Comparative Analysis of Cyber Terrorism Laws of India and Other Countries

Indra Kumar Singh,
Assistant Professor, GLA University, Mathura. (U.P). E-mail: indra.singh@gla.ac.in
Dr. Tarun Pratap Yadav,
Assistant Professor, GLA University, Mathura. (U.P). E-mail: tarun.pratap@gla.ac.in

Abstract--- Cyber Terrorism is a term that is seen in the news very regularly. It is a broad term and encompasses a wide variety of events and concepts. Cyber Terrorism affects the world deeply and India, particularly, has been a victim of various terror acts perpetrated by different groups.

The potential threat posed by cyberterrorism has provoked considerable alarm. Numerous security experts, politicians, and others have publicized the danger of cyberterrorists hacking into government and private computer systems and crippling the military, financial, and service sectors of advanced economies. The potential threat is, indeed, very alarming. And yet, despite all the gloomy predictions, no single instance of real cyberterrorism has been recorded. This raises the question: just how real is the threat?

This research paper have highlighted International and National initiatives governing laws related with cyber terrorism, insights into Information and Technology Act, 2000 (India) and need for administrative reforms in this field.

Keywords--- Cyber Terrorism, Cyber Law, Information and Technology Act.

I. Introduction

A new category of cybercrime that combines terrorism and internet is referred to as "cyber terrorism." As a result to the increasing reliance on the Internet, it is claimed that terrorist organizations now have a new stage to achieve their societal economical, and political motives by piling attacks or making threats against networks of the computers and other information setups. It has been definitely a challenge to understand the environment associated with that of cyber terrorism without first understanding the nature of terrestrial terrorism because the parameters of what defines terrorism are fuzzy when it comes to traditional terrorism and cyber terrorism.

II. Conceptual Analysis of Terrorism

During the French Revolution of 1789, the ruling class invented the word "terrorism" to describe the deeds of the revolutionaries. Religious, cultural, political, social, psychological, and economic aspects are only a few of the many causes of terrorism that have occurred throughout history. Since a spate of airline hijackings in the 1960s, terrorism has been a constant source of concern for the UN.

The discussion of terrorism has gained attention in international politics since the attacks of September 11, 2001, and it has now entered a new phase in which transnational activity has increased and become simpler and in which terrorist organizations can use information technology to increase the impact of their actions and the delivery of their horrific messages. There has been a huge and at a global level understanding among various countries that terrorism cannot be associated with any particular regional or cultural boundary and that it is merely single of several tools used by the ones who are looking for opportunity to lay thorns for thestates and eventually take power. This understanding has emerged in the midst of frantic UN discussions about as how to tackle with the new terror threats that are posed by Al Queda, ISIS, Boko Harm, Lashkar-e-Taiybha, and others.

Terrorism is not a usual crime it differs from other crimes in that it is committed in the name of a political, social, or religious ideology. Terrorism is never committed against a single person or a small number of people; it is always directed at a state or a cultural-religious community and results in mass damage.

Despite the fact that terrorism has a long history in both personal which means at a nations level and international affairs, there is in the current time no complete, succinct, or universally acknowledged legislative definition of the term. It's hardly surprising, then, that the international communities had been not able to agree on a simple and complete legal definition of the term "terrorism." Furthermore, certain international communities and well-known academicians have made attempts to define terrorism as follows:

Terrorism is defined by the UN Office on Drugs and Crime and Terrorism Prevention Branch as: Terrorism is a distinct type of crime that generally combines aspects of warfare, politics, and propaganda. Terrorist organizations are typically tiny for security reasons and due to a lack of popular support, making discovery and infiltration difficult. Terrorists' goals are occasionally shared by a broader constituency, but their methods are often despised.

Terrorism has been defined at the European Union level by the Constituent Assembly of the Union as: People or groups that do use or adversely affect to use violence against a nation, its organizations, its populace in broad sense, or specific individuals out of fervour, separatist desires, or other irrational or open to interpretation reasons in an effort to instil fear in the public, between official authorities, or among particular people, social groups, or the broader population.

