disaster Security*- It is a method that involves executing risk evaluation, setting up preferences, developing recovery policies in case of a disaster. A solid plan of action should be there in any business for disaster recovery in order to restart regular business operations as speedily as practicable after a disaster.
- *Network Security*- It incorporates activities to secure the usage, confidentiality, authenticity, safety and integrity of the network. Powerful network security aims diversity of threats and prevents them from entering or invading the network. The ingredients of network security include firewall, virtual private networks, anti-spyware, anti-virus, intrusion prevention systems.

III. IMPORTANCE OF CYBER SECURITY

Cyber Security is crucial since military, corporate, government and various other groups accumulate and store huge amount of information and data on networks and several other devices. A lot of that particular data or information can be safeguarded against disclosure that is unauthorized, the revelation of which can lead to adverse outcomes. Organizations disseminate sensitive data throughout networks as well as to several other devices during their business activities and cyber security explains the technique adopted to safeguard that information and particularly the systems employed to process as well as store the same. With the expansion of volume and worldliness of cyber attacks, certain measures are required to be taken by the organizations equipped with protecting information in relation to financial records, national security, etc.[14]

IV. CHALLENGES OF CYBER SECURITY

There has been a drastic change in the cyber security environment over the years.[15] For an efficacious cyber security, it is essential for an organization to harmonize its endeavors throughout its whole information system. The most strenuous dare in cyber security is the

[14]Nate Lord, *What is Cyber Security,* (Mar.3,2019), https://digitalguardian.com/blog/what-cyber-security.
[15]John Mason, *Cyber security challenges and trends,*(Mar.3,2019), https://www.globalsign.com/en-in/blog/cybersecurity-trends-and-challenges-2018/.

constantly expanding nature of security threats. Conventionally, organizations as well as the government have aimed many of their tools of cyber security on circumscribed security, to safeguard their important system parts and to safeguard against known risks as well. At present, this technique is not sufficient due to the advancing and dynamic nature of risks. This results in more adaptive and proactive techniques been encouraged for enhancing cyber security. In the same manner, various regulations have been issued by The National Institute of Standards and Technology (NIST), with regard to structure of core work and functions with suggestions for inclination towards continuous monitoring as well as real-time monitoring, as conflicting to traditional perimeter based model.

V. Difficulties In Executing Security Measures Against Cyber Terrorism

Furthermore, this kind of event leads to negative fame for the corporation. Its rivals could utilize this statistic against them, and the organization will most probably lose business. However, the foregoing obstacles make formulating for and shielding against a cyber terrorism attack. All it requires is an advanced and complex invasion to deteriorate a small, normal or large organization. If the attack or invasion does not destroy the organization, the cost of such renovations may be very high and the goodwill of the company may be lost.

VI. Effects And Implications Of Cyber Terrorism

Cybercrime has destructive consequences on a country as critical infrastructures carry on to become more dependent on computer systems for their working. Notable difficulties arise for national security as well as public policies haven't been able to be handled with in the past. In case, we fail to take security measures for computer systems, then cyber terrorism can easily become a helpful instrument for terrorist organizations to destroy or probably even stop critical functions of that system.[16] Various consequences are as follows:

By the help of the web, the terrorist can influence much broader destruction or change to a nation than one could through killing some humans. From impairing nation's armed forces to closing off the power in a huge sector, the terrorist can influence more people at low risk, than via other methods. Cyber terrorists can deteriorate the economy of the nation by castigating the critical infrastructure in the advanced and big towns, such as electricity and water supply. Nevertheless, the collapse in the United States, of the North Western states, in the year 2008 on August 15, is not known whether it was a terrorist activity or not, or by

[16] Dr. Amita Verma, *Cyber Crimes in India* 229(Central Law Publications,2012).

assaulting the banks and various individuals of Al-Qaeda have attempted to aim the transportation systems, electric power grids as well as financial institutions.

