Cyber Terrorism and International Humanitarian Law

Sreoshi Sinha[1]

Abstract

Terrorism, the most violent form of perpetration has existed since the inception of human civilization. Though the conventional motives have remained the same, the traditional concepts and methods of terrorism have evolved into deadlier forms with the advancement of modern technology. Information technology is one such area which has increasingly allured the terrorists over the years due to the garb of anonymity it offers to the perpetrators of terror. The increased reliance on information technology by the terrorists has significantly given rise to security dangers and hence this new menace became a major challenge to world security and the phenomenon that evolved came to be known as cyber terrorism. The disastrous impacts associated with cyber terrorism made it all the more impossible to be control or prevented. The issues of safeguarding against the threatening of such operations still remain uncertain. Hence the Geneva Conventions or the current Law of War remains relevant to cyber terrorism, but yet the precise points of pertinence remain largely unclear. My central argument would dwell upon whether the International Humanitarian Law or the Law of War would be effective in preventing this newest form of terrorism or not.

Keywords: *Cyber Terrorism, Internet, Global Threat, Security.*

1. Introduction

In the absence of a universally accepted definition of terrorism, the general concept is that it has existed since the inception of human civilization and has been demonstrated as one of the greatest challenges to global security. In spite of endangering innocent lives and jeopardizing human rights and fundamental freedoms through ages, the international community has failed to frame an effective measure to prevent it. Rather with time the nature of terrorism has evolved. Though the old motives of terrorism have remained the same the conventional techniques and methods of terrorism have acquired newer disastrous forms. In the age of information technology, perpetrators of terror have attained an expertise to bring about the most destructive blend of weapons and technology, deadlier in nature. One such phenomenon that has evolved is cyber terrorism. This is a phenomenon where the cyber space is used to launch terror attacks[2]. It is capable of doing indeterminable harm not only by paralysing computer infrastructures but also using the cyberspace to assist and arrange traditional forms of terrorism, such as bombings and suicide attacks. This increased

[1] PhD Research Scholar, Nelson Mandela Centre for Peace and Conflict Resolution Studies, Jamia Millia Islamia, New Delhi

[2] Z Yunos and S Sulaman. "Understanding Cyber Terrorism from Motivational Perspectives." Journal of Information Warfare, 2017: 1-13.

dependency on information technology by terrorists might pose immense security risks on all the nations unless timely security measures are adapted to enhance prevention in the years to come. Cyber threats - cybercrimes, cyber terrorism, cyber warfare have become major concern for governments across the world.

Apparently, due to the ambiguous nature of the term terrorism, a universal concord on the derived term "cyber terrorism" could not be achieved; hence this issue is left to the independent apprehensions of the states. Apart from that, the traditional domain of warfare also does not include the cyber space within its ambit, due to which there might be problems in applying legal mechanisms such as the fundamental principles of International Humanitarian Law (IHL) to prevent it. Therefore, to understand cyber terrorism in the context of International Law this paper addresses whether the current "**Law of War"** or "**International Humanitarian Law" (IHL)** applies to cyber terrorism or not.

To find out the answer, this paper shall make an attempt to discuss the evolution of the term cyber terrorism, the meaning and concept of the term and the rising incidents of cyber terrorism in terms of International Law, across the globe, the motives and methods behind an attack. It shall also discuss the regional and international mechanisms to prevent cyber terrorism, and recommend what more could be done.

2. Cyber Terrorism as a Legal Concept

So far, the international legal framework seemed to have provided several mechanisms on global terrorism until the world had witnessed the most violent form of this menace in September, 2001. Since 1963, till now there had been a set of eighteen international legal instruments (including the amendments) of which thirteen had already existed prior to the 9/11 terrorist attack. With the terrorist strike on the World Trade Centre in the United States, the focus on global security heightened and this gave an impetus for the establishment of significant international documents such as the "**2005 Convention for the Suppression of Acts of Nuclear Terrorism"** and the "**2006 United Nations Global Counter-Terrorism Strategy"**[3], the documents which were structured upon the earlier existing legal premises. But even though various developments in the existing international legal principles pertaining to terrorism came to being, certain elements remained unchanged, such as the failure to adopt the "**UN Comprehensive Convention on International Terrorism"** due to major confusion over the definition of terrorism. Certain other components such as the "**recognition of self-defence"** in response to a **terrorist attack** by a **non-state actor** were

