P-ISSN: 2709-6254	Journal of Development and Social Sciences	April-June 2022,Vol. 3, No. 2
O-ISSN:2709-6262	http://dx.doi.org/10.47205/jdss.2022(3-II)96	[1076-1091]

Journal of Development and Social Sciences
www.jdss.org.pk

RESEARCH PAPER

Legal Framework of Right of Self Defense in Cyber Warfare: Application through Laws of Armed Conflict

[1]Shan Ali [2]Sabira Naz Qureshi

1. School of Law, Bahria University Islamabad, Pakistan
2. School of Law, Bahria University Islamabad, Pakistan

PAPER INFO

Received:
March 18, 2022
Accepted:
June 25, 2022
Online:
June 27, 2022

Keywords:
Accountability, Conservative Critique
Cyber Warfare, International Humanitarian Law, Proportionality

***Corresponding Author:**

sakambohadv@gmail.com

ABSTRACT

Cyberwarfare is a worldwide danger to governments, organizations, and people. Cyber Warfare affects computer systems and networks as a battlespace. International Law faces this difficulty. Without technology, war is unthinkable today. Cyberwarfare is a new tactic of warfare in armed conflicts. As modern warfare doesn't follow IHL standards and concepts. The legal vacuum in present legislation and issues IHL faces when considering Cyber Warfare is also noted. Eventually, IHL is adopted in Cyber Warfare to resolve problems quickly. In recent decades, the use of cyber methods in armed conflicts and how International Law applies to such circumstances has been a major concern. In this research paper, I first evaluate major humanitarian and legal concerns and show that the use of computer networks during armed conflicts is now a reality and a critical issue for the international community to address. In today's malware-ridden cultures, malicious cyber activities may disrupt and hurt people. Second, I present a short review of the international debate concerning cyber warfare during armed conflicts, focusing on the applicability of the Law of Armed Conflicts to cyber espionage. Cyber activities, or cyber warfare, are unquestionably governed by IHL. I also look at how IHL rules and principles apply to situations other than armed attacks involving cyber operations, as well as adequate protective regimes for cyber-attackers and infrastructure, such as health and humanitarian facilities. In this study, I examine whether IHL may be applied to cyber-warfare if it becomes an armed conflict. Conservative Critique evaluates the present IHL infrastructure to govern Cyber Warfare.

Introduction

More than 30 nations have backed initiatives to disrupt information networks throughout the globe in Cyber Warfare. Computer systems are often not the end target of attackers since they manage international infrastructures, such as airports or power grids. Attacking states may shut down airports and power infrastructure through computer networks. Almost all governments know that today's nations rely heavily on computer network systems for everything from transportation to commercial services. Hackers have codes that can be given by computers to collapse these systems, which might be just as effective and devastating as traditional military operations using guns, men, and missiles. Cyberattacks may come from anywhere in the globe with little evidence, unlike kinetic armed operations. It's hard to track down an attack's perpetrator, making revenge harder.

Cyberwarfare depends on a variety of factors. Such assaults involve the identification of people targeted, what the attackers are doing and how they accomplish it, and how much damage they wreak using malware. Cyber Warfare is a fight between two

nations, not between individuals. Attacks must be severe to fulfill standards. Individual hacker assaults or hacker groups may not constitute Cyber Warfare unless backed and engaged by state agencies. In the dark age of Cyber Warfare, there are many hazy lines. Hackers are often given help by state officials so they can deny their operations. The legal status of Cyber Warfare is unknown, hence there are few rules or no International Law that may handle it. Cyber Warfare is handled by current legislation, although it's haphazard, unorganized, and susceptible to interpretation.

Many governments are motivated to exploit, and the lack of a legal framework has created a grey area. Many countries are unsure how states will respond to international law to investigate Cyber War methods. Law experts have spent years explaining how International Law applies to Cyberwarfare. The researchers' work led to the creation of the Tallinn Manual, a document produced by a group of legal specialists and sponsored by the NATO-affiliated Cooperative Cyber Defense Centre of Excellence (CCDCOE) in Estonia's capital, Tallinn.

