THE IMPLICATIONS OF CYBER CONTINGENCIES IN INTERNATIONAL HUMANITARIAN LAW

Abhivardhan

Amity University Lucknow, Uttar Pradesh

Humanity has been the observant of various conflicts occurring within itself and so, has the International Humanitarian Law. This has become a quite considerable domain for observation, when it is to be tested how the wake of an ultimate digital revolution leading to the evolution of cyber age, social media and cybersecurity laws have lead to discover a newer set of legal institutions, which keep the equality of the sovereigns, which are inept with the cyber realm in the International Community. Liability and responsibility shifts us to consider how the IHL may turn out to be either a Public International Law or a Private International Law or a bridge between them for every human and statutory instrument, when both of the concepts become more applied and real in their presence. Pursuant to the Geneva and Hague Conventions, the cyber realm needs a more attention to regulate and identify the reachable aspect of IHL, which in the end represents individualism and representation. This inquires to discover a wider manifestation of the realm of phasing and representation-oriented privacy in the budding global cyber community, but has been so far quite limited, which must be dealt with a wider application in the IHL. The paper thus elucidates the various implications of cyber crises and revolution in various countries with a critical analysis of how these contingencies are going to change the fate and face of International Humanitarian Law with special references to various legal instruments and incidents in the cyber world.

Keywords- Cyber Crisis, International Humanitarian Law, Social Media, Cybersecurity Law, International Responsibility.

INTRODUCTION

The events of the Second World War, and concern to prevent a recurrence of catastrophes associated with the policies of the Axis Powers, led to a programme of increased protection of human rights and fundamental freedoms at the international level.[1]. Similar contingencies arose in response to the moving of a Soviet War Memorial, when hackers began interfering with Estonian government websites through distributed denial of service attacks[2] ascribing the NATO treaty, which guarantees its members against a territorial

[1] Crawford, James (2008). *Brownlie's Principles of Public International Law*, Seventh Edition, Oxford University Press, p. 634. [Hereafter Crawford].

[2] Connell, Mary Ellen O'; Arimatsu, Louise (29 May 2012). *Cyber Security and International Law*, International Law: Meeting Summary, Chatham House, p. 3. [Hereafter Connell].

intrusion, yet the era of cyber war and electronic intrusion represents a threat akin to traditional warfare that is of a new, still-developing nature.[3] This underlines a newer beginning paving the way towards a more interesting subject-matter of consideration on how the IHL is going to be shaped. Hence, let us understand the Cyber jurisprudence of nations that has a pervading influence towards the fate of a contribution to the IHL. On 20 July 2008, weeks before the Russian invasion of Georgia, the "zombie" computers were already on the attack against Georgia.[45] The website of the Georgian president Mikheil Saakashvili was targeted, resulting in overloading the site. The traffic directed at the Web site included the phrase "win+love+in+Rusia". The site then was taken down for 24 hours.[67] Jonathan Zittrain, cofounder of Harvard's Berkman Center for Internet and Society, said that the Russian military definitely had the means to attack Georgia's Internet infrastructure. Bill Woodcock, the research director at Packet Clearing House, a California-based non-profit group that tracked Internet security trends, said the attacks bore the markings of a "trained and centrally coordinated cadre of professionals." Russian hackers also brought down the Russian newspaper Skandaly.ru allegedly for expressing some pro-Georgian sentiment. "This was the first time that they ever attacked an internal and an external target as part of the same attack," Woodcock said. Gary Warner, a cybercrime expert at the University of Alabama at Birmingham, said that he found "copies of the attack script" (used against Georgia), complete with instructions for use, posted in the reader comments section at the bottom of virtually every story in the Russian media.[8] Bill Woodcock also said cyberattacks are so cheap and easy to stage, with few fingerprints, they would almost definitely stay around as a feature of modern warfare[9]. Then, we seek a story that "the Stuxnet worm was designed and released by a government--the U.S. and Israel are the most common suspects--specifically to attack the Bushehr nuclear power

[3] Ruus, Kertu (2008). *Cyber War I: Estonia Attacked from Russia*, The European Institute. Retrieved from http://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia.