The Department Office of the Coordinator for Terrorism by the state, USA has defined terrorism as a premeditated, politically motivated violence that is perpetrated against a non-combatant targets by sub national groups or clandestine agents, usually intended to influence an audience.

This term is being used to legally prevent terrorist attacks in the United States, despite the fact that it seems to exclude persons acting alone as terrorists. Iranian religious scholar AyatullahTaskhiri, who accuses the US of supporting terrorism, defines terrorism as an act committed to further an immoral or corrupt objective, endangering national security, and violating the rights upheld by religion and humanity. According to Bruce Hoffman, terrorism is an act of aggression performed with the intention of accomplishing political aims, it has significant psychological repercussions, and it is typically carried out by non-state actors as well as revolution organizations.

Thirdly, the definition of terrorism brings out three key characteristics: first, the victims of a terrorist act are generally the Authority of a State or an international organization;

Second, the threat of violence is intended to intimidate, instil fear, or persuade the primary target to do or refrain from doing something; and third, the definition of terrorism reveals three key characteristics: (s). Presenting it in other way, terrorism is the use of repeated acts of violence to further social, political, and religious aims in an effort to instil fear in its targets and control, terrify, or force them, which can include both the general populace and the government.Cyber terrorism has few global features, that are as following:

- It is an act which is performed to putforth an object oriented destructive or disruptive message to the government(s).
- There exists numerous ways to convey this message, viz., through denial of services, sending threatening emails, defacing of government websites, hacking and cracking of crucial governmental systems or 'protected systems',disrupting the civil amenities through destroying the proper working of the digital information systems, etc.
- It is capable to impact the computer system and the network setups in a complete way, it could also affect the governing system, and it could affect the population of the target area to create a threat.
- Computer systems and electronic communication technology are accessed as a main tool to achieve extremist purposes.
- The complete acts could be inspired by religion based, social orevenpolitical ideologies.
- Generally done by hi-tech offenders.

Who are Cyber Terrorist?

While considering about the cyber terrorists, two questions can be easily created by an intellect.

- Whether the existence of terroristsorganizations real.
- Whether have these organizations been created recently?

The greatest threat appears to come from organizations that have historically functioned in the "real" world, despite the fact that there are certain organizations of "pure" cyber terrorists operating in the world. Terrorist organizations can now readily disseminate their messages to the entire world over the Internet, while typically having no access to television or radio communication. the requirement for many sizable terrorist organizations to either maintain their own websites or have webpages specifically dedicated to their organizations. The alleged perpetrator of the gas bombing on the Tokyo subway system, Aum Shinrikyo, has its own website.

The Party of God, HIZBULLAH, as well as anti-Western and anti-Israeli terrorist groups, have always been linked to numerous heinous attacks, including the bombing of American military barracks in Beirut and the destruction of its own website. These websites enable terrorist groups to communicate with their intended target audiences, which is the global populace from the perspective of the United States. According to the United States, Al-Qaida is the most dangerous terrorist group and is regarded as their number one opponent. The ability of the group to manipulate US energy facilities including water distribution, communication systems, and many other crucial infrastructures was scouted, according to US officials, who claim that computer data was seized in Afghanistan.

International Initiatives to Combat Cyber Terrorism

Not surprisingly, the public conversation has concentrated on the regulatory aspects of cyber crimes generally and cyber terrorism specifically due to the ever-expanding scope and negative effects of information technology on people, society, business, and government as a whole. Regulating cybercrime has created basic concerns that have never been addressed in the setting of real-world contextual experiences because of its unique characteristics and qualities.

Without a doubt, any national legal response by a particular nation will be of little use in containing the transnational menace of cybercrime and cyber-terrorism.

To effectively investigate and prosecute cybercrime and cyber terrorism conducted remotely and with an expanding spectrum of international targets, a well-established network or inter-State will be required. How will a system in another country be searched and seized? How can a nation ensure that a criminal who is a citizen of another nation appears in its courts to face justice? Nation-to-nation cooperation in the fight against cybercrime and cyber terrorism is crucial given the mechanics of international participation.

