CAN EXISTING INTERNATIONAL LAW REGULATIONS AND CYBER OPERATIONS MEET AT A JUNCTION?

Authored by: Vaibhav Sharma
Student
B.A.LL.B
University of Rajasthan, Jaipur, India

Abstract: The world of cyber space is full of potential, constructive and destructive. Lately, significant security concerns have arisen owing to exploitation of cyberspace for strategic development and diplomatic benefit by the States in international community. Last decades have witnessed not only inter-State cyber attacks but also conduction of cyber operations by non-State actors. Abuse of cyber realm becomes notorious when coupled with armed conflict. It serves multiple purposes for the attacker which includes, but is not limited to, psychological warfare, espionage, data manipulation and corruption, network breakdown and damaging infrastructure.

Such instances have caused scientists and scholars to throw light on this subject. Recent developments like release of Tallinn Manual and productive literature by US Naval War College have resulted in increased scholarships on the topic. However, no comprehensive and authoritative legal framework is present which could regulate the cyber operations. Attempts have been made by various researchers and experts to interpret provisions of existing international law in a manner which facilitates its application on cyberspace. This paper reviews all such attempts and analyses the various deliberations. This paper also examines the threat of cyberwarfare and the challenges which international laws might face. Lastly, the paper concludes with bringing focus on issues which remain unresolved and require insight of experts, both legal and scientific.

***Keywords*: International law and cyberspace, cyberwarfare, challenges in cyber security, international cyber law**

1. Introduction

21st century is faced with a serious challenge of existing and potential threats in the sphere of cyberspace. It may cause substantial damage to international and national security. Information and communication technologies (hereinafter referred as "ICTs") have unique attributes which make difficult for this threat to be addressed comprehensively. The nature of ICTs is peculiar in the sense that it is inherently neither civil nor military. Its purpose depends wholly on the motives of the user. Emanating from unpredictable sources, they cause disruptions targeting individuals, governments, businesses and national infrastructure alike.

With development of ICTs as tools of warfare and intelligence cyberspace is the new battlefield with new weapons. Lack of common understanding regarding acceptable State behavior in this new domain creates instability and misperception in international relations. Meddling through cyber tools in States' internal affairs has left the States on guard defending their military as well as civil societies from foreign intervention.

The Titan Rain attacks[1] in year 2003 (which gave hackers access to sensitive US defense information), cyber attacks on Estonia[2] in year 2007 (affecting its banks, ministries, government departments, news, broadcasters and even Estonian Parliament), attacks on Georgia[3] in year 2008 during armed conflict with

[1] James A. Lewis, *Computer Espionage, Titan Rain and China*, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES – TECHNOLOGY AND PUBLIC POLICY PROGRAM (Dec., 2005), *available at* http://cybercampaigns.net/wp-content/uploads/2013/05/Titan-Rain-Moonlight-Maze.pdf (Last visited: Mar. 28, 2019).
[2] Elizabeth Schulze, *When this country faced a suspected Russian Cyberattack – it took some big steps to stop another*, CNBC (September 21, 2018), *available at* https://www.cnbc.com/2018/09/21/when-this-country-faced-a-suspected-russian-cyberattack--it-took-some-big-steps-to-stop-another.html (Last visited Mar. 25, 2019).
[3] See, Captain Paulo Shakarian, *The 2008 Russian Cyber Campaign Against Georigia*, MILITARY REVIEW, pg 63, 63-68 (Nov.-Dec. 2011).

Russia and Stuxnet virus attack[4] in 2009-2010 (believed to be created by US-Israel against Iranian Nuclear Program) are some of the major instances of inter-State cyberwarfare. Indications of attempts by terrorists to compromise ICT infrastructure have also been observed which may intensify in near future. All this compels us to dive deep into international law jurisprudence and technological advancements to erect defensive and offensive frameworks.

States have already initiated increased strategy and policy making to defend and attack in cyberspace. For example, the US' Department of Defense (DOD) established Cyber Command which has undertook responsibility for defending DOD information networks. It is "[P]repared to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to [US'] adversaries."[5]

It is significant for international law not to leave this space unregulated and letting it end with massive interferences and warfare. Many scholars and academia of international law studies have put forward concerns in this matter. Computer scientists also share significant concern in this sphere because of the huge utility of the cyber tech in contemporary times. Enormous literature has been produced collectively by cyber and legal experts sharing their viewpoints and concerns on the subject. It is because of the combined efforts of both fraternities that we are able to initiate logical discussions to appropriately solve the problems and complications of the cyber space to some extent. While it would be wrong to state that we have overcome all the difficulties and are prepared to tackle singlehandedly all future disruptions, we have indeed come a long way and have a further long road to go.

Since cyber warfare is relatively new concept and no express provisions are available under international law for its regulation, analogies can be drawn between conventional warfare and cyberwarfare incorporating certain legal provisions of the former to regard the latter. Although such attempts have been criticized pertaining to their 'incomparable' nature, they are worth examining and hence are discussed ahead. They provide us with legal solutions to the present and potential future problems. But before reaching to the ways of tackling cyberwarfare it is necessary to discuss some important definitions in this context not only to be able to comprehend both technical and legal aspects of this domain, but also to take command over participation solution-deriving process of the academia.