[3] "'India to garner support for anti-terror initiative CCIT at BRICS'. *The Economic Times*, 15 October 2016. Retrieved 17 November 2017"

expressed by the "**Security Council in Resolutions 1368 and 1373"**[4] of the "**right to self-defence"** by the United Nations. Though some authors are of the opinion that the threat of cyber terrorism is just a presumed danger and not a fast approaching legitimate threat to quickly work upon, but yet it can be said that post the 9/11 along with a few other serious instances of non-state actors using cyber space for launching conventional attacks, there is a serious reason to start framing technology specific terrorism laws since with such a quick technological evolution, it might not be very far when the danger of this life-threatening cyber terrorism would explicitly start demonstrating itself.

It was not possible for the international legal community to arrive at an agreement on the definition of the term terrorism because of the disparities on the legality of the use of violence for political ambitions. Due to this ambiguous and indefinite characteristic, there is an absence of any legal or any academic definition of this term. So mostly, the definition of 'terrorism' is left to the individual explanation of the states. This lack of a legally accepted definition of conventional terrorism, often acts as major hindrance in describing the nature of cyber terrorism and hence, there is also no definite accord on a permanent definition of the derivative term "cyber terrorism" that was first propounded by Barry Collin in 1997. In the midst of this existing debate, academicians and experts have tried to give suggestions on how to define this concept of cyber terrorism depending on its targets, methods, motivation, and the importance of computer use in the act. Such suggestions include social aspects emphasizing that terrorism is mostly stimulated by "egoism, intolerance, lack of dialogue and inhumanity, greed and accountability", psychological aspects stating "terrorism is a tactic to coerce behavioural change in an adversary" and lastly legal perspectives implying that the distinction must prevail between "attitude and methods" of terrorism.

2.1. Definition

Apart from the existing lack of a universally agreed definition of the term 'terrorism', defining cyber-terrorism becomes all the more complicated also because of the very fine line of distinction between any cyber-attack and cyber terrorism. Cyber terrorism may considerably overlap with cybercrime, cyber war or ordinary terrorism, depending on the context of the crime. Whether a particular cyber-attack would be termed as a cybercrime or a cyber-terrorism and whether the adversary would be referred to as a cyber-criminal or a cyber-terrorist would largely depend on the nature of the deployment, purpose and motive of such an attack. According to the founder of the Kaspersky Lab, Eugene Kaspersky, "**cyber terrorism**" is a more

[4] Ibid.

precise term than "**cyber war**"[5]. This is because, according to him, "with today's attacks, we are clueless about who did it or when they will strike again. Hence, it is not cyber-war, but rather cyber terrorism." He also identifies the massive scale cyber weapons, such as the Flame Virus and Net Traveller Virus along with other biological weapons, stating that in an integrated world, they have the capacity to be equally destructive. Apparently, the narrow line of difference between cyber-crime and cyber terrorism also implies that the motivations and goals behind the two might not be the same. Hence, when an act is perpetuated for economic ambitions instead of ideological ones, it is usually termed as a cybercrime whereas the label of "cyber terrorism" can be assigned only to actions by lone actors or individuals, independent groups and organizations with an intention to create fear among the general population, and also to such acts resulting in casualties or severe destruction of nature and infrastructure.

Again, if similar legal treatment is provided to both conventional and cyber terrorism then attacks that create fear and intimidation amongst the general population, endangers lives and property having a political or ideological motive behind the act of spreading terror can fit into the definition of cyber terrorism. For example, modern terrorists are the ones who not only electronically break into the target's computers networks using the internet but also cause major disruption of infrastructure and immense physical harm endangering millions of lives and property and grossly affecting national security at large.

On the other hand, keeping in mind the conditions of the attack required to be referred to as a case of cyber terrorism, it can be said that any action that instils terror cannot necessarily be termed as terrorism unless there is an ideological motivation or a political purpose behind such an attack. So, in that case if a certain incident of attack backed by an ideological or a political goal, in the cyber space can create fear and terror within the civilian population then only it might be undisputedly referred to as cyber-terrorism in general. Hence, if death and physical harm is considered a compulsory part of a probable definition of cyber terrorism, then any conventional terrorist attack that took place till date and was planned and executed with the help of cyber space can be referred to as a case of cyber terrorism.