In light of this, the has researcher made an attempt to conduct a comparative analysis of legislative measures implemented by the USA, the United Kingdom, and Australia. Following a thorough examination, concluding remarks will be drawn in regard to application in India to enhance the legislative measures implemented inthe Information and Technology legislation and to close the holes in Indian cyber laws.

Measures Taken

The rapid increase in cyberterrorism has forced State and organizations at international level to reform the global security related to cyber architecture for striking down cyber terrorism.

International Forums

- ***Conventions on the issue of Cyber Crime***

The first legally binding international treaty on cybercrimes was established by the EU and is known as the Budapest Convention. It proposes to adapt investigating procedures on cybercrimes for member states and strives to harmonize domestic laws, including an international cooperative framework. This pact excludes India.

- ***The United Nation (UN)***

  i. **UN Strategy on Countering Global Terrorism:** The plan is for demonstrating of dedication of all UN members so as to eradicate the terrorism in all possible its forms. The resolution aspires in increasing of the international and regional collaboration and the coordination in among states, private players of the nations, and others in the fight against cyberterrorism. It also wants to stop the spread of terrorism via cybernetworks.

A resolution asking members to have an assurance that the cyberspace is "not a safe haven for the terrorists" was completed for the sixth review of the plan in 2018. It exhorts its member nations to combat terrorist tactics, provocation, and even recruiting, even online.

  ii. **United Nations Office of Counter-Terrorism:** The UNOCT was established on June 15, 2017, by resolution of the UNGA, in response to the Secretary-report General's on the UN's role in helping member states implement the UN's counterterrorism policy. In essence, the UNOCT supports member states' counterterrorism activities, particularly those against cyber terrorism. It offers multi-stakeholder collaboration to protect each country's cyberspace from cyberterrorist threats.

It has even started a number of projects aimed at increasing the capacity of states to defend against cyberattacks and educating the public about cyber terrorism.

  iii. **United Nations Security Council (UNSC):** A UNSC resolution for the protection of CI was adopted in 2017. In order to prevent, protect from, respond to, and recover from a cyberenabled terrorist attack on the Nations Computer Integration, the member states were urged by the resolution to create collaboration with all international and regional partners.

It even requests operational intelligence sharing between the governments regarding how terrorist organizations are using communication technologies.

USA

- ***Cyber Security and The Infrastructural Security Agency Act***

The Act stipulated that the CISA would assist in securing American cyber networks and CI, developing US cybersecurity formation, and growing potential for cyberattackdefence. Additionally, it protects the ".gov" domain network used by the federal government. Additionally, it is home to the National Risk Management Centers (NRMC), which address the greatest strategic threats to the nation's critical infrastructure as well as vital operations whose disruption could have a grave impact on American national interests in security and the economy. President of USA issued an executive order in 2017 to modernize US cybersecurity capabilities in response to growing cybersecurity threats against CIs and other vital assets.

- ***National Cyber Strategy of the US***

The policy, which was unveiled in 2018, aimed to fortify US cyberspace and prepare for cyberattackdefence. It even emphasizes defending against cyberattacks and securing CIs and federal networks. The main objectives of the cyber policy are to defend the American people, maintain peace, and advance American interests. Even military action is allowed to stop cyberattacks.

UK

In order to defend its computer networks from cyberattacks, the UK implemented the National Cyber Security Program in 2015. A five-year-old National Cyber Security Strategy was also made public in 2016, with the goal of making the UK's internet more safe and resistant to intrusions by 2021. As a result, the National Cyber Security Center was established in 2017 with the goal of responding to sophisticated cyberattacks.

Initiatives Taken to Combat Cyber Terrorism in India

India's perspective on cyber terrorism If the 26/11 Mumbai attacks were examined in detail, it would become clear that the terrorists' use of the internet for communication and research about their target demographic and the location led to similarly terrible effects in India. In July 2011, explosive attacks in a busy city market in Mumbai's Jhaveri Bazaar were also carried out using digital technology. In the 2010 Varanasi bombing case, the Indian Mujahidin claimed responsibility for the attack through online communication.

The Indian Government was alerted by this and immediately took aggressive action to improve cyber security, including modifying the Indian Information Technology Act, 2000 to forbid terrorist activity online.

