Indian Government Initiative to Counter Cyber Terrorism

Sugandha Chaudhary, Department of Law,
Galgotias University, Yamuna Expressway
Greater Noida, Uttar Pradesh
Email ID: sugandha.rmlnlu@gmail.com

ABSTRACT: Over and over again, the Government of India has demonstrated that it is not at peace with the current cyberspace attacks and has continuously dealt with the consequent shock and fear among the general population and the danger to national security. Nevertheless, the proper time, method, result and feasibility of any government intervention remains a major concern and calls for protective steps on the part of people, businesses and companies. One of the most important characteristics of a professional legal system is that it can keep pace with developments in culture. The aim of the Promulgation of the Information Technology Act, 2000 was to cater to those developments that changed the environment as a whole. Yet, because of its clauses aimed at holstering e-commerce, this act proved to be deficient, though cyber criminals were not given much consideration. The act barely had 10 pages concerned with cyber crime. The lawmakers did not comprehend the unbridled pace at which this legislation could be outstripped by technology. It is really important to learn law from now on.

Keywords: Government, Law, Information, Technology, Section, Crime, Guidelines.

INTRODUCTION

By 2008, when "The Information Technology Amendment Bill 2008" was passed the world had radically changed and the line between genuine world and the virtual world was obscuring. By at that point, cyber – psychological oppression had just reappeared in the country. Acquainting arrangement related with this threat was without a doubt a need of great importance. In fact, this change was an automatic response to the 26/11 dread assaults that shook the entire country in 2008. The fundamental focal point of this Act was on the perspectives identified with cyber-crime and cyber-psychological warfare. Section 66F was presented through this revision which discusses Cyber Terrorism and discipline for the equivalent. This section remembers all such acts for cyber-psychological oppression, which are danger to the solidarity, trustworthiness, power and security of the country or strike fear in brains of individuals through upsetting the approved admittance to a PC asset or gaining admittance to a PC asset through unapproved means or making harm PC organization [1].

In the event that these acts cause wounds to people, cause demise of any individual, harm or destruct any property, causes disturbance of fundamental supplies or benefits, or contrarily influence the basic information structure, they become culpable in nature. The discipline for this offense is from three years up to detainment for life relying on the gravity of the act. Nonetheless, while this section endeavors to characterize cyber-psychological oppression, it is practically incomprehensible for one section to incorporate all acts that may add up to cyber-illegal intimidation. The world has not gone to an agreement with respect to the meaning of illegal intimidation itself. At the point when we come to 26/11 assaults, the fear mongers just utilized correspondence administrations to give a helper to the psychological oppressors who had attacked the Taj Hotel. This correspondence helper doesn't come surprisingly close to this section [2].

Even however Section 66F doesn't discuss communicational angle, Section 69 discussions about giving bearings with respect to capture attempt, decoding or observing of information utilizing a PC asset. Section 69A discussions about hindering community to any information, though Section 69B considers checking and gathering traffic information for Cyber Security. Henceforth, the act has thought about communicational viewpoint, despite the fact that it has neglected to do so with regards to Section 66F. The test here is to incorporate the part of correspondence associate to the spread of fear in this Section with the goal that this turns into a viable apparatus for fighting cyber-psychological oppression [3].

DISCUSSION

India came up short on a legitimate Cyber Security Policy before 2013, and this the norm would have stayed intact for some time had it not been for Edward Snowden, the informant who released National Security Agency's reports. This release uncovered before the world the weaknesses that the cyber space was defenseless to. Branch of Information Technology (DIT) delivered the National Cyber Security Policy in 2013, defining significant standards and covering plenty of activities from limit working to a legitimate structure for crisis reaction. Yet, this strategy has confronted a ton of fire for not being at standard with the strategies of cyber develop countries. Above all else, India actually doesn't have a satisfactory public security principle and even the technique that is being practiced is insufficient. An administrative lacuna that this arrangement faces is that it didn't experience public assessment being only a strategy, and cyber organizations overlook it on the guise of this approach being neither restricting nor enforceable. Besides, with approach of new advancements like distributed computing and consistently expanding client base for PDAs, the move of reprobates has moved towards these mediums while the arrangement doesn't mull over these. As of late, holding fast to the cyber security strategy, administration of India has attempted different activities to counter cyber-psychological warfare and different associations have been framed to deal with India's cyber local area [4].

