ISSN 2063-5346

CYBER-TERRORISM: A GROWING MENACE TO CYBER SECURITY

Dr. G.Mallikarjun[1], B MD Irfan[2]

[1]Asst. Professor of Law, NALSAR University of Law, Hyderabad.

[2]System Analyst, NALSAR University of Law, Hyderabad.

Article History: Received: 12.05.2023 **Revised:** 25.05.2023 **Accepted:** 05.06.2023

Abstract

Cyberattacks, which pose a threat to modern states, organizations, and international relations, are the focus of this article. By comprehending its concepts and meaning, the first section of the article aims to explain cyber-attacks which are said to be cyber terrorist attacks, among other cyber-attacks. It also examines the various efforts that the Indian government has made to combat cyber terrorism on a national and international scale. The author will also find out the methos and tools which are generally used cyber terrorists. It tried to figure out options for how cyber terrorism could be tackled in the future. The author also discusses the efforts made by the Indian government to combat cyber terrorism on a national and international scale with the evaluation. The author also discusses the efforts made by the Indian government to combat cyber terrorism on a national and international scale with the evaluation. It tried to come up with strategies for dealing with cyber terrorism in the future. Along with the evaluation, the author also discusses the Indian government's efforts to combat cyber terrorism on a national and international scale. It will concentrate on the evolution of India's cybersecurity policy over time. How India is effectively assisting the international organizations in the fight against cyberterrorism on a global scale, as well as in the national level to combat cyber terrorism. In conclusion, the researcher will advocate for international cooperation to combat cyber terrorism collectively

Introduction:

Cyberspace is a necessary component of the modern world. The current increase of internet users is due to the ease of accessibility of smartphones and low-cost data plans. The expansion of cyberspace in India was aided by DIGITAL INDIA program and other initiatives by the Central Government. Currently, the development of cyberspace is being used by terrorists to disrupt the peaceful coexistence of nation states. Cyberterrorism has the potential to completely devastate a nation's political and economic structure. India and other developing nations are heavily affected by the actions of such cyberterrorists. The harm it poses is not well understood by the general public though. The inability to control the situation is a problem for the democratically elected administrations. Malicious software programs infected our computers, vital data stored on computer servers were stolen, confidential data were altered or fabricated, and government websites, including the Ministry of External Affairs, the Income Tax Department, the Employment Office, important temple websites, and the Defence Department (the R&D), were hacked by cybercriminals. Almost all countries are investing more and more because of the threat it poses to national security.

A new form of terrorism called as "cyber-terrorism" has emerged in the technologically advanced digital world along with the rise of the traditional form of terrorism.[1] Cyberterrorism, a kind of cybercrime, has engulfed the world with its all-pervasive presence and accessibility. With the unbounded capacity of technology and the reach of the internet, cyber terrorism has developed into a dangerous area of the law that requires immediate protection in all judicial systems. It is more important than ever to pass legislation that addresses the grave crimes of cyber terrorism since there are already obstacles to legal problems involving cyber crimes, such as jurisdiction, investigation and gathering evidence. The purpose of this study is to define the characteristics, risks, and effects of cyberterrorism. Further, it aims to establish the features, dangers, and consequences of cyberterrorism. Following which, the paper seeks to look into international and Indian Laws that govern over the complex sphere of cyberterrorism.

CYBER TERRORISM

In the late 1980s, Banny C. Collin of the Institute for Security and Intelligence (ISI) first used the phrase "cyberterrorism." The term "cyber-terrorism" is debatable and still lacks a definition. Cyberterrorism is a term used to describe the creation of new innovation and technology, as well as the expanding reliance of mankind on the cyber based media and cyber technologies. "Despite the fact that cyber terrorism has been recognized as a significant hazard, there doesn't seem to be an all-inclusive meaning." Cyber-terrorism is defined by Denning as the assembly of cyberspace and terrorism where assaults on computers, systems, and the data put away in that are completed to threaten or force a legislature or its near pupils in promotion of political or social activity/destinations, and should bring about savagery against people or property, or if nothing else cause enough mischief to create dread."[2] It is critical that universal efforts are made to re-survey the extension and advancement of components behind cyber terrorism to ensure that enactments do not make escape clauses for cyber threat/hazard-based oppressors.[3]