[4] Markoff, John (12 August 2008). *Before the Gunfire, Cyberattacks*, The New York Times. Retrieved from http://www.nytimes.com/2008/08/13/technology/13cyber.html.

[5] Wentworth, Travis (23 August 2008). *How Russia May Have Attacked Georgia's* Internet, Newsweek. Retrieved from http://www.newsweek.com/how-russia-may-have-attacked-georgias-internet-88111.

[6] Danchev, Dancho (22 July 2008). *Georgia President's web site under DDoS attack from Russian hackers*, ZDNet. Retrieved from http://www.zdnet.com/article/georgia-presidents-web-site-under-ddos-attack-from-russian-hackers/.

[7] (21 July 2008). *Georgia president's Web site falls under DDOS attack*, Computerworld, Retrieved from https://www.computerworld.com/article/2534930/networking/georgia-president-s-web-site-falls-under-ddos-attack.html.

[8] *Ibid* 6.

[9] *Ibid* 5.

plant in Iran[10]", which if "doesn't find one, it does nothing. If it does, it infects it using yet another unknown and unpatched vulnerability, this one in the controller software. Then it reads and changes particular bits of data in the controlled PLCs. It's impossible to predict the effects of this without knowing what the PLC is doing and how it is programmed, and that programming can be unique based on the application. But the changes are very specific, leading many to believe that Stuxnet is targeting a specific PLC, or a specific group of PLCs, performing a specific function in a specific location--and that Stuxnet's authors knew exactly what they were targeting.[11]". It had "already infected more than 50,000 Windows computers, and Siemens has reported 14 infected control systems, many in Germany[12]" at that time, which attributes to consider how the expression and creation of an object can affect various other data systems. Now, this can be termed as a human right violation to a reasonable extent, which can tempt us to move to the intricacies of the IHL. Nothing compares to the destructive power of a nuclear blast. But cyber-attacks loom on the horizon as a threat that is best understood as an extraordinary means to a wide variety of political and military ends, many of which can have serious national security ramifications.[13] For example, computer hacking can be used to steal offensive weapons technology (including for weapons of mass destruction) or to render an adversary's defences[14] inoperable during a conventional military attack. However, the real-world impact of cyber conflict is still difficult to appreciate, in part because there have been no wars between modern, cyber-capable militaries. But an examination of international affairs over the past two decades suggests that cyber battles of increasing consequence are easy to find.[15] Since the earliest days of the World Wide Web, Chechen guerrilla fighters, armed not only with rifles but with digital cameras and HTML, have demonstrated the power of Internet-enabled propaganda[16]. In 2007, Syrian air defence was reportedly disabled by a cyber attack moments before the Israeli air force demolished an alleged Syrian nuclear reactor[17]. The abhorrent nature of nuclear warfare makes even a theoretical victory difficult to imagine. Deterrence by denial is a philosophy embodied in the Non-Proliferation Treaty

[10] Scheineir, Bruce (October 7, 2010). *The Story Behind the Stuxnet Virus*, Forbes. Retrieved from https://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html#76bf040851e8.
[11] *Ibid.*
[12] *Ibid* 11.
[13] Kenneth, Geers, (2010). *The challenge of cyber attack deterrence*, Volume 26, Issue 3, Computer Law & Security Review, 298-303.
[14] DA, Fulghum; R, Wall; A., Butler; (2007). *Cyber-combat's first shot*, Volume 167. Aviation Week & Space Technology.
[15] *Ibid* 14.
[16] P, Goble (Oct 9, 1999). *Russia: analysis from Washington: a real battle on the virtual front.* Radio Free Europe/Radio Liberty. Retrieved from: www.rferl.org.
[17] *Ibid* 15.

(NPT), and one reason behind current international tension with North Korea and Iran[18]. Likewise, cyber-attack tools and techniques are not nearly as dangerous as their nuclear counterparts, but they are by comparison simple to acquire, deploy, and hide. Hacker training and conferences are abundant: over the past 17 years, almost 1000 how-to presentations have been given at DEFCON. More sensitive hacker information can be kept secret, physically transported on a miniscule hard drive, or sent encrypted across the Internet[19]. A nuclear weapons program is difficult to hide[20] ; a cyber weapons program is not. Hence, this must be clearly estimated how will the realm of human rights of every user is protected and conceptualized. In fact, a great example is the term cyber security itself, which the European Union defines as "safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure[21]", which itself is void of any substantiated definition to give it a *jus cogens* and *sui generis* framework.