2. General Concepts

(Cyberspace and International Law for Use of Force and Humanitarian Law)

2.1.Cyber realm

2.1.1. Cyberspace

Different attempts have been made to define cyberspace. In 2003, The US Government's National Strategy to Secure Cyberspace defined cyberspace as "… composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fibre optic cables that allow our critical infrastructures to work".[6] The US military defined it as:

> "*Global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." It had also described it as fifth*

[4] For further reading, see Ellen Nakashima and Joby Warrick, *Stuxnet was work of U.S. and Israeli experts, officials say*, THE WASHINGTON POST (June 02, 2012), *available at* https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?noredirect=on&utm_term=.93580f2ff6a2 (Last visited Mar. 20, 2019).

[5] US Department of Defense, Cyber Command Fact Sheet, (May 25, 2010), *available at* https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-038.pdf (Last visited Mar. 21, 2019).

[6] See, *The National Strategy to Secure Cyberspace*, THE WHITE HOUSE, WASHINGTON DC, pg vii, (February, 2003) *available at* https://www.energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyberspace.pdf (Last visited Mar. 15, 2019).

> *domain of warfare.*[7] *Later on, its definition evolved to "the interdependent network of information, technology infrastructures that includes the Internet, telecommunications networks, computers, information or communication systems, networks, and embedded processors and controllers in critical industries.*"[8]

A US-Russia project on cyberspace also made attempt to define cyberspace, the common meeting points were less though because of no Russian equivalent of cyber. It described cyberspace as "electronic medium through which information is created, transmitted, received, stored, processed, and deleted." [9]

India, on the other hand, subscribed to the definition of International Standards Organization Guidelines for Cybersecurity released in 2012 and did not attempt to create a definition of its own. It stated cyberspace as "a complex environment consisting of interactions between people, software services supported by worldwide distribution of information and communication technology."[10]

2.1.2. Cybersecurity

Often cybersecurity and data security are used synonymously in legal circles. However, it must be noted that although data security constitutes a significant part of cybersecurity, it is not the only part. Cybersecurity involves not only data protection, but also protection of systems and networks of the public and private sector. For example, the cyberattack on Sony[11] not only hampered the information interests of the company but also offered severe obstruction to the routine business operations due to unavailability of its systems and networks. Cyber attacks are comprehensive attacks on cybersecurity and not only against information/data security.

According to cyber professionals, the aim of cybersecurity is based on Confidentiality ("the prevention of unauthorized disclosure of information."), Integrity ("the guarantee that the message that is sent is the same as the message received and that the message is not altered in transit.") and Availability ("the guarantee that information will be available to the consumer in a timely and uninterrupted manner when it is needed regardless of [the] location of the user") (CIA triad).[12]

On Cybersecurity the International Standards Organization states:

> "*The devices and connected networks that have supported Cyberspace have multiple owners, each with their own business, operational and regulatory concerns. The different focus placed by each organization and provider in Cyberspace on relevant security domains where little or no input is taken from another organization or provider has resulted in a fragmented state of security for Cyberspace.*"[13]

It is defined by International Telecommunication Union as:

---

[7] Ronald R. Fogleman, *Information Operations: The Fifth Dimension of Warfare*, Remarks delivered by Air Force Chief of Staff to the Armed Forces Communications-Electronics Association, USA, Washington DC, April 25, 1995, (Nov. 12, 2015), *available at* http://www.iwar.org.uk/iwar/resources/5th-dimension/iw.htm (Last visited: Mar. 22, 2019).
[8] *The Definition of Cyberspace*, Deputy Secretary of Defense Memorandum, (May 12, 2008).
[9] RAUSCHER KARL FREDERICK, AND VALERY YASHCHENKO, RUSSIA-US BILATERAL ON CYBER SECURITY: CRITICAL TERMINOLOGY FOUNDATIONS, pg 16 (2011).
[10] "India: National Cyber Security Policy 2013", Department of Electronics and Information Technology, Delhi: n.p., 2013, Web, (Nov. 14, 2015).
[11] Amanda Hess, *Inside the Sony Hack*, SLATE (Nov. 22, 2015, 8:25 PM), *available at* http://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html (Last visited Mar. 26, 2019).
[12] See Ashish Agarwal & Aparna Agarwal, *The Security Risks Associated with Cloud Computing*, 1 INT'L J. COMPUTER APPLICATIONS ENGINEERING SCI. (SPECIAL ISSUE ON CNS) pg 257, 257–58 (2011).
[13] "Information Technology—Security Techniques—Guidelines for Cybersecurity", International Standards Organisation, 2012, Web, (Mar. 28, 2019), *available at* https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en> (Last visited: Mar. 19, 2019).

> "*... the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:*
>
> - *Availability*
> - *Integrity, which may include authenticity and non-repudiation*
> - *Confidentiality"*[14]

The US Department of Homeland Security defines the same as:

> *"Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.*"[15]

Cyberspace and cybersecurity, however, are not self-contained concepts. To bring around it a comprehensive framework, understanding of Critical Infrastructure (CI), cyber deterrence, cyber weapons and other essential components are necessary.