The Internet-connected computer networks are severely disrupted under a cyberterrorism strike which are called denial of service attacks or distributed denial of service attacks. This is done with the aid of several tools, including phishing, malicious software, hardware techniques, programming scripts, computer viruses, and computer worms. To achieve political or ideological goals by intimidation or threatening behaviour, it can also be regarded as the use of the Internet to carry out violent acts that cause or threaten serious physical harm or the loss of life.[4]

It is not out of place to mention that the internet has been utilized as a medium for arranging fear based oppressor assaults, for enrollment of sympathizers, or as another field for assaults in quest for the fear monger's political and social targets.[5] Fear based oppressors have been known to have utilized the internet for correspondence, charge and control, publicity, enrollment, preparing, and financing purposes.[6] From that viewpoint, the test of non-state on-screen characters

[1] Benson, B.L., 2005. The spontaneous evolution of cyber law: Norms, property rights, contracting, dispute resolution and enforcement without the state. *JL Econ. & Poly, 1,* p.269.

[2] Dorothy E. Denning. " Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for InfluencingForeign Policy" http://www.nautilus.org/info-policy/workshop/papers/denning.html.

[3] Jus Dicere **,** Cyber Terrorism: Psychological Aspect, https://www.jusdicere.in.

[4] Anuraag Singh , Cyber Terrorism, the Real Threat to India's Security, https://www.deccanherald.com

[5] Nelson, B., Choi, R., Iacobucci, M., Mitchell, M. and Gagnon, G., 1999. *Cyberterror: Prospects and implications*. NAVAL POSTGRADUATE SCHOOL MONTEREY CA.

[6] Ibid.

to national security is to a great degree grave.[7] The government has taken various measures to counter the utilization of the internet for psychological militant related exercises, particularly in the repercussions of the fear based oppressor assault in Mumbai in November 2008.[8]

Parliament amended the IT Act, wherein the attention has been laid to check on digital wrongdoings by introducing Section 66F into the Information Technology (Amendment) Act of 2008 Act, which makes an act of committing cyberterrorism a serious offence. Adding this clause into the law was a necessary precaution to protect civil rights with the help of rules and guidelines in the name of Data Technology (Guidelines for Cyber Cafe) Rules, 2011 under the umbrella of the IT Act. While digital activism can't exactly be set in a similar class, a large portion of its attributes puts it unequivocally in the domain of digital psychological oppression both as far as techniques and end objectives.[9]

Tools of Cyber Terrorism:

The fundamental objective of cyberterrorist actions is to harm networks and disrupt them. This activity might temporarily divert the attention of security agencies, which would give the terrorists more time and make their job a little easier. Computer tampering, virus attacks, hacking, and other techniques may all be part of this process, these are:

Hacking: The most popular technique used by the terrorist to enter into the system or networks. It is a usual term used for any sort of unauthorized access or entry to system or a network of computers and it will destroy the complete data[10]. Hackers write or use ready-made computer programs to attack the target computer to destroy or otherwise to steal the security information and other confidential information. Which include sniffing, tempest attack, password cracking and buffer outflow allows hacking.

Trojan Attacks: A Trojan is an unauthorized programme which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing. In other words, it is a programme that pretends to produce desired output while virtually they are intended for doing something different[11]**.**

Computer Viruses: It is a programme, which infects other programmes via editing them. They spread very fast. After a virus infects a system, it attaches itself to other software, so that its activity is stimulated as soon as the host programme is executed. It has the ability to replicate and infect other programmes and files. Computer viruses are harmful, intended to inflict to perform malicious activities to destruct the sensitive Data.

Computer Worms: A set of programmes that can unfold purposeful copies of itself or its segments to other PC structures commonly by way of network connections.

Crime through E-Mails: Usually worms and viruses ought to connect themselves to a host programme to be injected. Certain emails are used as hosts by using viruses and worms. E-mails are additionally used for spreading falsehood, threats, and defamatory stuff.

Spear-Phishing: These attacks are similar as the' Phishing', which usually involve

[7] Furnell, S.M. and Warren, M.J., 1999. Computer hacking and cyber terrorism: The real threats in the new millennium?. Computers & Security, 18(1), pp.28-34.