While domestic laws and practices have been working to address cyber security concerns, the issue of cyber security is a truly transnational issue. Cyberspace is a borderless series of networks, and cyber security threats move across military, political, and geographical boundaries. Attackers can be highly targeted or they can choose to unleash a threat that could impact dozens of countries and millions, or billions of people at once. As domestic initiatives, and countries without extensive cyber security plans, have failed to stop the growing number of highly sophisticated transnational viruses and threats, international cooperation around cyber security issues[22], is becoming the focal point of civil society, governments, private sector, and others[23]. Thus, these are understandable to conclude at first-

[18] GP, Shultz; WJ, Perry; HA, Kissinger; S., Nunn; (January 4, 2007). *A world free of nuclear weapons.* The Wall Street Journal., Retrieved from http://online.wsj.com/news/articles/SB116787515251566636.

[19] *Ibid* 14.

[20] G, Milhollin; V., Lincy; (September 29, 2009). *Lifting Iran's nuclear veil.* The New York Times. Retrieved from http://www.nytimes.com/2009/09/30/opinion/30milhollin.html.

[21] (7 February 2013). *EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive*, European Commission. Retrieved from http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-onlinefreedom-and-opportunity-cyber-security.

[22] Green, Natalie; Rossini, Carolina; (2015). *Cyber Security and Human Rights*. Retrieved from https://www.gccs2015.com/sites/default/files/documents/Introduction%20Document%20for%20GCCS2015%20Webinar%20Series%20-%20Cybersecurity%20and%20Human%20Rights%20(1).pdf.

[23] *Ibid*.

- That accountability of protection of cyber realms at domestic and international levels are fatal and effectively different and deterrence is not only a way.
- That cybersecurity laws need a general principle of international law to govern the basic aspects of cyber programs.
- That the IHL needs newer legal instruments to recognize and limit the fatal contingencies that it has primitively faced; there is no general covenant or convention even, which widens the concept of cyber privacy and responsibility.

THE BASIC PRINCIPLES VACATED IN THE IHL FOR CYBER CONTINGENCIES

The IHL is primarily based on the Universal Declaration of Human Rights, the 1949 Geneva Conventions and various other human rights conventions, declarations to name a few. The difficulties in defining the boundaries of such new legal regime test fundamental assumptions in international law regarding self-defence and the use of force. Only through an analysis of the available legal frameworks may a compromise position be synthesized that responds to the unique challenges posed by IW while preserving the integrity of Articles 2(4) and 51 in the U.N. Charter system that together provide the primary bulwark against the proliferation of violence in international relations[24]. Shackelford analyses the Russian cyber-attack on Estonia and stipulates that "if IW is treated as a crime then the perpetrators would be subject to IHRL, while treating IW as a security threat would bring to bear IHL[25]". There is a paucity of literature dealing with these issues as well as the ethical and human rights implications of IW on national security[26]. Thus, a more basic realm regarding the responsibilities of sovereigns in the global cyber community is the International Telecommunications Union, which is a UN-based agency. However, treatments of IW outside the orthodox IHL framework are nearly[27] non-existent. This is strange since both IHL and IHRL exist to protect the integrity of the human person, but take different approaches towards that end. IHL norms operate within the spatial and temporal constraints of an international armed conflict occurring between two or more

[24] Shackelford, Scott J. (2009). *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, Berkeley Journal of International Law, Volume 27, p. 192. Retrieved from http://scholarship.law.berkeley.edu/bjil/vol27/iss1/7, p. 196, [Hereafter Shackelford]. See generally Carver, Jeremy et al., *The Role of Article 50 of the UN Charter in the Search for International Peace and Security*, 49 INT'L & COMP. L. Q. 528 (2000).

[25] Shackelford, *ibid*, p. 197.

[26] Shackelford, *ibid*. See, e.g., Jonathan B. Wolf, War Games Meets the Internet: Chasing 21st Century Cybercriminals With Old Laws and Little Money, 28 AM. J. CRIM. L. 95 (2000); Debra Wong Yang et al., Countering the Cyber-Crime Threat, 43 AM. CRIM. L. REV. 201 (2006).