Section 66F, which has defined and has also described cyber terrorism, was particularly introduced into this statute for this purpose. (1) Whoever- (A) with the aim to cause terror among the people or even any portions of the people, or to harm any of thebe it unity, integrity, security, or sovereignty of India- is prohibited, in regard to Section 66F.

1. Denial or cause the denial of access to any person authorized to have access to computer resources.
2. Attempting to get into or access of a computer resource without the authorization or even exceeding of authorized access.
3. Introduce or cause to introduce the Computers Contaminant and with means If such act results in or is likely to result in a person's death, bodily harm, damage to or destruction of property, interruption of a supply or service essential to the community's daily operations, or negatively impacts the crucial information infrastructures listed in Section 70, or (B) intentionally or knowingly seeks out or gains access to a computer resource without authorization or in excess of that which is permitted, thereby gaining access to any information, data, or computer databases that are restricted for reasons of national security or relations with other countries;restricted information, data, or computer databases, or a reason to believe that information, data, or computer databases that are so gathered may be used to cause or even likely to cause harm to the interest of India's sovereignty and integrity, the State's security needs, friendly relations with other countries, public notice, decency, or morality, or in relation to court disobedience, defamation, or even inciting an offence, or to the benefit of another party.

As cyberterrorism offences and even conspiracies to commit such offences are punishable by up to a life sentence in prison. According to the definition given above, cyber terrorism is the act of hacking, blocking, or contaminating computers in order to deny access to computer resources in general to people who are legally authorized to use them, as well as to gain or obtain unauthorized access to any information that is "restricted information" for the sake of national security, foreign relations, etc.

These horrifying acts may cause death and injury to people, property damage, a disruption of civil service that is essential to the life of a community, and also have an impact on the crucial information infrastructure. They are performed with the intent to threaten the security, sovereignty, and integrity of India or instil fear in the minds of people or a section of people. In the instance of the 26/11 Mumbai attacks, it was clear that the terrorists had exploited communication services to further their murderous plans rather than to hack or block the protected information.The monitored messages that the Indian government had access to throughout the prosecution of the Mumbai attack case would unmistakably demonstrate that the radicals were speaking only in accordance with their individual freedom of speech. When examining the communication as a whole, it became clear that this speech was being made in an effort to undermine India's sovereignty, security, and peace; as a result, it no longer qualifies as protected speech under Article 19A of the Indian Constitution.

In addition, it constitutes a terrorist act. This particular aspect is conspicuously absent from the definition given by section 66F. The IT Act, 2000 (amended in 2008) made laborious, surprising attempts to secure protected systems, as specified by Section 70. Any computer resources that could directly or indirectly impact the Critical Information Infrastructure are declared to be protected systems by the government through announcements in the Official Gazette. According to an additional explanation provided to this section, "Critical Information Infrastructure" refers to a critical computer resource for the nation's security, economy, and health and safety of the general population that, if destroyed or damaged, would have a "debilitating influence" on these concerns.

Insight into Information Technology Act vis-a-vis India

The nation is currently facing a high level of dramatic cyber warfare. However, as we continue to see, we are mostly unprepared to defend against China and Pakistan's cyberterrorist attacks against India. When Swedish "ethical hackers" were able to blog in detail about the email account and password of many Indian government institutions, including the Research for Defense and various Development Organizations, like the Academy of National Defense, etc., different gaps in the Indian cybersecurity environment were recently closed. The issue becomes more important partly because China has gradually improved its capacity to launch electronic warfare along with its fast (and covert) modernization methods for militaryarmour.In order to give the ongoing Indo-Pak confrontation over Jammu and Kashmir a new direction, terrorist organizations and Pakistani hackers are continuously stepping up their attacks on Indian websites. These terrorist organizations looked to the internet and information systems to expand their methods of combat into uncharted territory, give their conflict a lost-price dimension, and achieve their intended goal of causing harm. Particularly over the past few years, several hacker groups from Pakistan, like the hacker club of Pakistan which is Pakistan Hacker Club, have increased their attacks on Indian websites.