- *Electronic power system*- The electrical power grid is feasible for cyber terrorists. Suppose, the computer systems administering these networks could be damaged or shutdown, it could strike out power for many, which could result in prospective deaths if the network is not retrieved timely.
- *Economic and social life*- This includes forfeiture of sales during the deterioration, staff time, network obstructions, irregular access for business users, enlarged insurance costs owing to litigation, intellectual property loss- research pricing, loss of critical communications in time of crisis.
- *Water supply system*- Water systems could be one more target for cyber terrorism. For instance, if the flood barriers of a dam were aimed, a lot of deterioration could be the outcome involving the loss of lives. Furthermore, the water impartation could be closed down abandoning thousands without water.
- *Air traffic systems*- While aircrafts do not still function merely on computer networks, attacking the aircraft networks could distort it leading the thousands of postponements in flights.
- *Healthcare infrastructure*- Today, numerous of the healthcare networks depend on the web. Cyber terrorism could prospectively infect the healthcare amenities of a country. Computerized medical, hospital or health insurance data could be deleted or changed.

VII. PREVENTIVE MEASURES IN INDIA

It is necessary for India to take certain steps to counter the menace of cyber terrorism. The response needs to be an integrated endeavor of every security as well as the intelligence agencies with assistance from communication system corporations. There is a necessity to ameliorate the cybercrime police stations.[17] The procedure in this respect has started. Engineers from well-respected IT firms have been recruited to help in this, but there is a requirement to hire full time experts.[18]

National Cyber Security Council of India has recommended that the modern batch of employees in a cyber cell would definitely be computer and law graduates. This composition is favored because we require someone who has specialization not only in computer

[17] *CyberSecurity*, (Mar. 5,2019), http://www.nationalcybersecurity.in/download/DSA_April_ISSue%20article.pdf
[18] Dr. Mudawi Mukhtar Elmushraf, *"Computer Crime Research,"* The Times of India, April 08, 2004.

applications but also in law as well, owing to the fact that these both are interlinked. New batches of such combination of graduates are being sent to various training programmes.

Previous year, The Ministry of Finance updated its infrastructure to stop cyber strikes. They have found a two token arrangement which makes it compulsory that an individual take with him a usual password as well as a token that creates pin codes in actual time. While signing in, the individual will have to apply for both. In several sensitive sectors like defense, the employment of private laptops should be prohibited and very less systems should be linked to both internet as well as the intranet.[19]

Cyber security can't be dealt in segregation by any country. It needs joint attempts with other technology competent countries. Nevertheless, India is not a signatory to the 45-nation international convention on cybercrimes. Additionally, India still remains devoted to assuring the country's precious data from cyber threats, avert hacking and cyber terrorism.

VIII. INTERNATIONAL EFFORTS

The Interpol along with its 178 member nations is really doing an eminent job in contesting against cyber terrorism. They are aiding all the member nations and training their manpower.

The Council of Europe Convention on Cyber Crime, being the first ever International treaty for combating against computer crime, is the outcome of 4 years labor by specialists from the 45 members as well as the non-member nations, comprising USA, Canada and Japan. This treaty has already been executed after its ratification on 21st of March by Lithuania, in the year 2004. The Alliance of South East Asia Nations (ASEAN) has laid down schemes for sharing knowledge on computer security. They planned to create a regional cybercrime system and unit by 2005.[20]

IX. FIRST WEB WAR - THE CASE OF ESTONIA AND GEORGIA

- *Web War against Estonia*- Estonia is one of the most developed nation on the globe with regard to Internet usage.[21] On advent at the airport at Alinn, Estonia's capital city, a tourist is instantly hit by the feature that there is complementary Internet facility in the airport. Also, Estonia considers Internet access as essential and accepted to life just as the air one breathes.