2.1.3. Jeff Kessoff's definition of 'cybersecurity law'

Various statutes and policies lay down definitions of cybersecurity to meet the regulating requirements. But can and should 'cybersecurity laws' be defined? Jeff Kessoff, a researcher, argues in affirmative.[16] According to him, while one might argue about futility of attempting such definition, the definition will create "a broad taxonomy for policymakers and courts as they develop statutes, regulations, and court rulings that shape cybersecurity for generations to come."[17] It would suggest the subjects of the law, protective methods to secure the subjects and reasoning behind such cybersecurity.

When policy makers discuss cybersecurity, they are often not on the same page. He seems to believe that introduction of 'cyber law' definition would create a common playground for policy-debates. For example, while dealing with cybersecurity one might use it synonymously with information security. This would neglect the potential danger of cyberattack on connected automobile causing a highway crash or remotely controlling factory's systems causing explosions and injuries. Comprehensive framework and attention on cybersecurity becomes even more necessary in the era of Internet of Things where all devices ranging from medical to kitchen and air-conditioning to industrial equipments are connected to Internet. Hackers can manage to disable and manipulate thousands or more networks or cause vehicles to accelerate hundred kmph to crash into crowded spaces!

Answering the five questions of what, where, how, when and why are we securing [in cyberspace], the proposed definition is: "Cybersecurity law promotes the confidentiality, integrity, and availability of public

[14] "Definition of Cybersecurity", International Telecommunication Union, *available at* https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (Last visited Mar 11, 2019).
[15] "Explore Terms: A Glossary of Common Cybersecurity Terminology", National Initiative for Cybersecurity Careers and Studies, US Department of Homeland Security, *available at* http://niccs.us-cert.gov/glossary (Last visited Mar. 10, 2019).
[16] Jeff Kessoff, *Defining Cybersecurity Law*, 103 IOWA LAR REVIEW, pg 985-1030 (2018).
[17] *Id*., pg 989.

and private information, systems, and networks, through the use of forward-looking regulations and incentives, with the goal of protecting individual rights and privacy, economic interests, and national security."[18]

However, the proposed definition requires correction at two places – firstly, where it limits the law to use "incentives" and secondly, where it lays down exhaustive goals list for which the cyber law framework is to be created.

A law can use either coercion or incentives while dealing with a crisis. The option between two depends on what is suitable for the subjects of the law. There might be instances where incentives fail and need of coercion arises.

Also, the exclusive goals of law mentioned are insufficient. Individual rights, privacy, economic interests and national security are indeed essential, but such definition restricts the State to enact or enforce laws for a purpose other than protecting these. What if foreign intervention is done and it does not manipulate or hampers any of the above-mentioned four criterions? Should not the State be allowed to discretionally act exercising its sovereign power against a cyber movement emanating from a foreign source?

2.2.International Law for Use of Force and Humanitarian Law

International community has come a long way regulating wars and use of force. The purpose of United Nations declared in Article 1(1)[19] is:

> "*Maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace.*"

2.2.1. Force

Article 2(4) of the Charter declares that "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." The declaration uses word "force" instead of "war" and thus prohibits mixed actions which although against the spirit of peace, might not technically constitute act of war.

The 1970 Declaration on Principles of International Law elaborated and systematically analyzed Article 2(4). First, crimes against peace are constituted by wars of aggression for which there is responsibility under international law; secondly, to violate international frontiers or to solve international disputes States must not threaten or use force; thirdly, States are under the duty to refrain from acts of reprisal involving the use of force; fourthly, no force must be used by State to deprive people of their right to self-determination and independence; and fifthly, States must refrain from organizing, instigating, assisting or participating in the acts of civil strife or terrorist acts in another state and must not encourage the formation of armed bands for incursion into another State's territory.

While no amendment has taken place to Article 2(4), there are views considering whether the term 'force' includes forces beyond armed forces such as economic ones, for example, imposition of boycotts or embargoes against a State.[20]

The 1970 Declaration on Principles of International Law mentions duty as "duty on States to refrain… from military, political economic or any other form of coercion aimed against the political independence or

[18] *Supra* Note 16, pg 1010.
[19] The Charter of United Nations, Article 1(1)
[20] MALCOLM N SHAW, INTERNATIONAL LAW, pg 815 (7th Edition 2016).

territorial integrity of any state." The Charter of Economic Rights and Duties of States approved by the General Assembly in 1974 specified that "no state may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights."[21]

However, restraint on waging war is not exclusively imposed by the Public International Law. Some States like Germany and Japan are self-restricted by their own Constitution for resorting to use of force.[22]

For the force to be legitimate, it must be one within the accepted exceptions, essentially the right to self-defense or enforcement action mandated by the United Nations Security Council. The Charter provides with two related circumstances wherein the prohibition does not apply. First, measures authorized by Security Council acting under Chapter VII of the Charter; second, force exercised as right of individual or collective self-defence, as recognized under Article 51 of the Charter. A further possible exception is the use of force to avert humanitarian catastrophe.

Exemptions are also sought for humanitarian intervention based on the real concern of inadequate response against contemporary global security threats such as transnational terrorism, proliferation of weapons of mass destruction and humanitarian crises such as in Rwanda, Syria, etc.[23] Requirement of such interventions has led to evolution of a new legal viewpoint seeking construction of unilateral right to use force preventively or retrospective authorization by the Security Council for the use of force.