[8] Clark, A.M., 2006. *Cyber terrorism: political and economic implications*. Igi Global.

[9] Ibid.

[10] It is a kind of access without the permission of either of the rightful or person in charge of the computer, computer system or computer network (section 66 of IT Act 2000).

[11] See http://www.cidap.gov.in/documents/cyber%20Crime.pdf

sending a deceptive email to a specific person or organization in order to steal data or private information for malicious purposes. Even cyber criminals may, sometime, may also intended to install malware to send the same to the targeted person or organization.

Denial of Service: These attacks are aimed at denying authorized individual access to a computer or PC network with an intension to exploit security vulnerabilities in network software. These attacks have become common as they are easier to create and have a more disruptive capability.

Cryptology. Terrorists have commenced the usage of encryption, high frequency encrypted voice/data links etc. It would be a Herculean task to decrypt the information which the terrorists are sending through the use of a 512-bit symmetric encryption.

Challenges and concerns:

Some of the challenges and concerns are outlined below:[12]

a. Lack of digital security awareness and lifestyle in individuals also at the institutional level;
b. Lack of trained and qualified personnel to implement countermeasures;
c. Too many Data Security Associations have proven to be fragile because of the "scramble for the field" or the impulses related to money;
d. No strategy for email accounts, especially for surveillance team like police and personnel the office;
e. Cyber-attacks have come from fear mongers as well as from neighbouring countries adverse to our national advantages.[13]

Significant cyberterrorism attempts and attacks: At Global and the National Level:

Cyber terrorism is a type of terrorism where governments and nonstate actors use computers to attack other organizations. These attacks can include stealing data, extortion, and other methods. Cyberattacks are often conducted through methods such as email, chat, and social media. There are many different ways and purposes that attacks on computer networks, data stores, communication systems, command-and-control systems, or other systems can be carried out. The majority of cyberattacks and attempts to breach computer networks go unnoticed, despite the fact that many cyberterrorism attacks are widely reported.

Cyber Terror Incidents at Global Level:

Attack on Healthcare Providers: On 21st March, 2022, Shields Health Care Group (Shields), a medical services company headquartered out of Massachusetts, experienced a data breach that exposed the personal information of about two million patients[14]. Because Shields is dependent on relationships with medical facilities, the ripple effects of this might be felt far and wide. Up to fifty-three different hospitals and the patients they serve may be impacted.

In 15th August 2022, due to the ransomware advanced attack, a managed service provider (MSP) for the UK National Health Service (NHS), the NHS's emergency services across the UK were severely disrupted[15]. At the same time, another American MSP named

[12] Veerasamy, 4th International Conference on Information Warfare and Security March 26-27, Special issue of the International Journal of Pure and Applied Mathematics, 2009, p. 1625.

[13] R.K. Suri and T.N. Chhabra, Cyber Crime, Pentagon Press, New Delhi, India, 2003.

[14] Shields Health Care Group data breach affects 2 million patients (bleepingcomputer.com)

[15] See Advanced Ransomware Advanced Attack: Advanced Ransomware Cyberattack: Cloud MSP Recovery Updates - MSSP Alert by Joe Panettieri.

NetStandard was targeted, resulting in the suspension of its 'MyAppsAnywhere' cloud services. Since MSPs have access to the data of several firms, they present ransomware groups with an enticing bounty.

Attack on Marriott Data Breach: Marriott is one of the world's leading hospitality service providers. Nearly 340 million guests' information were compromised when Marriott was hacked in 2014. After the breach was discovered in September of 2018, the UK Information Commissioner's Office issued a fine of £14.4 million. Again, in January of 2020, Marriott was hacked, this time exposing the personal information of 5.2 million customers. More than 20GB of data, including guests' credit card numbers, was allegedly stolen by hackers in June of 2022[16]. Social engineering was used to get access to a computer at a Maryland Marriott hotel, according to the attackers. Even though the company will be contacting customers, Marriott insists that just about 300 to 400 people were affected.