Material and Methods

This work is going to use the Conservative Critique research methodology to critique the existing apparatus of IHL and its governance of the Cyber Warfare. Conservative Critique has been derived from the Conservatism of Thomas Hobbes where he wanted central authority for the state to function and remain intact. He propounded the need for clear laws and its enforcement to avoid any situation, where life would be brutish, nasty and short. Critical analysis techniques will be deployed to identify, examine and analyze the nature of Cyber Warfare and the deficiencies of IHL to deal with this challenge. The nature of the research is qualitative.

It is going to be a library based research where primary and secondary data will be used for the analysis. Primary data includes Geneva Conventions including its protocols while secondary data includes scholarly work of the expert in the relevant field. These will be articles, books, reports, and other types of narrations to be relied upon.

Cyberwarfare Arguments

IHL doesn't regulate Cyber Warfare, say many. Cyber Warfare is mostly unregulated under IHL. IHL may only apply to Cyber Warfare if it occurs during or causes a war. Whether a cyber-attack may approach the level of 'use of force' or 'armed assault' such that IHL rules apply to Cyber Warfare is questionable. Assigning the assault to a state or armed group will take time, but IHL cannot wait until then to assess whether the cyber-strike is a military operation. The international community needs clear norms and regulations that cover non-physical armed strikes to reflect 21st-century armaments and war technologies. The IHL often called the rules of armed conflict, is based on certain principles to discern between civilian and military objects and to protect civilians. IHL only applies in times of war, hence its principles are only valid then. Cyber warfare makes these concepts more important. IHL doesn't applicable to most cybercrimes and cyberespionage. It only applies to armed cyberattacks. In UN-mandated cyber procedures, it's disputed whether IHL applies to Cyber Warfare. When cyber-attacks target hospitals and grids, they violate IHL and the UN Charter, yet these bans won't safeguard computers.

IHL Struggles

This current world defies The Laws of War (IHL). To guarantee that IHL can execute its tasks in times of armed conflict and is fair enough to cope with current means and ways of war, it must be understood and react to these issues. Technology has created a new

battleground. IHL's cyberwar challenge has established a new warfighting realm. Conflicting groups often deploy remote-controlled drones. IHL has several issues. Cyberwarfare will be emphasized.

Rebels

IHL encompasses civilians and combatants. Law of War protects civilians and combatants. The US has invented the designation 'unlawful combatant' After 9/11, numerous Al-Qaida and Taliban militants were incarcerated at Guantanamo Bay. They're illegal combatants. The US says they're neither civilians nor fighters. They don't fit any of the IHL's categories, hence they aren't protected. So they were tormented widely. Since IHL doesn't specifically define illegal combatants, the legality is challenged. This is a challenge. This study focuses on Cyber Warfare, not illegal combatants.

Infantry

Child soldiers are another IHL concern. The participation of minors in wars is one of the legal efforts to control and underpins the creation of the rules of war. IHL aims to prohibit minors from being treated as prisoners of war if seized during armed conflict. Child soldiers should be treated as POWs. Children who commit war crimes or other terrible acts during wartime are protected from substantial punishment. Beginning in 1977, new protocols I and II oblige all state parties to take safeguards against child troops. Children under 15 shouldn't engage in conflicts or be enlisted in the military. The Geneva Convention and Additional Protocol I define IHL violations as severe breaches. The high-contracting parties should penalize them under universal jurisdiction. IHL prohibits child soldiers. Additional Protocols I and II ban the recruitment of juvenile soldiers.

Killer Robots

Killer robots are also a threat to IHL. Countries, professionals, and the public must investigate one of the most worrisome military technologies today. When no explicit convention or legislation exists on an issue, governments might outlaw the use of weapons beforehand under International Humanitarian Law. Rapid expansion in technology and AI might entail completely autonomous weapons, or "Killer Robots," in the near future. This could be a problem for the international community.

Nearly 50 nations met at the UN in Geneva for the first formal conference on "Killer Robots" International Humanitarian Law is thorough and can adapt to new technology. IHL's history illustrates that new technologies threaten it. With AI, humans are more likely to employ it for military purposes. The international community is concerned about weaponry. Killer robots pose a significant danger to mankind and the Laws of War (IHL). The following section will detail the study on Cyber Warfare.