The Information Technology Act validates legal guidelines pertaining to cyber terrorism. The Act's Section 66F introduces regulatory mechanisms for cyber terrorism. It outlines the three primary criteria for an act to qualify as cyber terrorism, along with the punishment, which can include life in prison:

The performed act has to be done with the intent to terrorize people, jeopardize or even threaten India's unity, integrity, security, and sovereignty.

The following must have happened as a result of the act:

- The unlawful blocking of any legally authorized individuals from accessing any online or computer resource or network.
- Unauthorized attempts to access or break into any computer resource.
- introduce any computer contaminants, directly or indirectly.

Harm: The act must have also resulted in harm, such as human death or injury, detrimental impacts on sensitive information infrastructures (CII), property damage or destruction, or disruptions likely to result in the disruption of services or supplies that are also vital to human existence.

Additionally, Section 66F has been applied in cases where a person gains access to a computer resource without the proper authorization or even by willfully exceeding that authorization. Other situations include when that person then obtains access to data that has been restricted for Indian security interests or whose disclosure would jeopardize India's sovereign interests, etc.

- ***The Protected System and CII***

The Act also includes a provision for "protected systems," which allows the appropriate authority to designate any computer resources as "protected systems" if they directly or indirectly impact the CII facility. When someone really secures or simply makes an attempt to secure access to the protected system, Section 70(3) allows for a fine and a sentence of up to 10 years in prison. The definition of CII according to Section 70's explanation is as follows: "The computer resource, which shall be definitely having a detrimental influence on the national security, economy, public health, or safety."The National Critical Information Infrastructure Protection Center (NCIIPC) has been designated by the national central government in regard to the national nodal agency for CII protection in accordance with Section 70A of the Act. To address issues related to cybersecurity and cyberwarfare, the central government formed the Defence Cyber Agency.

- ***The Indian Computer Emergency Response Team (CERT-In)***

Section 70B of the Act provides that constitution of CERT-In so to maintain the Indian cyber security and countering cybersecurity threats against it. The CERT-In is also expected to protect Indian cyberspace from cyberattacks, issue alerts and advisories about the latest cyber threats, along to coordinate counter measures to provide prevention and also respond in counter to any of possible cybersecurity incidents. It basically acts as nations check system and also alarm mechanism and performing acts like the:

- Gathering, analyzingand disseminating information about cybersecurity incidents; forecasting and issuing alerts on the cyberincidents.
- For emergency measures to handle the cybersecurity incidents.
- Gathering, analyzingand providing information about cybersecurity incidents; forecasting and issuing alerts on the cyberincidents.

In order to combat domain-specific cyber threats and build more secure cybersecurity systems in corresponding domains, like the power grids and thermal energy, India formed domain-specific computer emergency response teams (CERTs). In an order so as to meet the cybersecurity needs of such a crucial domain, sectoral CERTs have also been developed in the financial and defence sectors of cybersecurity.

Policy vis-a-vis India's Cyber Security

The 2013 release of India's National Cyber Security Policy intends to protect Indian cyberspace and concretely increase its resistance to cyberthreats across all industries. This attempts to build a strategy for safeguarding India's CII and a mechanism for effectively retaliating against cyberattacks. It also emphasizes developing a reliable and secure cyber ecosystem for the nation. Additionally, the regulation has helped create a safe computing environment and greatly increased both trust and confidence in electronic transactions. A crisis management strategy has also been put in place to combat terrorist strikes made possible by the internet. Additionally, the National Investigation Agency (NIA) Act was revised by the Parliament in 2019 to enable the NIA to look into and prosecute instances of cyber terrorism.The use of technology and threats intelligence is also crucial in the fight against cyberand conventional terrorism. The Multi-agency Center (MAC), which was established at the national level following the intrusions in Kargil, as well as subsidiary centres and those at the state level, have all been fortified and reorganized to enable them to operate on a 24x7 basis. The MAC includes even more than 28 agencies, and every agency engaged in counterterrorism is a member of the mechanism. It is a crucial component of the national programme as well.