Russia-Ukraine Conflict: The Russia-Ukraine crisis, which began in February 2022, comprised not just physical combat that displaced thousands and killed many—but cyberattacks as well. FortiGuard Labs has established that fresh viper malware was used to attack Ukrainian targets and identified it installed on at least several hundred PCs in Ukraine. It has come to light that several Ukrainian businesses have been the victims of sophisticated attacks using malware families like KillDisk and HermeticWiper[17], which are designed to wipe data from infected computers. In addition, malicious "Evacuation Plan" emails in Ukraine were found to have spread the Remote Manipulator System (RMS), a technology that allows users to remotely control devices. Ukraine also suffered a wave of distributed denial-of-service (DDoS) assaults. This included an attack on the State Savings Bank, which hampered banking services and cash withdrawals from ATMs, as well as disrupted the Ministry of Defence and Armed Forces networks[18].

Attack on Uber: It was discovered in September that a teenager had completely infiltrated Uber's internal systems. It appears that the intruder utilised a technique known as an MFA (Multi-Factor Authentication) Fatigue attack, in which, after obtaining a user's credentials and if the organisation uses MFA, the attacker repeatedly prompts the user to authenticate using their mobile device[19]. The worker initially rejects the intruder since they did not authenticate, but the attacker finally contacted the worker over WhatsApp, claiming to be from Uber IT, and telling them to approve the authentication request or else they would keep coming. The worker finally gave in after being harassed so frequently. An additional gadget allowed the attacker to compromise the MFA. Following this, the intruder connected to the company's VPN and started poking around. Fortunately for Uber, it appears that the hacker just did it out of curiosity and not for financial gain or some other more malicious purpose.

Attack on SolarWinds: According to Business Insider, SolarWinds, a technology company, was the target of a cyberattack that went unnoticed for several months. Private businesses like FireEye and numerous government agencies were able to be spied on by hackers who are

[16] See Hackers steal 20GB of data from Marriott hotel, and attempt to extort money from the hotel chain, https://www.timesnownews.com/technology-science/hackers-steal-20gb-of-data-from-marriott-hotel

[17] See What Is Cyber Warfare? https://www.fortinet.com/resources/cyberglossary/cyber-warfare

[18] Ibid

[19] Ryan Browne, Uber investigates 'cybersecurity incident' after reports of a hack on the company, https://www.cnbc.com/2022/09/16/uber-investigates-cybersecurity-incident

widely believed to be based in Russia[20]. As a direct result of the attack, the government of the United States imposed sanctions on Russia in April 2021[21]

Attack on CNA Financial: According to Bloomberg, insurance company CNA Financial paid hackers $40 million in March 2021[22]. following a ransomware attack that locked the company's computer networks and stole data. The company claims that the majority of policyholder data was not compromised by the attack.

These scenarios provide an illustration of the threats that cyber terrorism poses to organizations and governments all over the world. According to McAfee, a computer security company, cyber terrorism and other cyberattacks cost governments, businesses, and individuals more than $1trillion annually. Network safety Adventures figures that the expense of digital wrongdoing, everything being equal, will reach $10.5 trillion yearly by 2025[23].

Cyber Terror Incidents in India:

According to US-based cyber security company Norton, during the first three months of 2022, India experienced over 18 million cyberattacks and threats, with an average of approximately 200,000 threats every day.[24]

According to a recent SonicWall report, ransomware attacks increased by 105% over the previous year in 2021, while encrypted threats increased by 167%. While ransomware was popular in the report, there were also significant concerns about phishing and business email compromise (BEC) attacks, both of which saw significant increases.

Microsoft Exchange Attack - Hackers gained access to the accounts of at least 30,000 organisations in the United States alone, with 250,000 affected globally. In March 2021, Microsoft announced that nearly all servers affected by the attack had been patched and mitigated. However, it was still expensive and time-consuming to fix, and it caused significant damage to companies that had suffered subsequent breaches and attacks as a result.

Just pay Leak - According to independent security researcher Rajshekhar Rajaharia, the homegrown payment processing platform Juspay allegedly compromised the data of over 100 million customers. He claimed that an attacker had made two sets of data available on the Dark Web. One had 100 million customers' email addresses and phone numbers, while the other had 46 million card transaction details. In its defense, Juspay stated that a data breach occurred in August 2020, but that it only affected an isolated storage system that contained no sensitive information.