Nevertheless, observing instances where use of force has been carried out without prior authorization by the Security Council, not for self-defence and with intervention in other States, it seems it has been rightly suggested that the rules of international law on the use of force are dead.[24] However, the General Assembly of the United Nations at the level of Heads of State and Government reaffirmed "that the relevant provisions of the Charter are sufficient to address the full range of threats to international peace and security. We further reaffirm the authority of the Security Council to mandate coercive action to maintain and restore international peace and security. We stress the importance of acting in accordance with the purposes and principles of the Charter".[25]

2.2.2. The right to self-defence

Article 51 of the UN Charter provides:

> "*Nothing in the present 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. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security*."

The opening phrase of this Article specifies "nothing in the present Charter shall impair the inherent right of… self defence". This means that there existed a right to self-defence in customary international law over and above the UN Charter. For a force to be a valid act of self-defence under international customary law, it must conform to *Caroline*[26] formula as set down by the US in 1837. The US Secretary of State laid down

[21] Charter of Economic Rights and Duties of States, Article 32.
[22] Michael Wood, *International Law and Use of Force: What Happens in Practice*, 53 INDIAN LAW JOURNAL, pg 345, 346 (2013).
[23] For further reading, see Global Trends – Forced Displacements in 2017, UNHRC, *available at* https://www.unhcr.org/5b27be547.pdf (Last visited Mar. 29, 2019)
[24] M. J. Glennon, Why the Security Council Failed, FOREIGN AFFAIRS, (May/June 2003), *available at* https://www.foreignaffairs.com/articles/iraq/2003-05-01/why-security-council-failed (Last visited Mar. 29, 2019).
[25] General Assembly res. 60/1, ¶ 79. This followed similar statements by the Secretary- General's High-level Panel in its report *A More Secure World: Our Shared Responsibility* (A/59/565), ¶ 185-203; and by the Secretary-General in his report *In Larger Freedom: Towards Development, Security and Human Rights for All* (A/59/2005), ¶ 122-126.
[26] *The Caroline v. United States*, 11 U.S. 496 (1813).

the essentials of self defence. It required that a response in self defence must be based on "existence of necessity, instant, overwhelming, leaving no choice of means, and no moment for deliberation."[27] It also necessitated that the act must not be unreasonable or excessive. This principle was accepted by the British Government and is accepted as part of customary international law.[28]

Right to anticipatory or pre-emptive self defence exists. The most recent example of such right is India's pre-emptive strike in Pakistan wherein biggest training camp of JeM in Balakot was struck, leading to elimination of "a very large number of JeM terrorists, senior commanders and group of Jihadis who were being trained for fiyadeen action…"[29] However, this right of self defence is limited by principles of necessity and proportionality.

2.2.3. War and International Humanitarian Law

International law not only prescribes laws governing resort to force (*jus ad bellum*), but also laws to regulate conduct of hostilities (*jus in bello*). Earlier, this law was called law of war and later, law of armed conflicts. Today, it is known as international humanitarian law. It seeks to extend protection to wide range of persons. It draws distinction between combatants and those who are not involved in actual hostilities.

The rule of International Humanitarian Law (IHL) applies to armed conflicts; this makes declaration of war unnecessary for this code to apply. In any of the conventions or protocols, "armed conflict" has not been defined. It has been stated by the Appeals Chamber of the International Criminal Tribunal for the former Yugoslavia in *Tadic* case[30]:

> "*International Humanitarian Law applies from the initiation of such armed conflicts and extends beyond the cessation of hostilities until a general conclusion of peace is reached; or, in the case of internal conflicts, a peaceful settlement is achieved. Until that moment, international humanitarian law continues to apply in the whole territory of the warring states or, in case of internal conflicts, the whole territory under the control of a party, whether or not actual combatant takes place.*"[31]

The Geneva convention of 1864 concerns itself with the wounded and sick on land and emphasises that the members of armed forces and militias shall be respected and protected in all circumstances. They assert for humane treatment by the party to conflict into whose power they have fallen. For example, torture and biological experimentation is forbidden. They are not to be left deliberately without medical assistance and care.[32] Belligerents, if wounded and sick are also to be treated as prisoners of war.[33]

The Geneva Convention of 1906 concerns itself with the condition of wounded, sick and shipwrecked members of armed forces at sea. It is similar to the first convention in multiple aspects. It also provides that under no circumstances hospital ships are to be attacked or captured.[34] These provisions were reaffirmed and supplemented by Protocol I, 1977, Parts I and II.

The Geneva Convention of 1929 is concerned with prisoners of war. It is a comprehensive code focussed on requirement of humane treatment in all circumstances. The Geneva Convention of 1949 deals with

---

[27] A Martyn, 'The Right of Self-Defence under International Law – the Response to the Terrorist Attacks of 11 September' (2002) Department of the Parliamentary Library Current Issues Brief, No 8, 10.
[28] *Supra* Note 20, pg 820 (7th Edition 2016).
[29] Statement by [Indian] Foreign Secretary on 26 February 2019 on the Strike on JeM training camp at Balakot (Feb. 26, 2019), *available at* https://mea.gov.in/Speeches-Statements.htm?dtl/31089/Statement+by+Foreign+Secretary+on+26+February+2019+on+the+Strike+on+JeM+training+camps+at+Balakot (Last visited Mar. 10, 2019).
[30] *Prosecutor v Tadic*, (IT-94-1-AR72) ICTY.
[31] *Id*., pg 488.
[32] Convention for the Amelioration of the Condition of the Wounded in Armies in the Field (Geneva, August 22, 1864), Article 12.
[33] *Id.*, Article 14.
[34] Geneva Convention For The Amelioration Of The Condition Of Wounded, Sick And Shipwrecked Members Of Armed Forces At Sea (August 12, 1949), Chapter III.

protection of civilians in the time of war. Protection of civilians in occupied territories is covered in Section III of Part III.