Cyber Krieg

Beginning in the 20th century, nations and individuals became increasingly reliant on IT, the most significant development in contemporary times. They use computers and computer networks to run the entire state, including health care, businesses, and military operations, such as payroll and other records, sale and purchase, research and development, manufacturing, and dealing with armed forces, and delivery of food, water, and energy networks. Terrorists even utilize the internet to launch assaults, let alone governments. States employ cyberspace quickly in the battle to damage opponents' infrastructure, civilian items, and armed assets.

Cyberwar creates a distinct battlefield and challenges the rules of war (IHL). Most scholars agree that IHL applies to Cyber Warfare. Cyberwarfare is 'international' and

demands an international legal reaction. The interstate use of cyber force is not regulated under international law. From state to individual persons in the 21st century, computers and advanced information technology are essential. The international community hasn't decided on how to apply international humanitarian law ("IHL") to modern battlefields. After describing the entire Internet system and emphasizing several cyber warfare incidents, this article will argue that Cyber Warfare violates the conventional concepts of difference and neutrality more than Conventional Warfare. States have huge incentives to participate in illicit cyberattacks notwithstanding the risk of war crimes charges.

Cyber Warfare belligerents breach differentiation more than in traditional battles. Many cyber operations violate the principle of neutrality, so cyber conflicts are more likely to have these violations than traditional wars. Rather than criticizing all cyber means and methods, International Humanitarian Law should be understood and modified to encourage the use of cyber warfare in certain situations and give nations more direction on how to conduct these attacks.

Some of the numerous issues facing International Humanitarian Law are outlined above. This study will concentrate exclusively on Cyber Warfare and IHL. Future studies may concentrate on the other difficulties mentioned. Arguments in Favor of Cyber Warfare

There are many arguments in support of Cyber Warfare in contrast to traditional or kinetic wars (Jones, & Janicke, 2015) Arguably, in the past, an actual Cyber War has never happened and is not occurring in the present and there are no signs of this happening in the future. Rather than heralding a new era of violent conflict, so far cyber-attack that we can say has happened do not reach the level of an armed attack, in the eyes of International Law. As there was no harm to the lives of the civilians and the consequences were less than the kinetic attack which does not rise to amount to an act of war as damages to the data and hacking information do not amount to an armed attack, even cyber-attacks that because damages do so only indirectly.

To sum up, here, it is stated that Cyber Warfare is not a danger to international peace and security. It is further argued that instead, a cyber-attack that is launched with aim of material destruction or damage to the life of civilians must utilize the force or energy embedded in its target (Farwell, & Rohozinski, 2011) As for instance, disrupting electricity grids or shutting down an air traffic control system and causing trains or plains to crash do not inflict direct harm to the people as they are mostly carrying out by the hacker not by the state authorities and therefore cannot be considered a threat to international peace (Rid, 2013).

Secondly, cyber-attacks are more reasonably deniable than traditional attacks. The reputational cost of bringing a cyber-attack that causes collateral damage is likely to be less as well (James, 2017). There is a possibility of another argument in support of Cyber Warfare. Traditional wars are very long taking years to finish. A few examples are the Hundred Years War in the history of Europe. Other examples could be the First and Second World Wars, and the recent is War on Terror lasted for almost two decades. Cyber Warfare would not take that long if it happens in the future.

Deterrence Theory

During the time of the cold war, deterrence theory was the first preferred framework that analyze the military doctrine to elaborate on the influence of nuclear weapons and further argued that nuclear power and its consequences, such war (nuclear war) will not go to war with each other, and this also applied to the theoretical framework to cyberspace, as cyber deterrence. The concept of deterrence related to military operations

dates back to the 1920s/30s. deterrence theory get more prominent and developed to its present form in times of the Cold War, between the US and Soviet Union. The US Army analyzed that there is no difference between deterrence in the domain of cyberspace and any other domain. In cyber warfare, the theory of deterrence and its application leads to a series of conclusions for policy making (Askin, 1997).