III. Analysis and Recommendations

The Legislative Reform

- ***The Information Technology Act***

India, whose economy is now even referred to as being in rapid development, wants to take control of the global supply chain and internationalize its economy. This kind of vision also brings with it a significant responsibility to safeguard cyberspace from potential risks, such as acts of cyber terrorism. India has, nevertheless, been particularly open to cyber threats. Transition, with major economic activities transpiring through digital platforms during the COVID-19 pandemic, the dreadful impact of cyber terrorism has intensified.

The objectives of the cyber terrorists is into to ruin the CI of the nation and few other services, be it like the telecommunication, or the banking, financing, military compartments and emergency services, are the most prone to and vulnerable that to cyber terror attacks. Hence, it is essential to comprehend potential of the cyberterrorism for a nation like India by keeping in mind that vulnerability of the Indian cyberspace to cyberterror attacks has sprouted enormously. In the year 2018, the then Home Secretary has even admitted to India's exposures to cyberthreats and its inefficiency or inadequacy in the act of to counter them. Therefore, reforming also modernizing of the existing machinery so as to counter the strategic challenges of the cyber terrorism.

As the Act enacts the provisions relating cyberterrorism, in regard to make it a more focused legislation to combat cyberterrorism, the following modifications are suggested:

(i) The legislation has been basically enforced for validation of e-procurement activity. However, the preamble is present must not remain to limit to the procurement. It must in addition inculcate the aim of resisting cyberterrorism.

(ii) The ambit of definition for the cyberterrorism should have been made way more extensive by also including 'the usage related to cyberspace and also communication' through the cyber space. The provided provisions does not cover the cyberspace use for communication and also the related purposes to fulfil and execute the terrorist objectives. The Act should also inculcate sections to bring under the ambit such acts in order to prevent the acts of cyberterrorism.

(iii) To keep a check on combating cyberterrorism, it is necessary for it to have a separate chapter that describes in detail all the complex components and aspects of the acts that constitute cyberterrorism.

- ***Indian Cyber Security Act***

The IT Act was modified in 2008 to include the parts pertaining to cyber terrorism. The terrorists' use of the internet has undergone a significant metamorphosis between 2008 and 2021, though. In order to utilize cyberspace for youth transition and to launch cyber attacks that cause such immense havoc or destruction, cyberterrorists are now utilizing a new, inventive way.In securing Indian cyberspace from potential cyberthreats and to safeguard the nation's cyber sovereign interests, the destructive technical order that has evolved to support cyber terrorism also calls for the modernization of the legal system.The Indian cybersecurity Act, which is intended to address the present cybersecurity issues and regulate all facets of cybersecurity, including cyberterrorism, should be taken into consideration for enactment in India. Additionally, the law would now allow for a more robust, rigorous, and effective legislative structure that is opposed to cyber terrorism in the context of future consolidations of the threat from this crime.

Administrative Reforms

- ***Numerous Organisations***

India's counterterrorism processes are controlled by a number of government organizations, which causes redundancies in the operations and authorities of the organizations. Only a few reformative steps, like that of the the appointment of theCoordinator of National Cyber Security to the National Security Council Secretariat (NSCS) and subsequent subordination of the central agencies to its whole authority, have been approved. Additionally, it is crucial to provide the three core agencies—CERT-In, NCIIPC, and the defense-oriented Cyber Agency—exclusive responsibility for cyber security with clearly defined jurisdictional boundaries for their activities. The territorial limits of activities must, to the extent practicable, be specified in legislation in order to avoid the development of a parallel leadership system that causes unjustified work overlap.

To maintain India's cybersecurity system current with the constantly changing cyberspace, there must also be a frequent evaluation of the competencies of organizations. The National Cyber Security Administrator must with full efficiency integrate the actions of the cybersecurity authorities to strengthen India's capacities to counter cyber-terrorism because what is not currently a CI may become intrinsically vital for maintaining national security tomorrow.

- ***Awareness Programme***

In order to protect the nation from potential cyber threats, including cyber terrorism, the authorities, like UNOCT, must implement cybersecurity awareness programme and create an educational environment. In acquainting people with the threat of cybersecurity in a time-bound manner, the government should also take into consideration starting a cyber literacyprogramme (at first in the areas susceptible to cyberattacks). Also with COVID-19 pandemic and the majority of firms operating digitally via the internet, it is especially crucial.