Under the IHL are provided protections to the sick and wounded, prisoners of war and civilians and occupations. In addition to the victims of armed conflicts, the law also regulates the conduct of military operations in a humanitarian fashion. For instance, Article 48 of Protocol I rules that distinction must be drawn between such population and combatants and between civilian and military objectives. Military objectives are also restricted to partial or complete destruction of those objects which by their nature, location, purpose or use will confer a military advantage.[35]

In referring to this principle, Judge Higgins noted that "even a legitimate target may not be attacked if the collateral civilian casualties would be disproportionate to the specific military gain from the attack."[36] Complications occur in context of dual-use objects such as bridges, roads and power stations which facilitate both civilian and military purposes.

Article 51[37] prohibits making civilians object of attack (as long as they do not take direct part in hostilities). Provision provides that no act or threat of violence with the primary purpose of creating terror among civilian population must be made. "Constant care" is also mandated during conduct of military populations to spare the civilian population and objects.[38]

Article 54 provides protection to cultural objects and places of worship. Protection is also conferred upon objects deemed indispensible to human survival such as foodstuffs, agricultural areas, drinking water installations, livestock, as far as they are not used as sustenance solely for armed forces.[39] Article 56 of the protocol prohibits attacks on installations storing dangerous forces such as nuclear stations.

Hague Conventions of 1899 and 1907 constitute second arm of the IHL. They plant restrictions on use of class of weaponries which conclude in immeasurable and unnecessary human suffering.

International Humanitarian Law is based on ensuring human dignity in the times when blatant disregard is paid to it. Human rights are concern more or less of all mankind. In today's times where fighting is no longer restrained to delimited battlefields, significant necessity has arisen for such regulations. However, although the conventions entitle people with certain rights, it is highly improbable that masses would be aware of existence of the same. And when the war breaks, it is generally too late for dissemination of knowledge.

3. Application Of Existing International Laws In Cyberwarfare

As per the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security's recommendation, the UN Charter and International Humanitarian Law are the only international laws relevant to cyberspace. Release of Tallinn manual on applicability of these laws to cyberspace has further aided focus on cyber war. It is a study on how existing international laws apply on cyberspace and cyberwarfare. It is characteristically academic and non-binding.

3.1. Use of Force and Right to Self Defence

The UN Charter contains provisions relevant to conflicts in cyber space. Article 1 of the Charter provides for maintenance of international peace and security, Article 2(4) for restraint on use of force. Article 51 protects the "inherent" right to self defence. Article 2(4) of the Charter states that "[All] members shall

[35] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) (June 8, 1977), Article 52(2).
[36] Dissenting Opinion, Legality of the Threat or Use of Nuclear Weapons, ICJ Reports, 1996, pg 226, 597.
[37] *Supra* Note 35, Article 51.
[38] *Supra* Note 35, Article 57.
[39] *Supra* Note 35, Article 54.

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."[40] The term "force" was kept ambiguous at the time of drafting Charter. International Court of Justice has stated that under the UN Charter, Article 2(4) and Article 51 apply to "any use of force, regardless of the weapons employed".[41] This statement is accurate reflection of international customary law.

Conventional weapons are classified and regulated on the grounds of their capabilities of destruction, killings and sufferings. Malwares, on the other hand, do not demonstrably kill. Destruction of properties by it is generally below the threshold of aggressive action.

Tallinn Manual states not all cyber operations can be classified as "force"[42] by giving example of instances concerning "non-destructive cyber psychological operations intended solely to undermine confidence in a government or economy." The only cyber operations classifiable as "use of force" are those which are conducted or otherwise attributable to State and rise to the level equivalent to an "armed attack"[43] in terms of scale and effects.[44]

The complication in this framework is that a large number of strategic cyber operations might get away with impunity. Damage to life and property during cyberwarfare is largely low in comparison to war waged with conventional weapons. Blood and human dignity are better preserved in the former case. It must be noted that the purpose of both wars differ. While one is aimed to cause destruction of life and property, another executes disorder targeting the CIA triad (Confidentiality, Integrity and Availability). Because of the distinction in their ends, laws must not be equally applied in both cases. Unequal stances ought to be treated unequally.

It is submitted that what constitutes use of force in the cyberspace must be evaluated not on the grounds of whether it constitutes "armed force" or not (as Tallinn Manual states), but in accordance with the proportional damage that it has caused to the information CIA triad and networking capacities of the system. Until the international legal framework develops a new model to deal strictly with the cyberspace, the existing laws can be used. But they cannot be applied without the mentioned discrimination.