[27] Shackelford, *ibid*, p. 197. See, e.g., Cpt, Hanseman, Robert G., *The Realities and Legalities of Information Warfare*, 42 U.S.A.F. L. REV. 173 (1997).

states[28]. Thus, it is correct to estimate what Shackelford meant- "The widespread, amorphous use and rapid evolution of the Internet challenges state sovereignty and makes[29] international law slow to adapt." Even this aspect of basic realm of cyber spheres of relativity and influence brings us into the purview of Private International Law. However, this an also never be forgotten that this self-manifestation has provided a specific contribution to the soft power of nations such as the People's Republic of China, United States of America, India, the European nations and especially, Japan. Thus, the legal background of cyber intervention is of no concern because of the policy concerns of soft power, whenever needed and regulated by the state practice of various nations, which actually encourages the relevance of a global community. The growing interest of states in 'cyber security' has taken place against a background of important shifts in the global strategic environment: the rise of China as a global economic and regional military power; the global financial crisis, the effects of which are still resonating; and an increased assertiveness in international and regional politics on the part of many rising[30] middle-income states. The uncertainty in the international environment provoked by these shifts has added to the sense of complexity surrounding discussions and debates on 'cyberspace' and the use of information and communications technologies (ICTs) for attaining political, military or economic advantage.[31]

However, this is also imperative that "the broadest positive opportunities for the further development of civilization, the expansion of opportunities for cooperation for the common good of all States, the enhancement of the creative potential of humankind and additional improvements in the circulation of information in the global community[32]" is also an imperative subject-matter of consideration. A better analysis can be done by understanding how cyber acts are primarily taken into the purview of criminal jurisdiction and accords. The 2001 Convention on Cybercrime[33] recognizes the "profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks[34]"

[28] Reynolds, Jefferson D. (2005). *Collateral Damage on the 21st Century Battlefield. Enemy Exploitation of the Law of Armed Conflict, and the Struggle for a Moral High Ground*, 56 A.F. L. REV. 1.
[29] Shackelford, *ibid*, p. 198.
[30] Kavanagh, Camino; Maurer, Tim and Tikk-Ringas, Eneken (2014). *Baseline Review ICT-Related Processes & Events Implications For International and Regional Security*. Retrieved from http://f.cl.ly/items/0t073Y3i3P0v2o2x0q39/Baseline%20Review%202014%20ICT%20Processes%20colprint.pdf>, p. 8. [Hereafter Baseline Review].
[31] Baseline Review, i*bid*.
[32] *United Nations General Assembly, sixty-sixth session*, Resolution adopted by the General Assembly on 2 December 2011 [on the report of the First Committee (A/66/407)], *A/RES/66/24*, p. 1.
[33] *Convention on Cybercrime*, ETS 185. [Hereafter Budapest Convention].
[34] Budapest Convention, *ibid*, Preamble.

with the presumed necessity to "deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct[35]. However, irrespective of the implied nature of the Convention ipso *facto* and *ipso jure*, if only a minuscule portion of cybercrimes and other offences entailing e-evidence is brought to justice, it risks failure of governments in their obligation to protect the rights of individuals and society against crimes and loss of faith in the rule of law. Securing e-evidence for criminal justice purposes is particularly challenging in the context of cloud computing where data is distributed over different services, providers, locations and often jurisdictions, and where mutual legal assistance is often not feasible[36]. Trillions of security incidents are reported each year and millions of attacks against computer systems and data are recorded every day. However, a tiny portion of such attacks is actually reported to criminal justice authorities. India is no exception. According to the National Crime Records Bureau, 9,622 incidents of cybercrime were recorded in 2014 under the IT Act, Indian Penal Code and state and local laws. Even if this represents an increase of 69 percent from 2013, cybercrime accounted for only 0.13 percent of all crimes recorded in 2014.[37] While India is confronted with the same challenges, it is not participating in this work, nor sharing its experience and shaping future international solutions as it has not yet decided to join this treaty.[38] Hence, for only nation, when the contingencies do not arise to be quite favourable, when the cyber realm is failingly curbed under criminal jurisdiction and juridical purview, the concept of International Humanitarian Law is someway made to be protected, but this just amounts and proceeds towards a cogent protectionism, which is hoped to be decreasing into a dynamic equilibria of nothing but a mature perspective of thought. Same is the case, when it comes to the matter of communication, where we must understand that every element of expression in that form is sometimes subjected for purview of finding an intent, which is the basis for widening the approaches of criminal jurisprudence for furtherance of action. This is appreciable to an extent as it has not been a long time, since we humans have developed a cyber realm. However, the best setback that IHL and IHRL duly suffer is the absence of a civil approach. We can hope that within a reasonable expected time, this may happen. Hence, if there is a vacation of something in the principles of IHL and IHRL furthered, then these can be the possible defects-