However, in absence of a concrete and agreeable definition of both terrorism and cyber terrorism, academics and organizations have suggested a wide range of some possible definitions of cyber-terrorism that comprises of

---

[5] "Eugene Kaspersky quoted in News core, "Security expert warns of cyber world war," Fox News, 1 November 2011, accessed 28 June, 2015, http://www.foxnews.com/tech/2011/11/01/expert-at-london-internet-security-conference-warns-cyber-war/."

the idea that terrorists can cause untold destruction of human life, a global economic and financial chaos and a massive damage to the environment. Their acts can range from hacking and intruding essential government networks, money laundering from financial networks, stealing intelligence information, disrupting daily services to vandalising networks by deleting or altering information and hijacking and controlling major computer networks. However, any definition of cyber-terrorism would have the following components in common:

i. An attack that is stimulated by a political, ideological or religious goal

ii. When an act is perpetuated with an intention to intimidate a government of a state or a segment of civilians

iii. When an act gravely disrupts infrastructure and state machinery

Keeping these common components of a probable definition of cyber terrorism intact the "**Federal Bureau of Investigations" (FBI)** has defined cyber terrorism as "Any premeditated, politically motivated attack against information, computer systems or computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents whereas the **North Atlantic Treaty Organization (NATO)** characterises it as any cyber-attack using computer or/and communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal".[6] The **United States National Infrastructure Protection Centre** defined cyber terrorism as: "A criminal act perpetrated by the use of computers and telecommunications capabilities resulting in violence, destruction, and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a political, social, or ideological agenda." Again, the **Technolytics Institute defines**[7] cyber terrorism as: -"[t]he premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives or to intimidate any person in furtherance of such objectives." After appearing in the defence literature of the in the US Army War College of 1998, the term 'cyber-terrorism' had been defined by the **National Conference of State Legislatures**, as:

> "[T]he uses of information technology by terrorist groups and individuals to further their agenda. This can include use

[6] "22 U.S. Code § 2656f - Annual country reports on terrorism LII / Legal Information Institute."

[7] The Technolytics Institute Cyber Warfare Centre: An independent think tank, working in the fields of cyber issues.

> of information technology to organise and execute attacks against networks, computer systems and telecommunications infrastructures, or for exchanging information or making threats electronically. Some of the examples might be hacking into computer systems, introducing viruses to vulnerable networks, web site defacing, denial-of-service attacks, or terroristic threats made via electronic communication."

However, from a legal perspective, an acceptable definition of cyber terrorism would state the notion of (conventional) cyber terrorism today as the use of electronic networks taking the form of a cyber-attack to commit such acts that are criminalised by the existing legal instruments prohibiting terrorism and international customary law, that results into instilling terror and death among the general population.

2.2 Evolution of Cyber Terrorism

Decades ago, Winston Churchill (the Prime Minister of United Kingdom from 1940 to 1955) termed World War II's emerging Electronic Warfare Technologies the "Wizard War." Today, the Wizard War has evolved into the Internet! And we simply call it: info War, Cyber Espionage, Cyber Warfare, cyber fraud or simply Cyber Terrorism! Wars have been a part of human history since inception. Right from the cruel and biblical wars such as Cain and Abel to the most technologically advanced form of wars such as the Second Lebanon war and the Iraqi war of 2003, humanity has witnessed them all. There have been two major world wars and more than 250 conventional wars since 1914. Apart from the various common reasons for which they are fought, there is another common characteristic to all wars: that is, they bring in modernity and new weapons. Modernity, economic wealth and justice amongst all, had been a common characteristic in the development of nation states in the modern era and growing dependence on technology in turn had been an essential component of modernity. Among much technological advancement, the evolution of information technology is one of the most prominent.

With the increasing dependence on information technology, terrorists and anti-nationalists are fast adopting this newer and modern concept of warfare. This is because it is one of the easiest and cheapest ways for the terrorists to conduct low intensity warfare by a lone actor sitting at any part of the world, through cyber-terrorism. Besides this, the terrorist organizations also take recourse to the web to reach out to their audiences and sympathisers without having to use other media such as television, radio, or holding various press conferences. Such websites designed by these terrorist organizations often contain content and instructions on how to make

explosives and chemical weapons, that helps boost the enthusiasm of their lone sympathisers.