It is necessary to pay attention to what is the Potential of Damage (PoD), that is the vastness and sensitivity of information or crucial character of the particular network of the targeted ecosystem. Consider a State (let's say State A) against which a ferocious cyber attack is done. 90% of its sensitive data is stored in and networking is completely through cyberspace; the State however did not suffer serious complications. Another State (let's say State B) has relatively less cyber networking ecosystem but suffered losses in considerable percentage of the networking system. Now if we consider both the cases we will rightly observe that State A had a greater PoD than State B, although the latter suffered losses. According to the existing international laws, the case of greater damage (and equivalent to "armed attack") would constitute "force". But it is submitted that it is the PoD that needs to be made ground for assessing whether cyber operation constitutes "force" or not. It may be argued that such a ground will result in counter-operations that would be of preemptory nature (since retaliations might be done prior to cause of any real damage). But it needs to be acknowledged that in the modern economies data and networks perpetuate lives, erasure of which is largely irreversible, unlike property and troops which can be resurrected (with some cost indeed).

The proposed principle of assessment based on PoD will also help in instituting considerable cyber deterrence by demotivating proliferation of cyber weapons to a large extent.

[40] Charter of the United Nations, Article 2(4).
[41] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, pg 226, ¶ 39.
[42] MICHAEL N. SCHMITT, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, Rule 11, commentary ¶ 3 (2013).
[43] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, pg 14., ¶ 191.
[44] *Supra* Note 42, Commentaries to Rule 11 (2013).

Tallinn Manual, however, seems to ignore PoD. For assessment of cyber force, Tallinn Manual suggests certain factors (non-exhaustive) which include severity, immediacy, invasiveness, directness, measurability of effects, military character, State involvement and presumptive legality.[45] Due attention to PoD, unfortunately, remains unpaid in this list.

If the principle of PoD is systematically applied, it will also fill the void which Tallinn Manual leaves by not allowing self-defence operations to the cyber attacks which although are not destructive, are psychologically undermining and irritating.

3.2.Sovereignty

Sovereignty is one of the foundational principles of international law and is considered a "basic constitutional doctrine of the law of nations."[46] It refers to "the collection of rights held by a state, first in its capacity as the entity entitled to exercise control over its territory and second in its capacity to act on the international plane, representing that territory and its people."[47] Sovereignty, in other words, can be understood as encompassing "the whole body of rights and attributes which a state possesses in its territory, to the exclusion of all other states, and also in its relation with other states."[48] Article 2(1) of the UN Charter states that "the [UN] organization is based on the principle of the sovereign equality of all its Members."

In different domains, the principle of sovereignty is unequally applicable. For example, airspace over a territory is strictly supervised and any unsought intrusion is considered as violation of international law. In reference to seas, on the other hand, transit through territorial sea of another state is permissible, but can constitute international law violation under certain conditions. In the case of space, objects in orbit and outer space (including above another State's territory) are beyond nation's territorial claim and can be exploited by all. But how sovereignty can be determined in cyberspace is a question faced by us. Unlike land, air, water and space, cyberspace is not a natural domain. It is a man's creation interlinking devices and data, suspended on servers and networking suspensions.

Attempts were made prior to Tallinn Manual to deal with sovereignty in cyberspace. The challenge, earlier, however, was not to check legality of whether State could violate another State's sovereignty by unaccepted intrusion, but to identify when cyber operations could do so. It was a preliminary step. In view of Tallinn Manual, no State can claim sovereignty over cyberspace per se, but only on cyber infrastructure located on its territory.[49] Regarding the consequences of such sovereignty, it states:

> "*First, that cyber infrastructure is subject to legal and regulatory control by the State. Second, the State's territorial sovereignty protects such cyber infrastructure. It does not matter whether it belongs to the government or to private entities or individuals, nor do the purposes it serves matter*."[50]

The view propounded in Tallinn Manual is correct and practicable. Cyberspace is an artificial domain. It is an abstract domain existing in servers and infrastructure which need to be located at certain lands, seas, air or space. We cannot establish exclusive control over this domain of a State because the data and networking essentials are ultimately grounded at fixed and concrete domain which can be either of the four domains (air, land, water and space).

If a cyber attack is launched against a State, it means operations have been carried out with an intention to conduct hostilities on the State's websites, data and networking tools. All these targets are rooted and arise from particular technical infrastructures. These infrastructures are located in State's territories. Henceforth, if an attack is done in the State's cyberspace, it equals attack on State's sovereignty. If a State intrudes

[45] *Supra* Note 42, Rule 11, Commentary ¶ 9 (2013).
[46] JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW pg 447 (8th ed. 2012).
[47] *Id*. pg 448.
[48] Corfu Channel (U.K. v. Alb.), Merits, 1949 ICJ REP. 4, 43 (Apr. 9) (individual opinion by Alvarez J.).
[49] *Supra* Note 42, Rule 1, Commentary ¶ 1 (2013).
[50] *Id*., Commentary ¶ 5.

another State's cyberspace and coerces its government by using cyber tools, it might constitute intervention[51] if such coercion is not otherwise permitted under the applicable provisions of international law.

3.3. International Humanitarian Law

The use of cyber operations in armed conflict can potentially have devastating humanitarian consequences. International Humanitarian Law (IHL), as discussed above, is the law to govern conduction of hostilities. It is derived mainly from two set of conventions – Hague and Geneva. While Hague Conventions of 1899 and 1907 plant restrictions on use of weaponries that conclude in immeasurable human suffering, Geneva Conventions extend protection to people who are not directly part of conduct of hostilities such as sick and wounded combatants, Prisoners of War (PoW), civilians, etc.