- A more civil and mature approach towards directing a sui generis legal instrument to innovate the reaches of International Law from its traditional realms, is absent;

[35] Budapest Convention, *ibid.*
[36] Seger, Alexander (October 20, 2016). *India and the Budapest Convention: Why not?* Retrieved from http://www.orfonline.org/expert-speaks/india-and-the-budapest-convention-why-not/.
[37] *Ibid.*
[38] *Ibid.*

- Deterrence and curb of legal control over a newly recognized realm of human instruments and the sovereigns, which can we state as state and non-state actors, such as in the case of cybersecurity law and the Budapest Convention duly signify that cyber realm needs more interactable approach;
- Cybersecurity and cybercrime laws do address the outwardly concerns of the IHL; it is not sufficing either; instead we need a cogent surface of International Humanitarian Law, which is beyond the limits and purview of expression of Media Law;

A CRITICAL ANALYSIS OF SOME GENEVA CONVENTIONS OF IHL AND THE HAGUE CONVENTIONS ON WAR

The nature of the 1949 Geneva Conventions signify a basic realm of International Humanitarian Law as a ground to determine the basic contingencies of war, where the 1951 Geneva Convention on Status of Refugees is a wider but curatively specific insight of IHL on refugees and various other principle related to them. The main reason for international humanitarian law in general, and the Geneva Conventions in particular, is to put a limit to barbarity in an extreme situation like armed conflict. It is recognized, then, by all that even wars must have limits. The limits that must be applied are essentially in the Geneva Conventions plus other treaties of international humanitarian law.[39] International humanitarian law is applicable whenever a situation of violence reaches the level of armed conflict. The underlying causes of the armed conflict have no bearing on the application of IHL. However, alongside with a[40] re-examination of established tenets of ius ad bellum, there seems also to be a questioning of the basic principle that whenever armed conflict does occur, it is governed by IHL (ius in bello). Invocation of the justness of the resort to armed force, particularly in the "war against terrorism", has not infrequently served as a justification for denying the applicability of the full range of international humanitarian law norms in situations where that body of rules was undoubtedly applicable[41]. Here, the so-caused applicability justifies Under humanitarian law applicable in international armed conflicts, civilians enjoy immunity from attack "unless and for such time as they take a direct part in hostilities".[42] However, the causative interference in hostilities exist as a very

[39] (August 12, 2009 12:24 GMT). *Sixty Years Later, How Relevant Are the Geneva Conventions?* Retrieved from https://www.rferl.org/a/Sixty_Years_Later_How_Relevant_Are_The_Geneva_Conventions/1798177.html.

[40] ICRC, (2003*). International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, 28th International Conference of the Red Cross and Red Crescent*, 03/IC/09. Retrieved from https://www.icrc.org/eng/assets/files/other/ihlcontemp_armedconflicts_final_ang.pdf, p. 8. [Hereafter ICRC].

[41] ICRC, *ibid*.