As we know that "Cyber Weapons" require a specific legal development, quick retaliatory cyber strikes are impossible. Therefore, due to the fact that the attribution requires, retaliation with cyber means cannot be done ad-hoc. Defense and offense must thus be joined into a broader deterrence strategy (Bendiek, & Metzger, 2015). In human beings' affairs the Deterrence of attack has a long history, so the relationship between the rise of a new kind of battlefield and a result it is necessary to discover a new strategy of a weapon for deterrence to acquire the applicability to Cyber War. The non-ending competition between the development of the new kind of weapons and their use, and the defensive response to them. In order to adjust deterrence theory to deal with the new form of threat of Cyber Warfare, which has started a new chapter in warfare. Cyber warfare has brought a new challenge to the international community (Lupovici, 2011). The deterrence theory and its application to Cyber Warfare relate to ambiguity with this respect, at first recognition and attribution of an attack, and second the uncertain effect of any attack. The difficulty around the attribution and control of its impacts make the deterrence of Cyber Warfare unique and difficult. The implications of this uncertainty can show that there is a need for development to expand the ability to apply deterrence to Cyber Warfare.

Realist Theory

There is an enormous implication of national security to Cyber Warfare. Which is now considered outer space, which is also recognized as a new battlefield. The dependency on the space-based platform in order to observe the actions of an enemy has increased with great power and communication with military forces of land-based. It is critical to secure rotating satellites in cyberspace, as well as provide targeting information to precisely guided munitions. To be sure, that the satellites are accessible to conventional targets, like space mines and missiles, as well as to direct energy munitions, like for example, particle beams and leaser (Carter, 1984) Furthermore, a cyberattack that destroys these critical assets that link to control stations is a less expensive and less visible means to eliminate them.

The electronic connection of it once incapacitated, any country would find that its military is seriously weakened for reconnaissance, it is reliant on satellites. navigation, and communication. In a conflict with a competitor, this effectively eliminates the using force. Not only does the legal distinction between peace and war apply to cyber warfare, but it also extends from the physical to the virtual realm. And the new challenges require a new kind of response. Those states that a few years ago were not considered the new technology are now using cyber technology to attack the world's most prominent nations by using viruses (Mosteanu, 2020)

These threat states are likely to move in order to plan security planning depending on anticipatory self-defense. Like defense for the interest of the nation is thoroughly rooted in International Law. Nations require in avoiding future threats and repelling those that are already ongoing, as long as their responses are reasonable to the threat and exclusively target those who are participating in such attacks. Anticipatory self-defense is more expansive and allows states to take precautionary actions without having to wait for an imagined threat to emerge (Mueller, Castillo, Morgan, Pegahi, & Rosen, 2006).

Just War Theory

Just war theory has developed many centuries into its present form, the justification of war is evident from the defensive response from states or the United States Security authorization. The member states of the UN have altered the Just War theory in order to maintain international peace (Chesterman, S, 2002). Still some countries have found ways to justify their aggressive actions against a weak states even in contemporary times. Some scholars and international organizations have produced concepts in just war theory that wrongfully justify the aforementioned conflicts, and over time these notions of "responsibility to protect" (Focarelli, C. 2008). "humanitarian intervention," "pre-emptive and preventive self-defense," and the "unwilling or unable test" have emerged. These concepts have costs and are not justified. Since just war theory has continued to evolve and may be modified in the future Just War Theory.

As the growing scope of the internet has increasingly allowed people, government militaries, and organizations to work under the computer system. It also opens ways for actors to wage cyberattacks against all who use the internet. Today most of the national infrastructure, military system, government, and financial institutions operate by the digital system. The Just War Theory has played a big role in elevating the ethical and other use of new weapons throughout history, in this respect the theory of Cyber War is not different. The application of the Just War Theory to Cyber Warfare is greatly debated. Some scholars argued that the Just War Theory is irrelevant to Cyber Warfare. for considering morality, the Just War Theory is a useful tool applicable to Cyber War (Yates, 2013).

Generally, conventional Warfare is being addressed by The International Treaties and Agreements to provide protection to innocent people and also to prevent extra damages to their properties. These rules and principles are known as International Humanitarian Law and are deeply contributed by Just War Theory (Evans, 2005). In recent few years, there has been much debates whether the existing system is effectively applied to cyber warfare, or it is some different concept from kinetic warfare.