The derivation of International Humanitarian Law largely occurred after incidence of horrors of wars.[52] Law can offer no retrospective prevention of loss of life. It is therefore right to consider and regulate cyberwarfare in the present times instead of waiting for a cyber catastrophe to take place. At the time of formulation of such laws, cyberspace was not even at the horizon. No express provision of IHL, thus, regulates cyberwarfare.

However, as the Martens clause[53] states: "until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity and the requirements of the public conscience."[54] This position is supported by the International Law Commission, which has stated that "[the Martens Clause] ... provides that even in cases not covered by specific international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience."[55]

If cyber attacks take place during an ongoing armed conflict, laws of armed conflict are applied to cyberwarfare too, as happened in the case of Russia-Georgia conflict. In 2007, laws of armed conflict were not applied in cyberspace. But they were indeed applied in 2008 when the conduct of hostilities rose up to the point of 'armed conflict'.

The scope of application of IHL is limited to armed conflicts. This is also agreed upon in the Tallinn Manual[56] which states "a condition precedent to the application of the law of armed conflict is the existence of an armed conflict."

However, it is submitted that if protections and regulations are restricted exclusively to the cases of armed conflicts, it might leave void for the aggressors to overawe civilian populations in situations circumstancing otherwise. Cyberspace, unlike war frontiers, is a domain consisting heavy civilian segments. It is not predominated, although inclusive of, by militaries and diplomatic forces. Even minor operations against the networking essentials have the potential to stump civilian necessities massively. It is, therefore, required to widen the ambit with placement of blanket ban on any interference in civilian cyber space, whether during armed conflict or not. This concern is further incremented by the fact that while militaries may be well

[51] *Supra* Note 42, Rule 1, Commentary ¶ 7 (2013).
[52] Ayalew, Y. E. (2015). Cyber Warfare: A New Hullaballoo under International Humanitarian Law, 6 BEIJING LAW REVIEW, pg 209-223, *available at* http://dx.doi.org/10.4236/blr.2015.64021 (Last visited Mar. 28, 2019)
[53] The Clause was based upon and took its name from a declaration read by Professor von Martens, the Russian delegate at the Hague Peace Conferences 1899.
[54] Preamble to Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, July 29, 1899.
[55] UN Report of the International Law Commission on the Work of its Forty-sixth Session, May 2 – July 22, 1994, GAOR A/49/10, pg 317.
[56] *Supra* Note 42, Rule 20, Commentary ¶ 2 (2013).

prepared to resurrect their infrastructure and counter the attacks, the civilian infrastructure are not established in the first place with an eye on such international cyber warfare.

Tallinn Manual's another condition necessary for application of the IHL is internationality of the conflict.[57] For the conflict to be international, it must be between two or more States. What if the operations are carried out by State supported non-State actors? The International Group of Experts asserts that mere support for non-State actors does not transform the conflict into 'international armed conflict'.

The Tallinn Manual 2.0 provides an articulate account of how International Humanitarian Law can be applied into the cyberspace. It pays serious attention and comprehensively deals with multifarious aspects of a cyber war.

However, even if due regard is paid to the concepts of accountability and responsibility of criminal actions, certain challenges exist:

1. Human Shield tactic

International Humanitarian Law safeguards interests of civilians and non-combatants during the times of war. States may use civilian employees working in field of science and technology to develop cyber tools. During the process of such development, the protection to such civilians would come to an end as because of his "continuous function [that] involves the preparation, execution, or command of acts or operations amounting to direct participation in hostilities."[58] But once the person detaches himself from the job, he regains his protection. He, thus, possesses dual indivuality.

2. Unique attributes

Certain treaties and conventions aim to restrict proliferation and use of conventional weapons. Such treaties work by primarily classifying weapons on the basis of usage and destruction. Cyber weapons, on the other hand, cannot be classified in pigeon-holes. Similar regulations are difficult to enforce, even if one succeeds in enacting, because of unique attributes of cyber weapons such as dual use, ease of replicability, anonymity, lack of attributability, and difficulty in monitoring and verification.[59]

Conventional weapons destroy the target along with itself once hit. Cyber weapons, however, retain their individual existence. After release of a malware it can be redeveloped, innovated, reused and re-launched not only by the developer but by any person with technical expertise.

Owing to technological advancements, anonymous attacks are possible. While it is easy to attribute attacks by conventional weapons to a State or Non-State actors, it is difficult to ascertain from where the cyber operations have been convened. It is also possible for attackers to send data indicating remote area as source of attack instead of the real situation. This creates amplified risk of incorrect attribution.

Another complexity in dealing with cyber weapons is that after launch of a cyber attack, accurate surveillance of its effects is difficult and sometimes impossible. Monitoring of to what extent has operations succeeded is necessary not only to assess the damage, but also to cure the disabilities which might have occurred in systems besides countering the attack.

3. No strong demands by States to restrict cyber weapons

Although cyber operations have been conducted a large number of times, there is no strengthened demand to restrict development of cyber weapons. Countries which have been victims of cyber attacks should be in forefront on demanding restrictions and bans. But they are not. The major reason behind this silence is the

[57] *Supra* Note 42, Rule 22 (2013).
[58] Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian law*, INTERNATIONAL COMMITTEE OF THE RED CROSS, pg 853, *available at* https://www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf (Last visited Mar. 29, 2019).
[59] CHERIAN SAMUEL, MUNISH SHARMA, INDIA'S STRATEGIC OPTIONS IN A CHANGING CYBERSPACE, pg 6 (2019).

wish of developing cyber weapon capabilities themselves without being constricted by restrictions. The result of this ignorance is that cyber criminals gain unrestricted space to develop dangerous tools at their disposal and have playground to practice in absence of any international pressure.