For example, in 1999, an individual named David Copeland, who perceived himself as a terrorist, had murdered 3 individuals and harmed 139 in London. He did this with the assistance of bombs set in three unique areas. During his trial it was found that he utilized Terrorists Manual (Terrorist Handbook - Forest, 2005) and How to Make a Bomb (How to Make Bombs - Bombs, 2004), which had been downloaded from the Internet.[8] With the help of the web they can also plan their course of action, recruit, distribute propaganda and raise financial funds from their sympathisers across the world. Cyber-attacks are more attractive for the terrorists also because they offer a garb of anonymity to the perpetrators of terror and this execution requires more modest number of individuals and littler assets. Hence, these are all the advantages that the terrorists enjoy on using the cyber space to conduct to spread terror. But to know exactly, how it all had begun, we should take a look at the evolution of this phenomenon.

Cyber terrorism as a phenomenon emerged back in 1990s, when the sudden and rapid dependence on internet use gave rise to several studies that dealt with the potential risks faced by the highly technology dependent United States. In 1990, the National Academy of Sciences initiated a report on computer security with the words, "We are at risk. Increasingly, America depends on computers. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb." At the same time, the quintessential term **"electronic Pearl Harbour"** (Richard Clarke) was coined, relating the threat of a computer attack to an American historical trauma. This phenomenon evolved from the 1990s onwards on to 2001 and featured prominently within the security and terrorism discourse soon after the 9/11 radical Muslim terrorist attacks on USA. Since then, cyber terrorism as a phenomenon had continued to evolve, with enormous humanitarian impact on civilian population. It has consequently now turned out to be imperative to examine the tenets of International Humanitarian Law (IHL) that may shield the civilian populace from the malevolent impacts of such an unequal warfare.

3. **Cyber Terrorism and International Humanitarian Law (IHL)**

While there is no specific treaty that deals with cyber-terrorism under international law, there are a number of sources, most importantly IHL and other customary international law rules and general principles of law that would be applicable to this phenomenon. Apparently, according to

[8] South Asian Terrorism Portal, India, available at: https://www.satp.org/ (visited last on Nov 7, 2019).

Andrea Bianchi,[9] IHL is sufficiently well suited to provide a "regulatory framework" and "effective mechanisms" to punish acts of terrorism.

Condorelli and Naqvi[10] opine that a demonstration of terrorist activities is censured in both international and non-international clashes, offering a framework for the arraignment and punishment of the individuals who execute them. IHL takes into account "the violent or systematic nature of terrorist acts perpetrated during conflicts although jus in bello suffers from its own set of deficiencies when it comes to terrorism and cyber terrorism."

Apparently, while dealing with IHL, and cyber terrorism, it is important to remember the distinction between jus ad bellum and jus in bello, where the former means the rules to be consulted before going to war and the latter meaning the standards of conduct after engaging into warfare.(ICRC) For jus ad bellum international law governs the use of force and the dividing line between the use of force and IHL remains unclear because a terrorist act might or might not imitate an armed conflict depending in particular circumstances in which it occurred. Under jus ad bellum, international law governs the use of force through Article 2(4) and Article 51[11].

While Article 2(4) of the UN Charter (UN Charter 1945)[12], "all Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations", Article 51 of the UN Charter emphasises that "nothing in the Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."

3.1. Jus Ad Bellum

3.1.1. Self Defence

Hence, as a part of the collective security system, a victim State might resort to the use of force on being authorised by the Security Council under Chapter VII of the UN Charter. In the context of cyber terrorism, tagging an enabled group with cyber-offensive capabilities as a 'terrorist' is

---

[9] Andrea Bianchi and Yasmin Naqvi. International Humanitarian Law and Terrorism (34) (Studies in International Law). Hart Publishing, 2011.

[10] Luigi Condorelli and Yasmin Naqvi. "The War against Terrorism and Jus in Bello: Are the Geneva Conventions Out of Date?" Oxford, 2004.

[11] Charter of the United Nations: Statute of the International Court Of Justice, San Francisco, 1945.