But the IHL and Just War Theory mostly focus on the intentions of the states, the results of attacks, and the means and methods through which the attack has brought. And this permits these customs to successfully be applied to a new concept of warfare, such as Cyber War. Although it is possible to bring these traditional guidelines into use, it still needed to be given to how perfectly the rules can be applied to Cyber Warfare. And this applicability of the rules needs to be elaborated/defined and accepted by the International Community in order to successfully regulate Cyber Warfare. As it has been stated that Cyber Warfare is a new kind of warfare and is considered a future threat to the world. Which is not addressed by any existing legal framework and there is a need for further interpretation in the present body of law (IHL) (Kaempf, & Tannock, 2018). So, in this article, the Cyber Warfare theory is related to my study which will be used to critique the contemporary apparatus of IHL as time is changing, and with the passage of time, the concept of war has also changed in the international domain.

International Armed Conflict (IAC)

The concept of armed conflict of international character is initially laid down in the Geneva Convention of 1949 and was developed in part to make the threshold of application a little more objective and factual and, therefore, remove the need for relatively and formal political recognition of a situation of war in the legal sense (Cullen, 2010). The situation of IAC happens when two or more sovereign states resort to the use of armed forces against each other. An armed conflict that takes place between a country and the international organization of another state also amounts to an Armed Conflict.

The definition of International Armed Conflict has been provided in Common Article 2 (1) to the four Geneva Conventions, which brings about the application of International Humanitarian Law. However, the rules that are applicable to No-international armed conflict have been given under Common Article 3 to the four Geneva Conventions, without giving a clear and comprehensive definition of such kind of conflict.

The jurisprudence of the international tribunal and the first 1977 Additional Protocol to the Geneva Conventions have expanded the definition of an armed conflict at the international level, and have also provided criteria for interpretation of this definition. The matter involved in those definitions lies in the responsibility to respect rules of conventional and customary humanitarian law, especially, it is applicable to the conflicts at an international level rather than the more limited rules applicable to those armed conflicts at the non-international level.

Non-International Armed Conflict

International Humanitarian Law governs the situation during war times. Conflicts occur between nation-states. IHL applies during international and non-international armed conflicts. Only a small portion of law applies, namely Common Article 3 of the Geneva Convention 1949 of Additional Protocol II (Lysaght, 1983). Common article 3 is applicable to the armed conflict of not an international nature but took place on the territory of the state party, and this kind of conflict does not have to involve the military of the state but involves two or more armed groups. The principles of IHL may be applied to non-international Armed Conflicts under extremely limited circumstances, such as when both the State involved and a third State acknowledge the insurgent group's belligerency. Recognition of belligerency is allowed thereby triggering the applicability of IHL if the insurgent group;

- Those territories that are occupied
- Established a government that exercised sovereign rights over the territory it occupied.
- Complied with the laws and customs of war during hostilities with the State. (Bartels, 2009)

The majority number of conflicts presently are of a non-international character. non-international armed conflicts occur when hostilities emerge between government and military forces, organized non-state armed groups, or such groups. Hostilities must reach a particular level of severity and the parties engaged must be well-organized in order to be classified as an international armed conflict. NIACs, as defined in common Article 3 and NIACs as described in Article 1 of Additional Protocol II, are distinguished under IHL treaty law.

- Common Article 3 relates to non-international armed conflicts that occur on the territory of a high contracting party. Armed conflicts in which one or more established non-State armed organizations which involved and classified as these. NIACs between state armed forces and organized non-state organizations may occur or may occur only between such groups.
- It establishes the necessary territorial control, enabling organized non-state armed organizations to use that territorial control and are capable to carry out a prepared and powerful armed attack in order to implement the Protocol.
- The armed conflicts which happen between two or more independent nations with military forces and other organized armed groups Additional protocol II directly

applies to such kinds of conflicts, unlike common Article 3 of Additional Protocol II does not apply to armed conflict of Non-state organized armed groups.

It is important to remember that the Additional Protocol II helps to improve and supplements common Article 3 without adjusting its current form of application, which means that this definition applies only to the validity of the Additional Protocol II, it does not apply to non-international armed conflicts.