Air India Customer Data Leak- In May 2021, India's national airline Air India announced that its data servers had been targeted by a cyberattack, and that sensitive data from 4.5 million customers around the world had been compromised. Passport information, ticket information, and credit card credentials registered between August 26, 2011 and February 20, 2021 were among the leaked data. The targeted servers that carried Air India customer data were managed by SITA, a Swiss-based technology company founded by 11 Star Alliance airline companies.

.

[20] The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal | Business Insider India

[21] FireEye hacked! Company attacked by foreign government hackers | Apps (republicworld.com).

[22] Bloomberg News, CNA Financial Paid Hackers $40 Million in Ransom After March Cyberattack - Bloomberg)

[23] Steve Morgan . Cybercrime To Cost The World $10.5 Trillion Annually By 2025 (https://cybersecurityventures.com)

[24] See https://www.livemint.com/technology/tech-news/india-faced-over-18-mn-cyber-threats-in-q1-2022-norton-11651657949149.html

The number of cyberterrorism-related threats that CERT-In addressed in 2020 was 11,58,208. They included malicious code, phishing, distributed denial of service attacks, website defacements, unauthorised network scanning and probing, ransomware assaults, data breaches, and vulnerable services.[25]

According to Goldman Sachs-backed company Cyfirma, the Covid-19 vaccine manufacturer in India has been hit by the Chinese cyber outfit APT 10, also known as Stone Panda. Confirm also cites connections between Stone Panda and the Chinese government. In November 2020, Microsoft discovered cyberattacks coming from North Korea and Russia. As per the version of Microsoft, these attacks targeted Covid-19 vaccination businesses in France, Canada, South Korea, India, and the USA. Similar to this, a US-based cyber outfit mentioned the Red Echo Chinese gang in February 2021. They alerted people that malware known as ShadowPad was being used by Red Echo to target India's energy industry. These are just a handful of examples; there are many more.

International Conventions to Combat Cyber Terrorism:

Cyberterrorism is a global, cross-border crime. So, a global reaction is necessary to combat cyberterrorism. According to statistics from recent years, multilateral co-operation and collaboration is the most efficient way to address the global issue of cyber terrorism. The need for such co-operation and collaboration is essential due to the fact that every country has its own rules to regulate extradition and legal aid under their domestic substantive law which governs cyber-crimes. Thus, to prevent and respond to cyber-attacks, the efforts should be on a global level so as to prevent and deter cyber terrorism. It is therefore said that the most effective form of international co-operation is to respond to cyber-attacks should be multilateral in nature.[26] In brief, treaties have to be adopted which will remove jurisdictional difficulties in the investigation of such offences and thereby, cybercriminals will be deterred from engaging in cybercrime and cyberterrorism.[27] In addition, the co-operation resulting from a treaty enhances the co-operation among signatory countries and technical co-operation beyond the boundaries of the treaty. The UN has not yet come up with a comprehensive convention to cover all acts of terrorism and cyber terrorism.

However, the Convention on cybercrime, also known as the Budapest Convention on Cybercrime, is the first international treaty seeking to address Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing co-operation among nations.[28] The primary goal of this convention is to promote international co-operation between nations. In order to prevent cybercrime and cyberterrorism, a policy with common agenda to curb the menace of cyberterrorism has been established. It also intended to address concerns about the safety of data in cyberspace. However, India and Brazil have not ratified this convention.

[25] Anuraag Singh , Cyber Terrorism, the Real Threat to India’s Security, https://www.deccanherald.com

[26] S. Suleyman, Cyber Terrorism and International Cooperation: General Overview of The Available Mechanisms to Facilitate an Overwhelming Task, in Responses to Cyber Terrorism 74e75(1st ed, Centre of Excellence Defense against Terrorism, 2008).

[27] A.D. Sofaer & S.Goodman, Past as Prologue: International Civil Aviation Agreements as Precedents for International Cooperation against Cyber Terrorism and Cyber Crime, in International Approaches to Co-operation against Cyber Crime and Cyber Terrorism (1st ed, Hoover Institution Press, 2003).