[42] ICRC, *ibid*, p. 9, *Additional Protocol I*, article 51 (3).

limited conception in International Law, which seems akin to what NATO did via invoking the Article 5 of their treaty in case of Estonia. Thus, this is understandable that liabilities and responsibilities enshrined in IHL on human and non-human instruments is no lucid but traditionally confined such that when a newer realm of human concurrence comes into discovery, it becomes so limited. In order to spare civilians and civilian property as much as possible from the effects of war, international humanitarian law prohibits disproportionate attacks. A disproportionate attack is defined as "an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[43] The disproportion between, on the one hand, civilian losses and damage caused and, on the other, the military advantage anticipated, raises a delicate problem: in some situations there will be no room for doubt, while in others there may be reason for hesitation. In such complex situations the interests of the civilian population should prevail. It should be kept in mind that international humanitarian law requires that constant care be taken to spare the civilian population, civilians and civilian objects. It must not be forgotten that even attacks that might be lawful, i.e. conform to the proportionality rule and other legal principles, nevertheless provoke enormous civilian suffering.[44] History has provided numerous examples of governments that publicly supported the protective provisions, but conducted gross violations on the battlefield in order to meet military objectives, with little documentation to prove their disregard for the Geneva and Hague conventions.[45] Same is the causative issue with cybersecurity and cybercrime laws, where the objective of International Humanitarian Law can be diminished and demeaned, which is unjustifiable. This is really not done as it does not provide a sui generis solution to a problem but enhances more complicated realms of human cum cyber worlds. In case of the 1951 Geneva Convention on Status of Refugees, there is present arguably the principle of non-refoulment, as provided for in Article 33. It states that all persons should enjoy the right not to be deported to a country where they may be subjected to persecution[4647], as the cornerstone of the convention. However, the basic principles of non-refoulment and of temporary refuge are customary in nature[48], it is

[43] ICRC, *ibid*, p. 12.
[44] ICRC, *ibid*.
[45] Anderson, Major Randall G. (5 June 1998). *A Historical Analysis of the Geneva And Hague Conventions and Their Protection of Military Medical Personnel, Facilities, and Transport During World War I.* Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a350093.pdf, 93-94.
[46] For more information on this principle and what it entails, see Weissbrodt, David S, The Human Rights of Non-citizens (OUP 2008), Chapter 6.
[47] Khan, Azfer Ali (2016). *Can International Law Manage Refugee Crises?* Retrieved from http://www.law.ox.ac.uk/sites/files/oxlaw/field/field_docu-ment/4.pdf, p. 56. [Hereafter Azfer Ali].
[48] Azfer Ali, *ibid*, p. 57.

highly likely that such obligations will be erga omnes. The application of such obligations varies, since it depends on the political will of States to take positive steps to enforce measures. Although it is particularly effective in isolated situations, it has yet to apply in a meaningful manner if a large number of States are potentially in breach, as is the case in the current context. This differs from specific regional enforcement, such as an obligation to respect the rights of refugees articulated in the ECHR or 1969 Convention on the Organization of African Unity (hereafter 'the OAU Convention')[4950] Henceforth, the impending perversion of the customary international law defeats the basic realms of IHL such as such Geneva Conventions in general. It is thus required that the matter of interests is curtailed in a way to provide optimal deterrence to the international legal personalities such as the states.

The innovative legal positions subsequently adopted to undertake military operations in Afghanistan and Iraq reflected this realist approach and have, not surprisingly, been subject to intense and unprecedented popular commentary[51]. A critical factor in the acceptance and incorporation of a new claim into the corpus of international law is whether it serves the common interests of the aggregate of actors. Thus, the responsibility of the international lawyer here is to assess innovative claims carefully for their contribution, in present and projected contexts, to the essential goals of law.[52] That is how the utility of Hague Conventions is adjudged is considered for subjected consideration. In modern international law, a doctrine-such as the Brezhnev, Carter, and Reagan doctrines-consists of a formal and credible statement by a significant international actor of a firm policy and the resolve to implement it upon certain contingencies. Doctrines are positioned at the interface of law and power. They are not based on a general right that is theoretically available to other states. By their nature, they constitute a demand for an exception. Not all doctrines conform with existing international law, but doctrines do contribute to minimum order by stabilizing the expectations of all actors as to the consequences of certain types of action and thus aid in avoiding adventures and mistakes.[53] "It must be that, in order to meet the legal requirement that a military target may not be attacked if collateral