States are focusing more on development of cyber warfare tools instead of placing common restrictions which are required to promote peace and cordiality. This has caused another race to begin in a way similar to nuclear weapon development and acquisition. It would be correct to predict that after certain extent of this development, arguments on methods to restrain this warfare will be initiated.

4. Network Dynamics

To understand the spread of infections on networks, improvised mathematical models are required. It is necessary to devise calculations which can determine what the eventual limits of destruction or infection are over a network affected by malware attack.[60] Structure of network has to be known in detail as prerequisite knowledge to devise coupled equations. Predictions are significant for cybersecurity. This is an issue largely ignored by the policy makers probably because of its scientific and technical character.

Network dynamics is essential to be considered in framing policies as it provides insight into working of networking systems. It is not assured, but developed mathematical calculations can aid policy makers into classification of cyber tools and weapons on the basis of their potential predictable mode of intrusion and followed disruption.

5. No common definition

The studies and projects revolving around cyber realm in international law have not yet arrived at particular set of definitions. When the scientists and scholars argue, they are never on the same page. Existence of fundamentally different definitions and intentions behind formulation of such definition obstructs lawyers and scientists to develop concepts which gain acceptance from all States. Every State has its different definition, if a definition at all. Also, more focus is put on explaining cyberspace; cyber warfare is still a little discussed topic.

The impact of establishing articulate terminologies is significant since on the occasion of forbidden cyber operations, the community of international lawyers can discuss the legality, consequences and post-operation effects while being on a common page. Moreover, if all States are able to agree upon a set of definitions, it would immensely help in determining *opinio juris* of the international community and therefore, will aid development of international law.

4. Conclusion

The general concepts relevant to legal development of cyberspace have been discussed. The international community is yet to arrive at common definitions on the subject. Although the nature of this domain is characteristically different from the other domains of land, water, air and space, highly influential accounts and opinions prevail as to how we can apply existing international laws to the new realm. Provisions relating to prohibition on use of force, self defence, armed conflict and humanitarian protection have been interpreted to engulf analogies found in cyberspace. Although voluminous content is available, no authoritative and binding conventions are formulated.

However, one major problem with the case of cyber realm's legal exposition is that the outlooks on policy are shared majorly by the States' militaries. Many influential researches on cyber domain and what regulations can undertake it are brainchild of army think tanks. This is problematic. It is because the militaries work on subjects with viewpoint of war and strategies to establish dominance and superiority. It extensively ignores the civil life concerned with the subject. The more exclusive focus is paid on cyber wars, more cyber wars might occur.

[60] Daniel M. Dunlavy, Bruce Hendrickson, and Tamara G. Kolda, *Mathematical Challenges In Cybersecurity*, SANDIA Report, pg. 7 (2009).

Since the outcomes are generally results of defence strategic brainstorming, countering them is considered essential by the adversaries. This is further generating unrelenting competitions in development of cyber weapons, tools and mechanisms. Using such military formulations might not result in good peace. Clausewitz described a very close, even unbreakable relationship between policy and war: "Subordinating the political point of view to the military would be absurd, for it is policy that creates war. Policy is the guiding intelligence and war only the instrument, not vice versa. No other possibility exists, then, than to subordinate the military point of view to the political."[61]

As agreed that cyber space is a wide domain, contemporary thoughts include more or less strategic viewpoints at international level where States essentially differ, instead of civil common playgrounds where the intentions are of cooperation and interdependence. Such research problems should be discussed by people who are interested more in development of the subject and less in its strategic exploitation.

Another problem that requires academic thought and research is the concern of establishing accountability and attribution. This concern is inclined more towards the field of scientists. As discussed above in the paper, technological advancements challenge the law by creating misinformation and misperception as to the source of cyber operations. This ends up making us unable to attribute attack to the correct source and thus unable in establishing accountability. If we are unable to do these necessities with precision, what use would be of law? In this sphere, law requires serious aid from science.

Another sphere where stress needs to be laid is in representation in the subject from Easter States as well. Currently, an overview over the present theoretical discussions bespeaks presence of imbalance in geo-political representations in cyber domain. To prevent controversies later, it is better not to miss the bus of evolution of cyber law. In the East, China, Russia and India are potential future players in the cyber domain.

Regulatory and legal debates will continue to revolve around the cyberspace for quite some time as technological developments have not stopped. Cyber law jurisprudence will settle itself when the technological advancements either complete or slow down considerably.

A giant revolution in cyber law jurisprudence might also take place once massive cyber operations between States result into catastrophe. All of the major war conventions have been formulated after the horrors of war, after realizing what wars can really lead to. Similar situation is with warfare. People are highly unaware about the destructive prospects in this domain.

[61] Carl von Clausewitz, *On war*, CLAUSEWITZ, *available at* https://clausewitz.com/readings/OnWar1873/BK8ch06.html (Last visited Mar. 29, 2019).