[12] Ibid.

not enough because for a state to exercise its right to self-defence against a cyber-terrorist group, it has to launch a violent act of a large scale that would constitute both an illegal "use of force" and an "armed attack." Moreover, any case of cyber-attack backed by a political or an ideological goal might not essentially trigger the application of IHL, unless the damage caused by such an attack is grave enough to cause physical injury or casualty on the civilian population, cannot effectively trigger an armed attack under the jus ad bellum. Even though in the great Wall Case the ICJ had concluded that there exists an inherent right of self-defence only in the case of armed attack by one state against another state, but along with this, the Court also remarked that the right of self-defence against aggressive non-state actors has been prevalent in internationally customary law outside the Article 51 of the UN Charter. Apart from this exception, Judge Higgins proclaimed that "there is nothing in the text of Article 51 that sets out that self-defence is available only when an armed attack is made by a State."

In regards to the positions of the countries to exercise their inherent right of self-defence in the case of cyber terrorism, it can be said that though the governments of the states are quite aware of the rising cyber capabilities of the non-state actors, very little has been done till now to counter it. When the "**UN Counter-Terrorism Implementation Task Force (CTITF) Working Group on Countering the Use of the Internet for Terrorist Purposes**" had requested the member states to submit their reports for the 2009 Report on countering the use of The Internet for Terrorist Purposes, none but only two states have submitted a list highlighting cyber terrorism as their greatest threat. On the contrary the rapid development of cyber offensive and defensive capabilities of states like US, China, Russia, Iran, Cuba, Israel and the UK, implies that these states advocate exercising their inherent right of self-defence on cyber terrorists and other non-state actors as a part of their collective security system. Apart from investing immensely in counter terrorism initiatives, only two states US and Israel have exceptionally used force against terrorists and states that have nurtured terrorists on its soil. Sometimes their efforts involved operations that went beyond the limitations of legal obligations. In spite of repeated condemnation of its self-defence acts, Israel continues to support the broader interpretation of the right to self-defence and it might do so even in cases of strikes of cyber terrorism. However, though initially the international community was not convinced with US and Israel's interpretation of the right to self-defence, there was a huge change of attitude post the 9/11, after which states considered the possibility of self defence against non-state actors. But the attention of the States shifted from the implementation of the right to self-defence to the issues of proportionality while assessing the

legality airstrike near Damascus in 2003, invasion of Lebanon in 2006,156 and bombings of Gaza in 2007–2012.[13]

Not only Israel, there were questions on the legality of the US' exercise of the right to self-defence until 2001, before the 9/11, after which things took a turn when Security Council in its Resolution 1368 straightaway implied that the US has the right to resort to self-defence against a terrorist organization. But prior to this, UNGA Resolution 41/38, had heavily condemned the bombings of Libyan Jamahiriya in 1986 carried out in response to the Berlin discotheque bombing along with the counter terrorist operations in Iraq in 1993 and Sudan and Afghanistan in 1998. Finally, the international community showed its approval of UNSC Resolution by being silent during Afghan invasion post 2001.This is very relevant in the case of cyber terrorism also because post the 9/11 attack, as an initiative to strengthen their counter terrorism strategy, President Bush made the Office of Cyberspace Security in the White House and delegated his previous counter-psychological warfare facilitator, Richard Clarke, to head it. The admonitions came now from the President, the VP, security counsellors, and government authorities: "Terrorists can sit at one computer connected to one network and can create worldwide havoc," forewarned Tom Ridge, chief of the Department of Homeland Security, in an representative observation in April 2002 stated, "They don't necessarily need a bomb or explosives to cripple a sector of the economy or shut down a power grid."

Today, the issue is no longer whether the violent acts of terrorist (and cyber terrorist) groups can constitute an "armed attack," or not, but rather how much state inclusion is fundamental "to allow the use of force against the territory of the host state." In this context, there are differences of opinions in the ICJ. While some judges during the Armed Activities case agreed, that if a terrorist attack by armed groups of a significant degree cannot be accredited to a particular State then there is no scope for exercising the right to self-defence. On the other hand, Judge Kooijmans believes that armed attacks are armed attack irrespective of whether it is executed under the patronage of a state or not[14]. Therefore, any country which tolerates any origin of cyber terrorist attack reaching a significant scale on violence, from its own territory can be subject to self-defence. There is a challenge over here also, because at times in the cases of cyber terrorist attack the location of the perpetrator might not be possible to locate. Then the victim state doesn't know which state to retaliate against. This might happen in lone wolf cyber-attacks where a devastating attack might be

[13] Benjamin S Lambeth, Air Operations in Israel's War against Hezbollah. Project Report, RAND, 2011.