Richard Baxter has written about the Vietnam War, he stated that though He added that, although it is easy to demonstrate that the US participation in the war has internationalized the conflict under Article 2 of the Geneva Conventions (1949), the entire law of war may be applicable. The International Court of Justice ruled in the Nicaragua case.

"The conflict between the contras'' military and those of the Government of Nicaragua is an armed conflict which is 'not of an international character".

The actions of the contras against the Nicaraguan government are thus governed by the law governing such conflicts, whereas the US actions against Nicaragua are governed by the law regulating international armed conflicts (Baxter, 1980).

IHL Governing Cyber Warfare

IHL appears today that applies to cyber operations which take place in the context of pre-existing and non-international armed conflicts. It is widely acknowledged that the idea of cyber war did not exist at the time when the most modern tools of International Humanitarian Law were being drafted, but this does not limit the application of IHL to such operations. The right of belligerents to choose techniques or means of combat has always been one of the most essential rules of IHL, the existing IHL explicitly anticipates that its rules and principles will be applied to newly developed ways and weapons of warfare. The context in which a means or method is used, not in its specific form, subjects it to the rules and principles of IHL (Melzer, 2011).

The scope of combat in the cyber domain is demonstrated through cyber operations. IHL either applies to some extent or does not apply at all, or its applicability completely depends on where the issue is along with the conflict spectrum. Without a doubt, certain situations are more difficult to assess than others, the analysis is shown below. Any analysis of conflict classification considers that there must be some connection between the cyber operation or conduct of hostilities and the conflict for IHL to apply. In another way, if a cyber-attack occurs and is still related to armed conflict, IHL will not govern such conflicts. Unsurprisingly, there can be an important debate relating to the scope and nature of the conflict in the cyber domain. Looking at the conflict category under IHL through a cyber-lens poses several challenging concerns outside of that threshold relationship (Wallace, & Jacobs, 2019).

It is a vital issue and matter to the international communities to take into consideration whether IHL (the Laws of War) is applicable in the domain of Cyber Warfare. A cyber-attack can be a Cyber Warfare if such an attack reaches the threshold of an armed conflict because the Laws of War (IHL) is deal only with the conflict of an international character and in certain situations with non-international or internal armed conflict (Bothe, Partsch, & Solf, 1982).

It has been declared that an international armed conflict is an act of war or any other armed conflict that may take place between two or more sovereign states, as stated under Common Article 2 of the Geneva Conventions of 1949, though one of the conflicting parties does not consider the situation to be a war. Article 1 of Additional Protocol II of

1977, on the other side, says that the protocol may be applied to all forms of armed conflicts involving military forces of a High Contracting Party and rebel armed groups or other organized armed groups that happen on the land of the High Contracting Party.IHL applies to both kinds of situations of international and non-international armed conflicts, as these two articles make clear (Droege, 2012).

There are two kinds of armed conflicts mentioned earlier,

1. Any other armed conflict between two or more states, including combating colonial supremacy, foreign occupation, and racist regimes in the exercise of their right to self-determination, as well as any other armed conflict between two or more states.

2. non-international armed conflict.

IHL is, however, applicable in the cyber-attack if it amounts to an armed conflict or if it is done as a part of an armed conflict. It is quite uncontroversial that when cyber operations are conducted in the context of an ongoing armed conflict then they are governed by the same IHL rules as that of conventional conflict, for example, if in similar or in addition to a bomb or missile attack, if a party to the conflict also brings a cyber-attack on the computer systems of its enemy, the IHL is applied both for the conventional attacks and cyber-attacks. The issue arises in respect of the applicability of IHL in a different cyber-attack.

Even if the attack is initiated on a computer network that is not used by state employees, such activities could result in significant human tragedy, especially in the event of an armed war. There must be a reason to be cautious that cyber strikes will be used to interrupt the infrastructure necessary to supply essential resources and services to meet the basic requirements of the civilian. For example, vital connections such as electric power grids, nuclear plants, water plants, and systems for the delivery, oil refineries, gas and oil pipelines, financial systems, hospital systems, railroads, and control air traffic systems all are heavily dependent on computer and internet systems susceptible to access and operation by cyber operations. The high level of interconnectedness and dependency between civilian and military structures elevates the dander that civilians and civilian objects will be harmed due to happening of Cyber Warfare (Diamond, 2014).