Public Informatics Center is liable for e-administration and helps Central Government bodies, State Government bodies, District level and other government bodies. It gives decentralized taxpayer driven organizations, correspondence network all through the country and other information technology administrations. Under the Department of Information Technology (DIT), there is a Computer Emergency Response Team (Cert-in), shaped in 2004, which helps the law upholding organizations in their battle endeavors. This group attempts to keep up the security of the cyber space through, as determined in its order, "upgrading the security correspondences and information framework, through proactive action and successful cooperation focused on security occurrence counteraction and reaction and security affirmation" [5].

In 2011, National Critical Information Infrastructure Protection Center (NCIIPC) was made as a development to Cert-in to turn away emergency with regards to basic Infrastructure, for example, guard, energy, space, telecom, banking, etc. Public Technical Research Organization is likewise answerable for keeping up the basic framework of the country. Yet, specialists accept that these associations have not actually been fruitful in keeping up their destinations.

BATTLING CYBER TERRORISM AT INTERNATIONAL LEVEL

At worldwide level, the hazards of cyber-psychological warfare have been recognized and potential measures are by and large gravely considered. Joined Nations is the greatest stage at the worldwide level which has offered significance to a need to brace the world against cyber-psychological warfare. The significant goal of the United Nation is to keep up the harmony of harmony and security. For the most part the UN works through legitimate instruments like shows or other lawful structure for the concealment of psychological warfare acts. UN as of now follows different goals to battle illegal intimidation and has additionally settled a Counter Terrorism Committee [6].

A couple of significant goals with regards to cyberspace are – Resolution 56/121 (2001) which is on "Battling the Misuse of Information Technology" and Resolution A/RES/2321 adjusted by UN General Assembly which centers around cyber illegal intimidation, public mindfulness and notices standard penalizations if there should arise an occurrence of various sorts of assaults. General Assembly additionally adjusted another goal in 2010 on "production of a worldwide culture of cyber security and assessing public endeavors to ensure basic information foundations". These goals direct the part states to build up their legitimate system and strategies remembering the work done by Commission on Crime Prevention and Criminal Justice, and furthermore the global and local associations which are working for controlling cybercrimes. These goals likewise advocate the requirement for multilateral collaboration among the part states and urge them to receive measures to battle and restrict the possible dangers. UN is assuming a crucial job in battling against cyber psychological warfare by advancing sound and facilitated procedures. Howsoever, it is likewise evident that the UN must be dynamic and subsequently requires applied transformation and underlying changes to meet the changing elements of cyber psychological warfare [7].

The Council of Europe made a Convention on Cyber Crime through its "Panel of Experts on Cyber Crime". It has even non-European states as its part. Its principle center is around controlling cybercrimes at a global level. This show partitioned criminal offenses into four classes – "offenses against classification, respectability, and accessibility; PC related offenses; content-related offenses; and offenses against encroachments and related rights." It endeavors to set up a typical criminal approach at a worldwide level to check cyber-crime and cyber illegal intimidation through worldwide co-activity and overseeing PC network through globalized action. It likewise attempts to manage issues, for example, revealing traffic information, blocking the substance, search and capture of PC information, etc. It likewise takes into account a trans-line admittance to the part states to put away PC information and setting up an organization for quick help between signatory countries. This show doesn't straightforwardly address the issue of cyber psychological warfare, in spite of the fact that Article 14(2) sub clause (b) and (c) of the show incorporate criminal offenses carried out through the methods for PC and assortment of confirmations in electronic structure, subsequently, can encourage intending to the issue of cyber-illegal intimidation. However, this show has not yet had the option to fit cybercrime laws of signatory states; rather, it is only a likely apparatus for making authority in cyberspace against cybercrimes. Numerous significant countries have not yet marked the show, India being one of such countries [8].