- ***Indian Cyber-security Services***

India's massive cybersecurity infrastructure is thought to be too large to be changed and developed from a single central point. You could say that everybody, particularly those who reside in rural sections of the nation, now accept cybersecurity risks as the new standard. In this regard, India ought to create the Indian cybersecurity Service as a part of the national civil service. In order to cope with all aspects of information security, including cyberterrorism, the country will have access to high quality personnel, who will be stationed in various communities at the basiclevel level. The all-India civil service will, as expected, equip state governments with more skilled cybersecurity officials to secure online activity and fix security breaches that fall under their control.

The planned civil service might also help the state police crack down on cybercrimes more quickly and effectively, which would enhance how justice is administered in these cases. In addition, the cybersecurity authorities will have the chance to work in various locations across the nation, such as as officers of all-India services, which will broaden their perspective and give them actual operational experience with cybersecurity difficulties presented by the general public, in contrast to the current paradigm. Therefore, just as officers from other civil services at national level do, Indian cybersecurity authorities would also have a much greater say over the majority of policy issues relating to cyber threats and cybersecurity that are of interest to others. This is because they have comprehensive background research and direct first-hand experiences that have given them actual ground realities.

Laws of Other Countries Vis-a-Vis Cyber Terrorism

The UK Act for Terrorism, 2000 is the legal instrument used in the UK to enact regulations on terrorism, particularly cyberterrorism. The Act's Section 1 states three requirements—intention, motive, and harm—that must be present for an act to qualify as terrorism. In addition, Section 1(2) provides a list of additional harms that a terrorist act may produce. Broadband providers, computer companies, stock exchanges, and other entities can all be considered electronic systems. Thus, the legislation in the UK has a broad definition of terrorism. In the same way as a real cyberattack, it may also be applied to a threat which is related to cyber attack Even cyberattacks that are just intended to "impact" authority are considered to be acts of terrorism.

- ***Australia***

After the 9/11 terror incident, the nation passed a group of five pieces of legislation as part of its anti-terror statute. The concept of terrorism found in Part 5.3 ofCriminal Code of Australia was integrated by the way Security Legislation Amendment Act, 2002 specifically for terrorism. The Criminal Code also defines terrorism in Section 100.1. Australian law similarly establishes higher thresholds than the UK's terror law for what constitutes terrorism. Therefore, cyberattacks meant to impact primarily the government and public sector do not qualify as cyberterrorism in Australia. The legislation requires that an act of cyber terrorism must have the intent to intimidate or compel a government in order to qualify as such.As a result, the cyberattack must be both intimidating and coercive. According to the argument, only actions that seriously interfere with, disrupt, or destroy electronic systems are covered by Australian terror law when it comes to cyberattacks. Because there is a "national resistance exemption" in the statute. It establishes that any type of dissent or protest that does not aim to kill, seriously hurt, imperil, etc., shall not be considered terrorism. As a result, the Australian Criminal Code, unlike its English counterpart, identifies a smaller number of cyberattacks as Cyber Terrorism.

- ***Canada***

The Canadian Criminal Code's Section 83.01 defined terrorism as any act or omission committed inside or outside of Canadian borders with the intention of achieving a authoritative, religion based, or ideological perspective, intimidating the general public or a particular group of individuals inflicting life threatening physical injury or the death, putting a individuals life in danger. In addition, laws in Canada incorporates an exception for political demonstrations, just like Australian law does. Although it stipulates that terrorist acts must "compel" a government to take a certain action or refrain from taking one, this provision establishes exceptionally high requirements for what constitutes a terrorist act. The term of terrorism in Canadian law includes attacks against both domestic and foreign organizations. As per British law, this creates a wider operational area against "global government entities." Attacks against people are also considered terrorist acts under Canadian law. It also states that an act must intend to interfere with a vital system, service, or facility in order for it to be considered cyber terrorism. This creates a new, high bar for the legal application of the term of terrorism in a cyberattack.