Principles of IHL

Principles of IHL which are applicable in times of war for protection of the civilian population are as under;

Principle of Military Necessity

The Law of Armed Conflicts is a part of international law restricting the harm and suffering caused by armed conflict. The principle of military necessity, which is similar to the principle of proportionality, is a significant part of IHL. The principle of military necessity permits actions that are required to achieve an appropriate military objective and are not banned by international humanitarian law. When there is a situation of an armed conflict the only lawful purpose is to weaken the adversary's armed forces capabilities (Benvenisti, 2009).

The modern law of armed conflict, therefore, with its strong humanitarian concern, necessarily requires a cautious difference between military and targeting civilians. It is based on an indirect and quite often elusive non-arithmetical formula that seeks to balance the expected armed benefits of a given operation against civilian deaths or harm to civilian

objects. If proportionality is the center of the problem, and humanity is one side of the equation, military necessity is the other.

Military necessity is defined as the ability of the armed forces to do whatever is necessary to achieve their lawful military objectives in warfare, provided that it is not otherwise unlawful in the meaning of IHL, for instance, enemy armed forces that have not withdrawn or are not hors de combat always are legitimate military targets in themselves, and may be attacked by the enemy at any time and in any place, regardless of where they are or what they are doing. (Goodman, 2013),

It is always placing limitations on every military activity that are the more restrictive approach to the doctrine of military necessity, however, interpreting it as always employing restrictions on the actions of military forces, In the sense that no such actions may be undertaken (despite its legality under international Humanitarian Law) unless it is essential in terms of military sense.

An attacking force, for example, may decide not to target certain opponent's military foundations that do not restrict its attack or would create a distraction from its primary goals. The legal idea of military necessity is not commonly similar to that of military advantage and this fact should always be highlighted, (which is a factual descriptor of the consequence upon which activities are predicated). Finally, "military necessity" is best described as the requirement, under any given set of circumstances, for the sake of military force to achieve justifiable military objectives (following the other principles of IHL) (Schmitt, 2016).

Principles of Distinction

The Laws of Armed conflict (IHL) rule of distinction means to protect those persons who are not participating in hostilities, specifically, common people. It is also intended to safeguard armed forces or combatants who have been subjected to illness, or as injured civilians. Protecting civilians in times of war has been provided under the rule distinction. Petersburg Declaration positively stated that the primary aim of war is to weaken the enemy state by attacking only its military forces.

In Hague Regulations the rule was further provided, which prohibited launching an attack on "towns, villages, dwellings or buildings which are undefined" therefore being "attack in the night" there may be a huge possibility of targeting innocent civilians and combatants indiscriminately (Chengeta, 2016).

The principle of distinction has now been included in the rules of war and it applies to both international and non-international armed conflicts. The Geneva Conventions' Additional Protocol I contains provisions concerning the rule of distinction. It also ensures that persons and their property are respected and protected in times of war. Parties to a conflict must differentiate between military objectives, as well as objects and military objects, and direct their attacks just against the military and their objectives, not civilians (Oswald, 2016). The population as such, as well as individual civilians, shall not be the object of operations.

Principle of Proportionality

Under the principle of proportionality, an attack is restricted if "there is a reasonable probability of causing incidental damages to civilian life, injury to people, or destruction to civilian property, which would be excessive about the material and direct military advantages expected". When it comes to applying IHL principles to the area of

cyber warfare, one of the most critical questions will be determining to what degree the term "harm" covers loss of functionality (Fenrick,1982).

On the other hand, as previously stated, it is unclear exactly which sorts of functional disruptions come within the relevant group of damage. Another issue in implementing the principle of proportionality would be determining whether the expected accidental damage to civilian objects is excessive in comparison to the expected military advantage (Dinstein, 2012).

To be sure, balancing predictable harm to civilians or civilian objects against anticipated military advantage was and still is a challenge to the world, but in the case of Cyber Warfare, the difficulties, However, as suggested previously, it is uncertain which types of functional disruptions fall within the relevant harm category. Another challenge in implementing the proportionality principle is evaluating whether it is proportional to this. The challenge of estimating the scope of collateral damage that can be foreseen exacerbates the problem (Voigt, 2008). This is true both because cyber operations are a relatively new notion of warfare with well-known consequences and effects, and because the interconnected nature of cyberspace makes it difficult to anticipate all of the possible outcomes.