[28] Report of Council of Europe on Convention of Cyber Crime, Preamble, Convention on Cyber Crime, Budapest, 2001. Convention on Cybercrime, opened for signature Nov. 23, 2001, Eur. T.S. No. 185, available at http://conventions.coe.int/ Treaty/en/Treaties/Html/185.htm

Indian Laws to Combat Cyber-terrorism

In India, the Information Technology Act, 2000 (the IT Act) provides penalties for cyber terrorism. The Act was amended to address the threat of cyber terrorism to national security following the 26/11 Mumbai terror attacks in 2008. Accordingly, Section 66F was inserted into the IT Act, wherein it is mentioned that

> "*an act committed with intent to threaten the unity, integrity, security or sovereignty of India or to terrorize the people of India, by Denying access to persons authorized to access IT resources, attempting to hack into computer resources without authorization, or attempt to exceed authorized access or any conduct which causes or may cause death or injury to any person, or damage or destruction of property, or may cause damage to or interruption of supplies or services or infrastructure essential to community life; suspending or affecting material information under Section 70, or likely to cause damage to the interests of the sovereignty and integrity of India, to the security of the State, to friendly relations with foreign States, to public order, decency or morality, or in connection with contempt of court, defamation or incitement to a crime, or for the benefit of any foreign nation, group of individuals or otherwise, commits the crime of cyberterrorism*".

The horrific acts which are mentioned in the Section 66-F certainly undermine the security of India or strike fear in the brains of individuals or a segment of individuals; and which may bring about death and harm to individuals, harm to properties, disturbance of common administrations which are basic to the life of a group, and furthermore influences the basic data framework. The compressive definition given in section 66F is intended to ensure to check the incidents of cyber terrorism as attacks characterized by Section 70 of the IT Act, 2000.[29] The IT Act, 2000 (As amended in the year 2008) had meticulously taken endeavors to secure ensured frameworks, which is characterized by Section 70.[30] The ambit of cyber terrorism is exhaustive as per the Sections 66-F, 70, 70-A and 70-B of the Information Technology Act, 2000. According to this section. The scope of cyberterrorism is comprehensive under sections 66-F, 70, 70-A and 70-B of the Information Technology Act 2000, which allows the government to maintain cyber security in the country. It is important to note that Articles 70-A and 70-B cover both the investigation procedure and the preventive measures. The term "Critical Information Infrastructure" in Section 66F is defined in the explanation contained in the amended Section 70. This is intended to protect systems and allows the government to flag an IT resource involved in setting up a critical information infrastructure as a protected system. Article 70-A provides that the central government establishes the IIC through a nodal national agency. Section 70-B empowers the Computer Emergency Response Team India (CERT-IN) as the national focal point to gather threat intelligence and assist the central government in responding to incidents.

Cyber Terrorism India: The Strategies to Combat

India has come up with a cybersecurity policy and legal framework to protect cyberspace with its 2013 National Cybersecurity Policy. The release of NCSP 2013 is an important step forward

[29] Nappinai, N.S., 2010. Cyber Crime Law in India: Has Law Kept Pace with Engineering Trends-An Empirical Study. *J. Int'l Com. L. & Tech.*, *5*, p.22.
[30] Ibid.

to check the cyber security problems. This policy document is intended to encourage all organizations, public and private, to appoint an individual as Chief information security officer (CISO) for cybersecurity initiatives. The overall objective of the National Cyber Security Policy (NCSP) 2013 is to create a secured cyber network and strengthened regulatory framework. It has envisioned addressing and mitigating cyber threats through the National Critical Information Infrastructure Protection Center (NCIPPC). CERT-IN has been designated as the central agency to serve as the umbrella organization for the coordination and operation of industry CERTs. This policy demands for effective public-private partnerships to create a research body on the future of cybersecurity. Other vital aspects of the policy include promoting cybersecurity research and development, developing talent through education and training programs, and creating a workforce trained in security.