In the year 2005, Estonia came to be known as the first and foremost nation on the planet to employ Internet voting in the local elections. Russia, popularly called as Estonia's historical

[19] Dr. Amita Verma, *Cyber Crimes in India* 229(Central Law Publications,2012).
[20] Vakul Sharma, *Information Technology Law and Practice* 242(Universal Law Publishing, 2011).
[21] Aparna Vishwanathan, *Cyber Law- Indian and International Perspectives* 5(Lexis Nexis, 2012).

foe, took Estonia's jump into the Internet era as a channel for prosecuting a cyber war. In April 2007, nearly one million computer systems over the planet, shut down the systems in Estonia. Also, there were huge distributed denial of service attack on various Estonian websites, comprising websites of various government ministries, etc. Estonia's Computer Emergency Response Team (CERT) set an organized answer and focused on safeguarding the most important resources while yielding less urgent infrastructure. Estonia's CERT declaredly executed an online 'deviation' policy that made aggressors hack websites which have previously been deteriorated.

- *Web War against Georgia*- In 2008, on August 12, precisely 6 days following the starting of the Georgia- Russian dispute, the Georgian Internet became the prey of a systematized cyber-attack, which accommodated various government websites with destruction and Denial of Service Attack. The Web defacement was succeeded by a Denial of Service attack which left the presidential site unable to be accessed. Several Georgian sites like those of need and various other sites were also coerced to close down by the attack.[22] It was broadly considered that the Russian Government had financed the attack owing to the fact that it coexisted accompanied by the time Russian troops furthered across the Caucasus and directed their tanks into South Ossetia.

Nevertheless, the systems used to execute the DDOS attack to be of unsophisticated Americans whose PCs have been subjected to be infected and taken over. As per the specialists, the castigation on various Georgian websites were more systematized, professional as well as advanced in character than the Estonian 2007 attack.[23]

- *Web War against India*- A common consideration has been established in the West, from constant reports of cyber strikes arising in China, that various cybercrimes derives from China. The US, France , Russia and Belgium have mentioned that China is undertaking to administer the cyber space in a derogatory manner through the means of cyber actions of the Chinese People's Liberation Army.[24] As per the reports, China has secretly set a time limit of the year 2050 for it to make it possible to prevent any form of military attack by the way of cyber warfare. Additionally, hackers have assembled into associations and Red Unions with supposed 'official backing.' At a

[22] Editorial, *" It is time for countries to start talking about arms control on the Internet*," The Economist, July 3, 2010.
[23] Stefanie Hoffman, *"Russian Cyber Attacks Shut Down Georgain Websites,"* Channel Web, August 12, 2008.
[24] Editorial, *"Nations blame China for recent cyber hackings,"* International Business Times, May 21, 2008.

corresponding time, China has safeguarded itself by a firewall called 'Great Red Firewall.'

A few years ago, it was asserted by the Belgian Justice minister that the offences in opposition to the Belgian Federal Government emerged from China and were credibly to have been accepted by the Government of China. As per a specialist namely, Mr. Brahma Chellaney, "The Chinese are inaugurating a latest front of unbalanced and uneven warfare for India." As stated by Mr. Chellaney, it is not explicit why a non-state actor would target the Government of India with regard to security.[25]

From 2006, it has been accounted that China has been prosecuting cyber-attacks not only on Indian computer networks but on governmental networks also. The Chinese are continuously scrutinizing and inspecting the official connections and networks of India which provides them control of the content and will entitle them to impair the networks during a dispute between two nations.[26]

In 2008, in the month of September, it was intimidated by the newspaper DNA that inferred Chinese hackers had contravened cyber security at large levels in the government of India along with various cabinet ministers criticizing that their email accounts have been subjected to cyber attacks, like hacking. In 2009, on February 21, it was announced by the Information Warfare Monitor that around 11 websites which were of several ministries as well as departments of the Indian government have been subjected to hacking by attackers by no other country than China. As per the details and data in the newspaper DNA, a superior officer of IT Ministry, mentioned 'Low to medium' potency cyber encroachments into web servers sustained by the Indian government have been accounted.[27]

In March 2009, as per the accounts, efforts were made at hacking the systems of Indian Embassies. Not only this, spyware was also discovered on computers. Eventually, the Ministry of External Affairs and Indian Embassies has circulated harsh rules and regulations on the use of e-mail by officials and levied rules necessitating them to constantly change passwords and to use emails only when routine communication is required. The Ministry has also started time-to-time security analysis and evaluation of all MEA computers in order to scrutinize spyware and other required computer threats.[28]