[49] Organization of African Unity (OAU), *Convention Governing the Specific Aspects of Refugee Problems in*
Africa (adopted 10 September 1969) 1001 U.N.T.S. 45.
[50] Azfer Ali, *ibid* 49, p. 57.
[51] Stephens, Dale; Lewis, Michael W; (May 2005). *The Law of Armed Conflict — A Contemporary Critique*, Volume 6, Issue 1, 55-85. Retrieved from https://search.informit.com.au/documentSummary;dn=045122777410391;res=IELHSS ISSN: 1444-8602. [Hereafter Stephens et. al]. Please refer to- Reisman, W. Michael, *Assessing Claims to Revise the Laws of War" (2003). Faculty Scholarship Series. Paper 1008*. Retrieved from http://digitalcommons.law.yale.edu/fss_papers/1008, 82, 90. [Hereafter Reisman].
[52] Reisman, *supra* note, p. 89.
[53] Reisman, *supra* note 52, p. 90.

civilian casualties would be excessive in relation to the military advantage, the 'military advantage' must indeed be one related to the very survival of a State or the avoidance of infliction (whether by nuclear or other weapons of mass destruction) of vast and severe suffering on its own population; and that no other method of eliminating this military target be available[54]" in the words of Judge Higgins in the 1996 *Nuclear Weapons Advisory Opinion*[55] by the ICJ Here, this is logical because it provides a reference for measuring what is proportionate, for example, the loss of a nation or its people, though it runs counter to the mutually re-enforcing levels of constraint that Greenwood envisages[56]. Thus, Judge Higgins would permit legitimate incidental injury of large parts of civilian populations of the aggressor state in some circumstances, provided the nuclear target within the aggressor state was a military one and that massive loss within the victim state was threatened. Within such a paradigm, the level of constraint anticipated by Greenwood by advocating compliance with the tactical limitations of the jus in bello actually becomes a mechanism of licence, permitting a broader canvass to assess the 'concrete and direct military advantage anticipated' within the terms of[57] article 51 of Additional Protocol I[58]. Even the principle of proportionality necessarily requires that 'value judgments' should be made as to the respective worth of attaining military objectives against the cost of securing such an objective.[59] It is not surprising that France, a country committed to an uncommon degree

[54] *Nuclear Weapons Advisory Opinion* [1996] ICJ Rep 226, 238 (Dissenting Opinion of Judge Higgins). [Hereafter Nuclear Weapons].

[55] Nuclear Weapons, *supra* note 55.

[56] Stephens et. al, *ibid*, p. 67.

[57] Stephens et. al, *ibid*, p. 67.

[58] Noted to: *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts*, opened for signature 8 June 1977, 1125 UNTS 3 (entered into force 7 December 1978) ('*Additional Protocol I*'); *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts*, opened for signature 8 June 1977, 1125 UNTS 609 (entered into force 7 December 1978) ('*Additional Protocol II*') (collectively '*Additional Protocols*').

Article 51(5) states: *Among others, the following types of attacks are to be considered as indiscriminate …*

(b) an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.

[59] Schmitt, Michael (1998). *The Principle of Discrimination in 21st Century Warfare*, Yale Human Rights and Development Law Journal, Volume 2, Issue 1. Retrieved from http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1010&context=yhrdlj, p. 143, 170; Please refer to generally Joan Fitzpatrick, Speaking Law to Power: The War against Terrorism and Human Rights (European Journal of International Law: 2003) Volume 14, Issue 2, p. 241; Heymann, Philip (2003). *Terrorism, Freedom and Security: Winning Without War; Jordan Paust, 'War and Enemy Status after 9/11: Attacks on the Laws of War'*, Yale Journal of International Law, Volume 28, Issue 2, p. 325.

to the idea of dissuasion, has designated that it is not acceding to 1977 Geneva Protocol I because of "the lack of consensus among the signatory states of Protocol I as to the exact meaning of the obligations they have undertaken so far as deterrence is concerned."[60] This implies the remnants of vague manifestations of those international principles, which must be tested in the light of realism, which shows how International Humanitarian Law and Conventions on War deal with the traditional aspect of judgemental degree.