This policy does not address India's leadership in various cybersecurity areas such as the development of international security standards, testing of ICT products, security standards and practices of solving the internet administration problems. To address diversity at the highest level, it is recommended that the Indian government restructure its high-level institutions to create a single empowered body that would work with the co-operation of international agencies by recognizing the guidelines issued at the international level to combat the cyber security. It is a known fact that the biggest obstacle to controlling cyber threats at the international level is the lack of international harmonization. There is currently no "internationally accepted definition" of cyberwar. In addition, there are no generally accepted cybercrime contracts. Thus, a rational and extensive digital security arrangement will have to be placed with international co-operation, by which the components like describing the internet dangers, the measures to mitigate the cyber-terrorist attacks by adopting the best practices apart from the law and rules with a worldwide collaboration, which may reinforce the formation of satisfactory hierarchical structures for digital security to deal with the cyber terrorism and security.[31] However, neither the private division nor the government one has possessed the capacity to assemble data frameworks that can be depicted as sensibly strong. There has not been sufficient thinking on the ramifications of digital fighting.[32]

The worldwide group is additionally occupied with an assortment of dialogs. NATO has taken the assignment of making digital security establishments in part nations.[33] A gathering of administrative specialists (GGE), set up by the UN Secretary-General, gave a report in 2010 on “advancements in the field of ICT with regards to global security”.[34] The report noticed that there was expanding proof that states were creating ICTs as "instruments of fighting and knowledge, and for political purposes". To stand up to challenges in the internet, the GGE prescribed participation among similar assistants among states and amongst states and common society.[35]Be that as it may, just CERT-In is commanded under the IT Amendment Act, 2008, to fill in as the national organization responsible for digital security[36].

[31] Collins, A., 2016. *Contemporary security studies*. Oxford university press.

[32] Rao, N.J., 2012. Cyber Security: Issues and Challenges. *CSI Communications*, p.13.

[33] Sofaer, A., Clark, D. and Diffie, W., 2009, May. Cyber security and international agreements. In *National Research Council, Proceedings of a Workshop on Deterring Cyberattacks*.

[34] Ibid.

[35] Chen, Y.S., Chong, P.P. and Zhang, B., 2004. Cyber security management and e-government. *Electronic Government, an International Journal*, *1*(3), pp.316-327.

[36] Section 70-B empowers the Computer Emergency Response Team India (CERT-IN) https://www.cert-in.org.in/

India, now, wants to improve its cybersecurity environment in line with its goal of becoming a digital nation. A campaign called Cyber Surakshit Bharat has been launched by the Ministry of Electronics and Information Technology. The National e-Governance Division of India is collaborating on this effort. Given how quickly India's governance structure has changed due to digitalization, it is crucial to have excellent governance. With such a move, the government would raise public awareness of cybercrime and strengthen the ability of all Indian government organisations to secure their CISOs and front-line IT personnel. In addition to raising awareness, the first public-private cooperation involves a series of courses to arm government workers with tools to combat cybercrime and assist professionals.

Conclusion

The first step in countering cyber terrorism is to make sure that people, businesses, and governments are aware of the growing threat posed by cyberattacks and how to stop them. Computer security professionals are crucial in preventing and reducing the risks that cyber terrorists pose to communities, organizations, and government agencies. Cyber terrorists and other online criminals will be thwarted by user education and advanced security measures.

With each passing year, legal systems around the world try to put new policies in place to tackle cyberterrorism. But with so many imaginative ways, the cyber perpetrators may try to operate in the cyberspace to find the gaps to launch cyber-attacks. However, it can be tackled by the co-operation and the coordination of the nations by altering the processes and laws already in place to deal with new forms of cyberterrorism. Additionally, the general population needs to be made aware of the risks, their sources of distribution, and how to respond in the event of terrorist strikes. All of these steps can help develop a secure environment.

Suggestion to combat cyber terrorism:

a. Need to sensitize ordinary citizens to the dangers of cyberspace terrorism. Cert-in should involve academic institutions and positive strategy;
b. Joint effort of all government agencies, including protection agencies to attract talented and qualified teachers to use countermeasures;
c. Cybersecurity no longer has the advantage of words and links same manager will get all help. No bureaucratic force should be allowed;
d. Agreements to identify with digital security, that is, indistinguishable from other traditional ascents;
e. Increased interest in this area related to money and work;
f. Indian organizations working on digital security should also participate in keeping an eye on our neighbors for potential IT advancements.