The primary worry of such countries is that the Convention may abuse the sway of the countries and furthermore that the Convention's protected innovation related crime arrangements are not viable with their creating markets. India has raised worry that since it has not been remembered for arrangements with respect to this show, its needs are not reflected in this show There are different stages likewise like Europol which oversees "Check the Web", where the police authorities of the part nations share information on psychological militant associations and fear based oppressors. Germany has additionally settled "Joint Internet Center", which acclimatizes information on dubious activities in cyberspace. "Checking Assessment and Partners" (MAP) was dispatched in 2009 by Interpol to screen activities on dubious sites, uncover important information and disperse it to the police powers of countries everywhere on the globe [9].

PREPARING FOR FUTURE: SUGGESTIONS

Web being an expansive medium, offers the fear mongers a chance to target distant zones while sitting at one spot. These cyber assaults are not generally contained to the virtual world, however can cause destruction in reality too. In future, as the basic framework and administration become increasingly more technology dependent, cyber psychological oppression may even outperform the dangers of illegal intimidation. Psychological oppressors would have the option to close down the entire working of a nation by focusing on the innovations which are running that country. Cyber illegal intimidation, being a worldwide danger, can be supposed to be a global crime. Accordingly, it requires a worldwide reaction. All inclusive purview can be applied to the acts of cyber-psychological oppression through global local area and states. Deal systems and standard global law can help fabricate a solid arrangement of all inclusive locale. Multilateral co-activity between countries is vital to battle this insidiousness.

At present, Council of Europe Convention on Cybercrime is the solitary deal against cybercrime at the worldwide level. In any case, since this Convention has not been endorsed by numerous significant countries, there is a need to either make a few renewals to this or structure another settlement after a discourse between the countries at worldwide stage, for example, United Nations. The best recipe ever, "separation and rule", has been utilized by dread proliferating offices since days of yore. Perhaps the most ideal approaches to battle cyber-illegal intimidation would be by fitting the cyber laws everywhere on the globe through worldwide deals. This may appear to be a considerable undertaking, however inception can be made by embracing estimates like liberal sharing of information on fear mongers and assaults, sharing new advances, reacting rapidly to reciprocal demands and references made by Interpol and other global knowledge organizations, directing cross country preparing trade programs [10].

On the homegrown level, a public cyber security regulation should be created and the meaning of cyber psychological oppression in Information Technology Act, 2000 should be extended to cover cyber correspondence which helps the fear mongers in making progress in their dread inciting missions. Definition of a National Security Policy by the Cabinet Council on Security which ought to be appropriately embraced by the Prime Minister Office can assist with making an enforceable enactment in this field. Cyber Security Policy can be made a subset of this arrangement. Notwithstanding this approach, a public cyber security tenet and Cyber Security procedure by individual services can help build up a level based "arrangement precept methodology" system which would guarantee a superior security of the entire country with regards to cyber-psychological oppression. Additionally, a zenith body should be made to investigate the cyber security instrument of the country. It ought to have the ability to investigate for strategy plan, spending distribution and usage of the cyber safety efforts everywhere on the country. Cert-in doesn't have any authorization powers, in this way, it ought to be moved under Ministry of Home Affairs from Ministry of Communication and Information Technology. It would prompt a straightforward line of detailing and Cert-in will have the responsibility over implementation and weakness appraisal.

The framework managers and the public authority need to remain exceptionally alert for any notice they get for cyber assaults anytime of time. Efficient and routine danger appraisal of basic information frameworks ought to be consistently led and given need for appropriate danger the executives. A legitimate cyber fighting and encryption strategy should be created. E-administration administrations are should have been given more cyber security. A cyber security organization can be made which acts as an extension between government offices and common offices to improve the country's strength against genuine electronic assaults, and upgrade the security. Keeping up the frameworks ought to be given most extreme significance by continuing to work framework, programming and hostile to infection programs exceptional; "securing" the framework; impairing every pointless assistance and upholding solid secret phrase ensured frameworks. Active safeguard measures ought to likewise be received, for example, finding the wellspring of assaults and forcing genuine danger and punishment, and counter assaults. With each assault, its eventual outcomes ought to be considered and legitimate measures ought to be taken to guarantee such assaults don't represent any danger in future. Faulty elements ought to be taken out, a harm evaluation ought to be done, the intact buildup ought to be apportioned and redistributed, reconstitution of capacities ought to be done according to their significance and pre-assault status ought to be reached without destroying evidences. Government associations just as different associations ought to make and uphold client strategies which cover genuine utilization, security issues and advance carefulness. The client approaches ought to be known to all workers and carefully clung to. The workers of such associations ought to be given appropriate preparing with respect to cyber security and an overall mindfulness among the mass likewise should be created.