On December 15, 2009, in Delhi, several computers in the office of the Prime Minister and

[25] Editorial, *"Breaches in the past could be more damaging,"* The Economic Times, April 7, 2010.
[26] Indira Bagehi, *"China mounts cyber attacks on Indian sites,"* The Times of India, May 5, 2008.
[27] Editorial, *"Hacking,"* The Economic Times, Nov. 28, 2017.
[28] Editorial, *"Computer Threats,"* The Hindu, Jan. 30,2012.

the Ministry of External Affairs were reportedly hacked by positioning a 'Trojan virus' from a mail allegedly sent from China. The said virus authorized the attackers to retrieve and delete the confidential Gmail Accounts of functionaries of the government.[29] The attack was uncovered by Google engineers in North California, who then arranged a confidential counter- offensive attack in order to find the Chinese invaders who had retrieved the government's personal Gmail accounts. The scrutinization were able to check the IP addresses as well as the Media Access Control (MAC) addresses of the hackers and made sure that they derived in China.[30]

As per a news in The New York Times, a group from Google distantly retrieved a computer system in Taiwan that they presumed to be the genesis of the attack and then discovered that the said attack had been schemed on the Chinese mainland. The concealed virus had occurred in an email and was planted in an Adobe Acrobat extension which had violated both Gmail as well as the security of various other networks. The Indian scrutinizers as well as Google engineers were of the opinion that the data appropriated by the way of Trojan could only be of advantage to a government.

On December 15, 2009 itself, several US computers, encompassing Google, broadcasted cyber-attacks from China, however China has refused to have any part in the attacks. The attack was outlined by National Security Advisor, namely, MK Narayan, who was quoted as stating that- This is not the first instance of an attempt to hack into our computers. Disturbed about the mentioned attack, The Government of India redirected a group of Intelligence executives to investigate the security norms of the computers in crucial Indian persuits around the world.

In April 2010, a high alert was furnished by the Army CERT, to every military establishments and installations to protect against concentrated large scale cyber attacks, which are being targeted on internet facing government associations, eminent brands as well as corporate brackets.[31] A Shadow Report of April 2010 describes how an India-centered group of spies , employed social networking sites including Yahoo, Blogspot , Twitter, Google groups mail attain charge of computers in our Nation after being contaminated by virus and other malware. The Shadow surveyors discovered that the hackers had appropriated confidential documents and information from the Indian Government.

[29] Editorial, *"External Affairs Ministry networks hacked,"* The Times of India, Jan. 16, 2010.
[30] Editorial, *"China behind hacking Indian government computers,"* The Economic Times, Jan. 19, 2010.
[31] Rajat Pandit, *"Army braces for cyber attacks-goes on High Alert*," The Times of India, April 7, 2010.

As per the above-mentioned report, Information with regard to various Indian missile systems was also appropriated. Various organizations infected by the attacks have been mentioned by the Shadows Report, which involves the National Security Council Secretariat and several other military educational institutions, companies, associations, etc.[32] An element called as Key Logger is also very destructive. Key logger is a computer programme which does screening of the systems and their data the second an individual hits a key on the keyboard. This data is in transferred to an outside controller so that it becomes possible for them to know when we change our password.

X. PRESENT SCENARIO

Computer malfunctioning, electronic perils and crippling risks explains the current era, where the whole planet has been transfigured into a Silicon Valley connoting legal revolution. Advantages are there and there is no suspicion in it, however, the threats involved therein increases uninvited concerns and apprehensions.[33] The word cyber terrorism builds up a persona of global calamity, changing the prescription formulae of hospitals causing thousands to perish, expanding pressure in the imparting of sub urban gas, leading to explosions and deteriorating communications of several U.S. banks as well as the economy also crashes into a fissure.

A terrorist always mishandles technology, making the innocent agonize miserably and least distress is caused to the terrorist himself. Such scenario of tragedy incorporates the daily diet of people enrolled to engage in cyber terrorism, 'the Internet's next bad thing.'[34] Luckily, this type of calamity is an engineering sensation and cannot be the work of a savage. The latest history and several studies have proved that the digital skill of the cyber terrorist is quite distant from the extremity where it can transpire as a real danger.