[14] "*The 1996 ICJ Advisory Opinion on threat or use of nuclear weapons, Hague*", 1996

carried out by an individual. For example, Osama Bin Laden, but again if the victim state's military operations attack those parts of the perpetrating country in search of just one man then this can raise the question of proportionality which is again another important principle under IHL. In these situations, the host country has to turn towards the Security Council for further opinion.

i. **Armed attack:** For IHL to be applicable there has to be an armed conflict involving an armed attack. Now as ICJ suggested in the Nicaragua states an armed attack is the one that is: "Executed by the State armed forces across international borders or by armed groups, irregular forces and mercenaries when (a) they are "sent by or on behalf of a State" to carry out an armed attack against another State and (b) the attack is of such gravity so that it amounts to an armed attack if it was conducted by regular armed forces of a State.[15]"

Thus, to be entitled as an armed attack, a particular act of violence should reach a significant threshold. The ICJ also upheld that in order to exercise self-defence, it is therefore mandatory to differentiate between the most dangerous forms of the employing force (constituting an armed attack from other less grave forms, and that the 'scale and effects' of that particular act can determine whether a use of force can be classified as an armed attack or not. However, when it comes to measure the scale and effect of an attack in the case of cyber terrorism, one can draw examples of the 2008 Mumbai Taj Hotel attack famously known as 26/11, which took away166 lives. Cyber technology was thoroughly used in developing and executing the operation.

On 15th May, 2012, Lieutenant General George J. Flynn of the US Marine Corps stated that the entire operation was pre-planned through Google Earth where for command and control the perpetrators had used cellular phone networks and social media to trace and fight back to the efforts of the Indian army to prevent them. Earlier a report had stated that Voice-over Internet Protocol (VoIP) software was used by the Pakistan patronised Lashkar-e-Toiba (LeT) group to communicate with the perpetrators of 26/11 on the fields to administer the actual large scale operations going on in the real field.[16] According to the Indian Intelligence sources, the entire attack was being watched live by the perpetrators on television through which each and every movement of the attackers were being closely monitored and instructions were being rendered.

---

[15] The International Court of Justice (ICJ).,n.d. available at https://www.icj-cij.org/en/court (accessed November 2019, 07).

[16] South Asian Terrorism Portal, India, available at: *https://www.satp.org/ (visited last on Nov 7, 2019).*

Again, during the Delhi High Court on attack on September 7, 2011, 15 persons were executed and another 87 severely injured. After a detailed investigation it was concluded that the terrorists had hacked into unsecured Wi-Fi internet connections to send e-mails after the attack. Apart from that, the savage assaults upon discretionary staff and upon their liberty also represented an "armed attack" in the Tehran Hostages case.[17] According to the **ICJ Advisory Opinion 1996 on the threat or use of Nuclear weapons**, that any attack that "releases radiation affecting aspects such as health, natural resources, agriculture, and demography over an extensive area with the potential to damage the natural environment and create deformity in future generations can be termed as an armed attack." Sometimes certain cyber terrorism attacks might not reach the significant threshold in terms of 'scale and effect' to reach the level of the 'use of force' and hence might be kept out from the self-defence framework. For examples, money laundering by terrorist organisations through the use of network might not give rise to the large-scale violence hence cannot come under armed attack regime due to their low intensity.

Therefore, whether an attack in the cyber domain can be brought under the self-defence threshold would depend much on the political circumstances in which it has been executed. Hence, in IHL, there exists a very blurred line between armed conflict and criminal law enforcement.

ii. **Necessity and Proportionality:** A state using self-defence should first make sure that the use of force in reciprocation to an armed attack is necessary and in proportion to the original armed attack and the principle of necessity implies that the victim state must first consider resolving the conflict by the available non-forcible measures, (where non-forcible measures might include diplomacy, law enforcement or sanctions) and if such non- forcible measures are ineffective in preventing the conflict, only then the states should take resort to forcible self-defence. After determining the use of force in self-defence, the state must now show that the response is proportionate. In short, in the jus ad bellum context, principles of necessity and proportionality limit the lawful use of lethal violence. Both jus ad bellum and the **jus in bello** are governed by the principle of proportionality. In the jus ad bellum context, proportionality has a quantitative and operational meaning. The quantitative feature of proportionality necessitates the scale and effect of the counter-force to be similar to an armed attack. In the context of cyber terrorism, exercising the right to self-defence necessitates the response to be necessary and proportional. This is because of the uncertainty that surrounds terrorism as any terrorist attack is always a sudden, instant and unpredictable occurrence. But with the intrusion of technology, cyber terrorism has taken this complexity to a whole new level

[17] Ibid.

as it now appeals for the revaluation of the principles of necessity and proportionality in a new light. It is now necessary for all states to clearly state its reasons to exercise the right to self-defence for acts which are far from being traceable.