Since technology is a steadily evolving substance, the approaches and methodologies should be broke down and refreshed at ordinary spans. Correspondence between different associations ought to likewise be smooth so appropriate admonitions can be given when it truly matters. A cautioning about their weaknesses can assist them with setting up solid preventive measures. The principle weapon of cyber fear based oppressors is their clothing of secrecy, cyber bistros and other public assistance stages which give web office give a stage to keep up this attire. Thus, it is important to follow security techniques like personality check of clients, keeping up appropriate records to keep aware of cyber psychological oppression. One significant block in fortifying the cyber security in India is the carelessness that is appeared to it with regards to subsidizing. While the web organizations everywhere on the world spend a normal of 5% of its assets on cyber security, Indian web organizations spend under 1% of their assets on security. Satisfactory subsidizing ought to be given in the field of cyber security and private area ought to likewise contribute in such financing. Also, India should attempt to make its laws and arrangements correlative to the global offices and shows, developing solid multilateral associations with the countries everywhere on the world so that there is a worldwide collaboration in critical conditions. A thorough examination ought to be finished by the public authority of its interests and all the partner bunches require to partake in this investigation and afterward structure international strategy destinations with respect to this issue. Media, being the disseminator of information all through the world, necessities to connect with people in general in a discussion and make them mindful in regards to such dangers.

Academicians and researchers can likewise help in this issue by giving their mastery on specialized, mental and moral issues engaged with this type of psychological oppression. Web Literacy should be expanded and advanced at singular level so that individuals can keep up cyber security at singular level. In addition, there is a desperate requirement for individuals to keep up great between close to home relationship to guarantee that individuals from family or companions don't get vulnerable to the impact of dread proliferating associations, for example, ISIS. Youthful personalities are generally susceptible and henceforth parental control and parental direction at legitimate time can save them from falling prey to the acts of conditioning by the psychological oppressor associations.

CONCLUSION

Cyber terrorism is better understood as instigating terror through the medium of cyberspace in general terms. Given the continuous series of events that have alarmed nations around the world, it can be fairly concluded that cyber terrorism, cyber warfare and cyber crimes are a serious concern, regardless of the futile categorization, and are constantly growing with the advancement of science and technology. As the cyber world reaches a level of ubiquity and transgresses itself throughout the world, it accumulates the potential to become a deadly terror propagation medium.

REFERENCES

[1] N. Kshetri, “Diffusion and effects of cyber-crime in developing economies,” *Third World Q.*, 2010, doi: 10.1080/01436597.2010.518752.

[2] H. S. Lallie *et al.*, “Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the paandemic,” *arXiv*. 2020.

[3] A. Bendovschi, “Cyber-Attacks – Trends, Patterns and Security Countermeasures,” *Procedia Econ. Financ.*, 2015, doi: 10.1016/s2212-5671(15)01077-1.

[4] R. Broadhurst, “Developments in the global law enforcement of cyber-crime,” *Policing*, 2006, doi: 10.1108/13639510610684674.

[5] K. Dashora and P. P. Patel, “Cyber Crime in the Society: Problems and Preventions,” *J. Altern. Perspect. Soc. Sci.*, 2011.

[6] M. McGuire and S. Dowling, *Cyber crime: A review of the evidence*. 2013.

[7] A. Guinchard, “Between Hype and Understatement: Reassessing Cyber Risks as a Security Strategy,” *J. Strateg. Secur.*, 2011, doi: 10.5038/1944-0472.4.2.5.

[8] P. M. Tehrani, N. Abdul Manap, and H. Taji, “Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime,” *Comput. Law Secur. Rev.*, 2013, doi: 10.1016/j.clsr.2013.03.011.

[9] B. Akhgar, A. Staniforth, and F. Bosco, *Cyber Crime and Cyber Terrorism Investigator’s Handbook*. 2014.

[10] C. Wilson, “Cyber crime,” in *Cyberpower and National Security*, 2011.