The enormous situation produced so far is now deprived of retaining its effect. Despite the fact that we are in the middle of emerging risks, still the "fire-spewing dragon of cyber terrorism," is yet at a secure distance and the whole situation is over-hyped. Nonetheless, the scenario is worrying and desires one to be ready to deal with the same. India is regarded to be inactive in advancing corrective evaluations in the occurrence of a web attack and has been unsuccessful to emerge with a combatant policy to counter the attacks and to improve the cyber security condition of the nation.

[32] *Id*. at 61.
[33] Talat Fatima, *Cyber Crimes* 194 (Eastern Book Company, 2016).
[34] Editorial, *"Data breach incidents in India higher than global average,"* The Times of India, July 23, 2018.

Violations of cyber security have become a day-to-day affair. As violations and contraventions start to directly affect the bottom line and is becoming common with every passing day, cyber security has come out as a serious concern.[35] It is now not just a technical issue which can be bequeathed to the IT groups to handle. Over the previous years, these breaches have gone more than financial crimes to well-arranged attacks on critical infrastructures.

XI. THE NATIONAL CYBER SECURITY POLICY

The National Cyber Security Policy plays a very important role in today's world. It differs from that of US and UK on account of degree of application or the characteristics and action plans. Accomplishment of proper application of the policies would require taking into consideration the cultural dissimilarities which could either hamper the implementation or uplift adoption.

Customary cyber security threat modeling methods have taken a sequential, deterministic attitude to cyber security risk management. It is internationally perceived that humans are the fragile brackets in cyber security to the degree that the proclamation "users are the enemy" has been discussed over about two decades in order to interpret the behavior of the operator while dispersing with cyber security issues.

India's National Cyber Security Policy was published by the IT Ministry Government of India in the year 2011 dated 26th March.[36] The mentioned policy recommends the formation of cyber security acknowledgement in the nation, boosting of the cybercrime incident response, advancing data protection techniques and law implementation potential for efficacious cybercrime prevention as well as prosecution targeted at enhancing user reliance on the Internet.[37]

The policy motivates constructive compliance of top International practices in cyber security and advances public private cooperation to tackle with cyber security problems. The Policy contemplates setting up of not only public institutions but private institutions also, in order to execute scrutinization, examine and organize watch, warning certain actions, allowing information exchange and help in restoration efforts.

The scheme also offers institution of sectoral CERTs in various critical sectors, for eg.- finance, energy, transportation, etc., which would comprise of its local squad of workforce

[35] V. Ananda Kumar and Krishan K. Pandey, "*Cyber Security and Culture: An Interdisciplinary Approach to Security for Cyber Security Professionals,"* 2 IJCC 130 (2015).
[36] Karnika Seth, *Computers, Internet and New Technology Laws* 396 (Lexis Nexis, 2013).
[37] Sandeep Mittal, *"Understanding the Human Dimension of Cyber Security,"* 2 IJCC 141(2015).

for incident response.[38] Furthermore, it also suggests Audit of Information Infrastructure yearly as well as designation of Chief Information Security Officer (CISO), well learned in information security to be appointed as a 'Point of Contact' to harmonize security policy, observance and intercommunicate with the Indian Computer Emergency Response Team, Department of IT, etc.

Additionally, it recommends foundation of Information Security Assurance Framework, encompassing the conception of national conformity assessment infrastructure. It focuses on pointing out the guarantee of the security pre-requisites of government as well as of critical infrastructure associations by the means of 'Enabling and Endorsing' activities.[39]

Enabling activities are supervisory attempts of government or its sanctioned establishments and endorsing actions are necessarily profit-oriented and may include more than one service supplier which provides such kind of services on fulfilling required qualification eligibility and acquaintance. These involve evaluation and accreditation of fulfilment with top IT policies in order to preserve security compliances and regulations, product assessment for security criterion. Instructing of IT security groups and other services in order to assist users in retaining IT security and requisite compliances.