3.2. Jus in Bello

Under the **jus in bello**[18] context of cyber terrorism, there are a lot of complexities that are associated with the context of terrorism and in turn cyber terrorism. Apparently, there's a very fine line of understanding between the use of force and the implementation of IHL, to the extent that any instance of a terrorist attack might or might not instigate an armed conflict or a war depending on the scale and effect of such an act. Hence a single terrorist attack not reaching a significant threshold might not give rise to a warlike situation. But the 9/11 did because of the scale of the attack and effects that it had initiated. Other controversies in the context of the applicability of IHL in terms of terrorism arise from the much-debated counter terrorism operations such as the war on terror. However, it is clear that IHL would apply in situations where a cyber-terrorist strike is executed as a segment of an ongoing armed conflict (or armed occupation) itself or if it triggers the armed conflict itself. Terrorism is prohibited equally in times of international or internal armed conflict and acts of violent cyber terrorism are also equally subject to necessity, proportionality, neutrality, humanity, distinction and chivalry.

i. Coming to the **legal mentions** of terrorism, though IHL does not specifically provide a definition of "terrorism", but it does outlaw most of the actions perpetrated during an armed conflict that would have been probably referred to as terrorist actions if committed during peace time. According to IHL, terrorism includes "indiscriminate acts of violence, deliberate attacks against civilians and civilian objects, the use of human shields", attacks on places of worship, and hostage-taking (ICRC 2018). According to **Article 33** of the **Fourth Geneva Convention**,[19] "IHL specifically condemns collective penalties and likewise all measures of (…) terrorism", and Article 4 of Additional Protocol II prohibits "all acts of terrorism and all other acts intending to spread terror amongst civilian population." Such attacks might not prohibit any lawful attack on military targets but definitely forbids any terror act that aims in terrorizing people. Terrorism is also listed as a "war crime" under the statute of the

[18] Yaroslav Shiryaev, "Cyberterrorism in the Context of Contemporary International Law." Legal Studies Research Paper No. 2013-03, University of Warwick, 2012.

[19] The Geneva Conventions of 1949 and their Additional Protocols." INTERNATIONAL COMMITTEE OF THE RED CROSS. January 01, 2018. https://www.icrc.org/en/document/geneva-conventions-1949-additional-protocols. (Visited last on Nov 07, 2019).

"**International Criminal Tribunal for Rwanda and Sierra Leone Special Court"**, as well as the "**1996 Draft Code of Crimes against the Peace and Security of Mankind**."

ii. As the IHL expects to oversee the **conduct of the state military**, cyber-terrorism might be considered as an old fashioned jus in bello terrorism if delivered by the state armed forces (in case of international armed conflict) or of organised groups controlling parts of state territory (in case of internal armed conflicts). Those actors who are not categorised as state forces will usually be included by the legitimate routine on regular terrorism. Such actors not falling within the state forces categories are generally overseen by the legal regime on traditional terrorism. Apart from that, the venture commenced by the state military forces are mostly debarred from this regime by special provisions in the "**2005 Protocol to the Maritime Convention"**[20], the "**2010 Protocol to the Unlawful Seizure Convention**"[21], the "**2010 Nuclear Terrorism Convention"**[22], and the "**2010 New Civil Aviation Convention"**[23]. In this way, soldiers seizing a civilian UAV and crashing it into a construction or causing a nuclear emergency in another state through digital attacks amidst an armed clash cannot be held responsible for ordinary terrorism. A related anomaly in regards to all armed forces within the scope of IHL, suggested by the West in the Draft Comprehensive Convention, is still under serious discussion. There is a dearth of sufficient ratification of the four above-mentioned instruments and hence there exists no customary international law on this. However, such exceptions do not point towards an existing legal gap because no matter how old fashioned the notion of jus in Bello is, because any act that contributes in terrorizing the general population leading to large scale violence and devastation would be considered an act of terrorism and be punishable under war crimes.

iii. Other than this, if a potentially violent terror attack through the cyber space is directed towards the civilian population or to force a state or an organization then it would be treated as no less than a conventional terrorism. In this setting one may consider, for instance, de-individuated digital deaths of people.

iv. In instances of armed clash, where conventional terrorism takes place through the cyber space, it might very well be seen as a crime from the point of need, proportionality, humanity, distinction, impartiality, and valour.