Hence, a mixed analysis of the Geneva and Hague Conventions can make us understand the following concluding points for adequate consideration-

- Both the conventions are still traditionalized that the scope of IHL needs revisions;
- Both the conventions share the same idea of traditionalized perversion in case of cybercrime and cybersecurity laws of the International Community;
- Both the conventions are incompetent to guide International Law for the formation of a synthetic jurisprudence and law for cyber realms other than of criminal intent and purview;
- The Hague Conventions have been overlooked by the International Court of Justice, which is due to the limitations of the Statute itself, but the Court must have adequately intervened and clarified the whole paradigm of the concerned as it did in the *Nuclear Weapons*[61] opinion of 1996;

INTERNATIONAL LAW FOR CYBER PRIVACY AND CIVIL CYBER REALMS: A QUESTION

It is not impossible to expect a cogent manifestation of International Law into a better and mature cyber law. However, the steps or reforms are not that easy. Thus, if we really require such legal jurisprudence and instruments for the International Community, we must trace the basic baseline for the insertion of an International Legal Personality into the requirement of the realm we need.

International Legal Personality (ILR) into Cyber Realm

All that can be said is that an entity of a type recognized by customary law as *capable* of possessing rights and duties and of bringing and being subjected to international claims is a legal person[62]. Generally, states and organizations represent as the so-called ILR into its

[60] See, e.g., (1988), DIETRICH SCHINDLER & JIRI TOMAN, THE LAWS OF ARMED CONFLICTS: A COLLECTION OF CONVENTIONS, RESOLUTIONS AND OTHER DOCUMENTS.
[61] Nuclear Weapons, *supra* note 55.
[62] Crawford, *ibid*, p. 115.

defined specificity as in case of *Reparation for Injuries*[63], when the ICJ had recognized in case of an international organization. Now, when it comes to basic human instruments other than NGOs, State Actors and Non-State Actors, it must be regarded that individuals, to the matter of restricted concerns and interests of the regarding entity concerned, must be granted a temporary status whenever required in consonance with the doctrine of *erga omnes* and the Customary International Law under limited repercussions adjudged. Moreover, we must understand that there must be these 3 imperative traits of such cyber ILRs-

- That their representation is only recognizable, when the principles of sovereign equality (for States), *competences d'attribution* (International Organizations) and the individual principle of neutrality of human rights (for Human Instruments via IHRL) with due neutrality towards subjective representation of a human being and its privacy.
- All the representations must be recognized in a phasing and phase-based concerned responsibility enshrined in the principles of International Law with a more realist and modern approach. The approach can turn out with majority of concerns. However, we must understand that an uncontrollable realm of humanity may take some adequate time to affirm a global and social equilibrium.
- Privacy, as a concept of civil rights, must emerge from its sui generis basics for due consideration and pure law to emerge into a more better connective realm of mankind to support cyber representation and realms into phasing matter of observance. Now, the term 'phasing' suggests the limitation of expression and communication and the information, which is concerned to be introduced or ought to be intervened. This is the idea of Privacy, where there is neither 100 percent nullity of intervention nor the totality of exposure or revelation, to be more mature.

RECOGNITION MECHANISM AND PRINCIPLES OF INTERNATIONAL LAW

International Law needs to first clarify with a clear demarcation of the concept of Privacy because a universal consideration of Privacy is the key to concerned effort towards recognizing the representation and participation of every International Legal Personality, where sovereignty must become a case of optimal responsibility and *sui generis* widening application of all its intrinsic and local cum extrinsic reliance, accountabilities and relations, whether reshaped or recognized by Customary International Law or *jus cogens* or any *Vienna Convention* concerned with the ad hoc purpose of origination beyond the vicinities and delicacies of relevance of representation, participation and recognition.

[63] Reparation for injuries suffered in the service of the Nations, Advisory Opinion, [1949] ICJ Rep 174, ICGJ 232 (ICJ 1949), 11th April 1949, International Court of Justice [ICJ]

This is not an absolute assertion so put. It is the *sui generis* viewpoint, which has its own matter of employability that it may be able to reach with time.

CONCLUSIONS

International Humanitarian Law is a pervading concept, which develops with a certain matter of insistence and resilience towards civil correspondence of cyber realms. The traditional reliance and basics of the Geneva and Hague Conventions do not bring forward a better set of cogence in the matter of suited directions to form a general international legal instrument for cyber realms. Thus, it generally ascribes that cyber realms are turbulent; but they must be dealt under the concerns of IHL and IHRL with phasing representations and recognitions.