The government of India has suggested application of Security Policy in conformation with the Information Security Standard. Presently, in India, around 246 establishments have acquired certification in opposition to the Information Security Standard. Aggregate number of these certificates across the globe accounts to 2814.

Additionally, Security Advisors have been enrolled for auditing and executing risk assessment of computer systems as well as networks of various government organizations, critical infrastructure associations and other sectoral associations. Currently, the government accredited the National Security Policy 2013, which carries with itself an objective to intensify cyber security in the nation and pay concentration on instructing and teaching the personnel. It targets to improve cyber security intelligence and avert cyber attacks and improve the incident response. The value and importance of cyber security is increasing day-by-day. It is mainly due to the following reasons-

1.) More and more establishments and associations are functioning online and therefore becoming more dependent on the Internet.

2.) More devices are linking to the Internet. Such devices are not limited to the computers or

[38] Carr Chris and Simon Harris, *"The Impact of Diverse National Values on Strategic Investment Decisions in the context of Globalization,"* 4 IJCCM 77 (2004).
[39] Ibid.

smart phones but includes security cameras, systems of all conditioning etc. These are, therefore, expanding the chances for systems to be distorted or information to be disclosed.

3.) Corporations are expanding the range of data they generate, capture and maintain online.

4.) Increased 'DIY' cyber crime instruments are being proposed online for lesser prices.[40]

XII. CYBER SECURITY VIOLATION

Establishments require sufficient cyber security owing to the threats caused by malicious hackers involving international criminal gangs. Security violations can be caused by the following people-

1.) Hackers who relish the provocation of interrupting into our computer network and systems.

2.) Hacktivists who attempt to distort our associations since they do not agree with whatever it does.

3.) Criminals who attempt to steal data from you so that they can sell it afterwards, or who maybe are warning you in an endeavor to take out protection money.

4.) Unethical competitors who are organizing industrial espionage.

Cyber security contravention may also arise owing to the out of date or weak technology, insufficient methods, persons who may be fraud, uneducated or inexperienced. Cyber security violations are recurrently occasioned by the non-success of process or negligence of individuals to adhere to assented process, common reason being that they don't view it as crucial or because the said procedure makes their life more complicated in some or the other way. Security threats can be recognized and tackled by strengthening up internal business procedures.

XIII. CONCLUSION AND SUGGESTIONS

By introducing sections 66F, 70, 70A and 70B, the legislators have applied-in the most important missing links in the legislative machinery. Cyber terrorism is actuality and so is the case with cyber security. If cyber terrorism is to be defeated, one requires the latter.[41] Therefore, the absence of comprehensiveness in law needs to be resolved with utmost importance.

[40] Jeremy Swinfen Green, *Cyber Security- An Introduction for Non-Technical Managers* 9(Gower Publishing Co., 2015).
[41] Vakul Sharma, *Information Technology Law and Practice-Cyber Laws and Law Relating to E-Commerce* 243(Universal Law Publishing, 3rd ed.).

Trying to ascertain and interpret terrorist activities in cyber space is essential, so that one can foresee and expectantly circumvents the attacks. The United States and various other developed countries depend deliberately on critical infrastructure in the configuration of computer networks as well as systems, depending on computer networks. The impersonality and strain in detecting cyber space operators, nonetheless needs that counterterrorism attempts be compulsorily intelligence-intensive, not only in physical space but also in cyberspace as well. Terrorists and fellow companions are uncovering themselves in a cyberspace shared as well as retrieved by defenders when employing cyberspace as an assisting instrument.

Counterterrorism must comprehend to take mastery of this vulnerability, and to do so without making too many compromises in the path of civil liberties or rights of person who is not an offender. Maybe, the endeavors that have attained the most clarity in this respect have been administered against terrorist financing. Three sectors that require the most instant concentration to deal with prospective high-influenced terrorism are as follows-

- *Technology for Efficaciously Gathering, Evaluating and Acting on Intelligence-* Approaches under this direction such as the utilization of data mining techniques or soliciting to advance technologies to enable correct trace-back and recognition have run into various difficulties like policy, technical and legal issues. The lately shut down Total Information Awareness project is probably the most remarkable case in point. Practically, it is very hard to trawl through the huge areas of cyberspace to attain actionable intelligence without a large number of false positives and without the dangers of settling the civil rights of law-obeying persons.