[20] "Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation," International maritime organization. 2010, available at http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/SUA-Treaties.aspx (accessed on October 30, 2019).
[21] Ibid.
[22] Ibid.
[23] Ibid.

Nevertheless, with similar aims and targets conventional terrorism and cyber terrorism may overlap in the years to come.

4. Conclusion

Terrorism as a major challenge to national security in the post-cold war era demonstrates itself in any relevant discussion of global security policy and international law. Keeping that in mind this paper has attempted to give a rough sketch of the legal concept of the term cyber terrorism and its status under the existing international legal framework. Though the concept of cyber terrorism is quite new yet the severity of the cyber-attacks by the terrorists on the relevant government infrastructures, financial institutions, organizations including the ones that use force of a significant threshold causing death and destruction can be devastating and cannot comply with either the values of the UN Charter or that of the IHL. Terrorism itself is an unconquerable phenomenon that had been distressing mankind through ages. Moreover, with the impact of modernity, terrorism has taken a new shape in the form of modern terrorism. Apart from lone wolf attacks which is also a new phenomenon, a modern terrorist is now capable to create havoc sitting in anonymous place just with the help of a mouse and a key board more than any conventional weapon. This phenomenon is increasingly alluring the modern-day terrorist because of many reasons including its cost effectiveness and also due to the garb of anonymity it offers. It is seen that although many international treaties exist to combat this global phenomenon, none of them provide for a binding regulatory jurisdiction. But even then the success of the existing international mechanisms, however less in number they are, to move a step ahead towards combatting cyber terrorism or terrorism on the whole not only depends on the ratification and implementation of these treaties and conventions but also on the efficacy of the big states of the world in complying with the provisions of such legal mechanisms. Cyber terrorism is a transnational phenomenon and only a comprehensive methodology towards battling terrorism in any shape, actualised through the activity of all-inclusive purview of global courts may most likely convey cyber terrorists to equity. Moreover, a universally agreed on legal definition of both the terms ‘terrorism’ and ‘cyber terrorism’ is required not only to categorise attacks and ease the investigation processes but also to bring in co-operation among countries to collectively fight this global threat. Apart from that, the multilateral organizations should improve their law enforcement policies so that they can keep away transnational offenders from misusing jurisdictional and legitimate provisos among national security plans. While coming up with cyber security measures a balance should be made between the safeguarding measures and civil sovereignty. It should exist between the specific interests of organizations and governments so much so that it should help form such a technological environment that will

have no room for fulfilling the unethical ambitions of the cyber terrorists, extremists and hackers.

All such measures can be successfully implemented if all the states unite for this common cause. To materialise this commitment all states, need to work towards replacing the inefficient political systems that operate within each of their territories. A new form of world politics should be introduced and preventing any forms of terrorism must thus be seen as one part of an even larger strategy, one that is geared to the prevention of all forms of international violence. The International community should not only focus its attention to eliminate this global menace but should also focus its attention towards a larger aim of elimination international violence. Only this step by the international community can probably help in eliminating the fear of this catastrophic menace thus retaining survival of mankind. It should be understood that amidst the play of global power politics the capabilities of states to prevent a further escalation of the risks related to cyber terrorism that may someday evolve into even newer forms of terrorism, shall become futile unless and until the world leaders put in enormous efforts to restrain their lure of superiority and primacy and instead focus their entire attention on the emergence of a new sense of global obligation. For this to materialise, a universal counter terrorism regime is needed with an inclusive understanding where all states, all men will be seen as one essential body and one whole community. This idea of oneness should not be based on the fanciful and mythical theories of universal brotherhood but rather on the idea that no matter how much individual states hate each other but yet they should be tied together to pursue the quest of survival. This state of peace, not Utopia of course, can only be achieved if policymakers and world leaders do away with their individual interest and private values and merge them with the interest of the nation. This shall hopefully offer a solution for the world to face such a massive menace together in the years to come.