IV. Methodology

Most of the data collected for this research paper was secondary based. Secondary analysis involves the use of existing data, collected for the purposes of a prior study, in order to pursue a research interest which is distinct from that of the original work; this may be a new research question or an alternative perspective on the original question. The following sources that were used to collect data were: books, journals, reliable internet sources and journal databases, as the information that was needed to compile this paper required information based on different laws of respective countries. It would have been very difficult to collect all the information that was needed using primary research as it would have been expensive and very time consuming, therefore secondary data was opted as another method.

There are many advantages for using secondary data as it has already been collected, therefore it is cost and time effective with high quality data that has an opportunity for longitudinal and cross cultural analysis. According toPrensky, secondary data helps refine research and design further research as it provides a full context for interpretation of primary research. While the benefits of secondary sources are considerable, their shortcomings have to be acknowledged. There is a need to evaluate the quality of both the source of the data and the data itself. The researcher must be careful when using secondary data as it is collected for a different purpose and therefore it is unknown to the researcher. With secondary data there are a few limitation that come with it such as the there would be a lack of familiarity with data then when you collect your own as you become familiar with your data, and the data that is not yours you may also find the complexity of the data to be a problem or they may find that the data is missing a key variable. The secondary data collection may neither be valid nor reliable. The data is also dated, which means new information will be published by the time this is used.

V. Results

As witnessed past two decades have witnessed a significant shift in the concept of national security as a result of new technical advancements. The new generation of offensive technologies poses a threat to nations not just in terms of physical destruction, but also in terms of destroying, altering, or incapacitating their information infrastructures. The fundamental cause of this dissatisfaction is the nature of cyberspace, where cyberterrorism occurs, which is continuous and unlimited in nature, ignoring all territorial and parliamentary barriers. In regardto the other aspect of the coin, if a nations cyber legislation is limited in scope, it will be unable to combat the terror of cyber terrorism in various nations.

Since the beginning of the technological dependent era it has been emphasized that both the crimes be it cyber crime or terrorism cannot be said as just a national issue but should be considered at an international level. The communication, commercial transactions and governance have become the impediments of time and space.

The international components of the commissions of cyber crimes and terrorism has created new issues,provocations for law, might be obtained in particular nation, the data altered in any of other, and the effects impactin a third. The result of this power is that its various sovereign domains, laws, and rules are put into action. The speed, mobility, adaptability, relevance, and worth of electronic transactions significantly undermine the present laws of international criminal norms.

VI. Conclusion

To summarize, the proliferation and development of computer networks are inextricably linked to the growth and development of our society in the long run, and we need to raise public awareness of this reality. The future war will be waged in a virtual network rather than on the field. To foster an international agreement on cyber deterrencespecially cyber terrorism, all countries must take the necessary measures. Vasudev Kutumbkum, which means “the universe is one family,” is a term stated in the Hindu Vedas. We must regard the entire cyberspace community as one big family, and we must be happy and able to contribute all we can to ensure the peaceful coexistence of everyone.

References

[1] Rao S.V., Law of Cyber Crime and Information Technology Law, 1st ed., Wadhwa & Company, Nagpur, 2004.
[2] Ilia B.&Susan N., International Criminal Law, 2nd edition, Cavendish Publishing, United States, 2003.
[3] Guadamuz A., Law and Society Approaches to Cyberspace, Ashgate Publishing Limited, Hampshire, 2010.
[4] Sahoo G.P., New Legal Dimensions of Cyber Crime, 1st ed., Satyam Law International, New Delhi, 2017.
[5] Sharma V., Information Technology Law and Practice, 4th ed. Universal Law Publishing, 2015.
[6] Malcolm N. Shaw, International Law, Cambridge University Press, 1st South Asian Edition, 2011.
[7] Gupta A., Commentary on Information Technology Act, 2nd ed., LexisNexis, Gurgaon, 2013.
[8] Verton D., & Brownlow J., Black Ice: The Invisible Threat of Cyber Terrorism, Mcgraw Hill Companies, NY,USA, 2003.
[9] Rodney D. Ryder, Guide to Cyber Laws, Wadhwa Publications, Nagpur, India, 2007.
[10] Dr.Amita Verma, Cyber Crimes & Law, Central Law Publications, Prayagraj, U.P, India, 2012.
[11] Information and Technology Act, 2000.