The action of this suggestion is also plagued with difficulties of jurisdiction that are massively compounded by the uncomplicated transnational access proposed by various constituents of cyberspace, most primarily the Internet.[42] What may be observed as serious in one nation whose cyber infrastructure may be employed as part of a terrorist activity may not even make the legislative radar screen of others which are part of an offence that crosses number of physical jurisdictions.

Most nations have devoted very little consideration to clearly making genuine crimes of the activities mentioned above, for example-employing cyberspace to directly attack or vaguely support attacks. Striving broadly adopted national legislations criminalizing actions which directly attack cyberspace or utilize cyberspace as a channel to attack other aims is an

[42] S.E Goodman, *Cyber Security: Turning National Solutions into International Cooperation* 65(CSIS Press, 2003).

essential goal. Having such legal provisions in the textbooks may also make lawful the issue of serious cyber attacks in a manner that aids in attaining development under the second as well as third suggestion also.

- *More secure Digital Control Systems for Handling Critical Physical and Telecommunications Infrastructure*- These systems need to be of a specific concern regarding terrorism, since there are specifically difficult issues linked with enhancing the security for such systems. These systems are mostly small, independent, and with forced power requirements. Security may not accurately fit with the space, real time or with power needs. Security precautions could also lessen performance or be troublesome with relation to the synchronization of the more immense activities.

Almost all of these control systems are either in private or mixed sectors, such as airports. These users may also fall short of the resorts to protect these systems in an efficient manner.[43] Though, the operators of such systems are small, but are very crucial, part of cyberspace users in our reference. Under this suggestion, potential risks in this sector are really of a great distress and must be given national precedence by those governments with suitable authority. Giving preference to protection would involve imparting several forms of help and technology to various private owners as well as users of digital control and management systems. Special attention should be rendered to transportation systems, since they have been favored in large numbers by the terrorists as prey and a source of delivery for decades.

- *Upgrading the Capabilities and Security of the Information Technologies for Emergency Responders*- Emergency Response is tortured by grave disintegration of communication between various players at national as well as local levels. Among other difficulties, this insubstantiality makes for information and control issues during emergency, difficulty where the resources of various jurisdictions are required to be conveyed to bear efficiently without any further delays.

Also, there are difficulties linked with sustaining and efficiently employing and operating databases with critical information which could be speedily and constructively brought to bear at the point of a disastrous attack. From a technological viewpoint, these difficulties are not hard to address. Infact, political as well as financial barriers are the core retardants to making advancement in the U.S. and other nations.[44]

Cyber attacks can be posed in multiple forms, therefore it becomes necessary for us to know

[43] Suresh T. Vishwanthan, *The Indian Cyber Laws* 101(Bharat Law House, 2018).
[44] Dr. Amita Verma, *Cyber Crimes in India* 237(Central Law Publications,2012).

the actual motive behind such threats so that we can reduce the upcoming risks at least to a cetain extent. This threat also needs to be taken more seriously in order to curtail the threat to the maximum magnitude.

Our attempts to prevent cyber threats is very far from satisfactory. There is a crucial obligation to spread recognition across the intelligence communities by the means of seminars and workshops. The cyber crime departments in India started with the aim of inspecting and monitoring crime related with spams etc.[45] But the situation today has got even more complex, with cases accounted being more complicated and the rate of conviction is still miserable.

With the expanding dependability upon the technology, it becomes equally important to safeguard it and ourselves in order to prevent them from massive deterioration, which is mainly taking place in the forms of cyber crimes. Taking the required precautions will not only make our lives trouble free but will increase the reliability of data and information also. Thus, one right action could serve as a solution for multiple problems, thereby making cyber space more dependable.

*****

[45]J.P. Sharma and Sunaina Konojia, *E-Business and Cyber Laws* 1(Bharat Law House, 2018).