Principle of Precaution

Precautions required under IHL precautions must be preserved by the belligerents against the effects of attacks while directing an attack. The principle Precautions to be observed in the attack are needed by a general rule, which may be applied to all forms of military operations (Fenrick, 1982). To protect the individual from any kind of harm and their objects from damage constant care must be taken in this regard. And specific precautionary requirements were established by additional rules. Those planning or deciding to launch an attack should do everything possible to confirm that only military objectives are targeted and take all appropriate measures while identifying methods and means of warfare to prevent or, at the very least, limit civilian casualties. If there is a risk that the principle of precaution and proportionality will be violated, the belligerent must be required to avoid or avoid an attack (Cannizzaro, 2006).

A party to an armed conflict, in the light of these rules, who is planning to direct a cyber-attack must do every plausible thing to gather the vital data of the state to verify that the planned attack is for the purpose of achieving a military objective and that the attack will not cause more damage to civilians. This may need bringing in technical specialists to identify the targeted system of a country and the systems to which it is associated, as well as the best manner to accomplish this object. The attack must be avoided wholly if the competence required to get and appropriately assess the information required is lost. Targets must be restricted to those targets as to which adequate information is available in such a situation.

In some cases, the responsibility to select means and methods of warfare with the purpose of decreasing civilian deaths may require belligerents to achieve their military objectives by a cyber-attack rather than using more harmful means such as conventional armed force. The duty to take necessary precautions against civilians and civilian objects in any attack to minimize loss or damages resulting from military operations requires that parties to an armed conflict keep military objectives separated from civilian population objectives to the maximum extent possible (Barber, 2010).

While observing the principle of precautions, civilian and military infrastructure must have distinguished by belligerents targeting a state. In reality, civilian and military cyber infrastructure, however, are so interconnected together, and that effort separating

them is considered not to be deemed easy. Belligerents would also have to take all necessary precautions to protect essential civilian infrastructure from the effects of cyber-attacks, such as ensuring that vital data can be safely stockpiled and effectively associated and providing for rapid restoration of civilian systems that have been damaged as a result of an attack (Droege, 2012).

The Principle of Accountability

Each party to an armed conflict, both states, and non-state armed groups, will be held responsible for complying with the standards of the International Humanitarian Law. To put it another way, the Law of War must be followed by all parties involved in armed conflict. the parties to an armed conflict will responsible under IHL for such violations (Chinkin, 1994).

For example, Israel launched a military operation in Gazza Strip with the state that aim of suppressing rocket attacks on Israel by Hamas and other armed groups of Palestinian groups in 2008. This military operation ended in 2009 when both parties to the armed conflict declared a ceasefire. According to the United Nations and the Palestinian health ministry, this armed conflict had affected more civilians. Palestine reported more than 500 civilians and damage to public and private property. Civilians had paid the largest price in this armed conflict between Israel and Gazza and both the parties alleged serious violations of International Humanitarian Law. All parties are responsible and accountable for any violations of the Law of War, according to the principle of accountability.

Research Findings

For a cyber-attack in order to qualify as one involving the requirement for the attacks as given under IHL, it must cause certain physical destruction or injury or death to a person as mentioned under the charter and IHL. However, in the age of warfare, physical destruction is less compared to kinetic warfare. Cyber-attacks will cause mere inconveniences i.e shut down the state system of many aspects like cause damage to economic structure, stealing data from banks one example is that shut down the New York Exchange for a week which resulted in the loss of an enormous amount of money which causes no tangible or visible damages (Castel, & Castel, 2016). So, it is reasonable to say that this research has found that IHL cannot assess the magnitude of damage in Cyber Warfare.

However, the consequences were far more serious than a single person's physical harm or injury. Similarly, the cyber-attack on Estonia shut down the banking websites with the view that the use of force could only be armed in nature (Hollis, 2007). A cyber-attack on the city of New York will not be considered a use of force. It is very hard to determine the sources of cyber-attack and is also an attribution problem.

This reality would provide many cyber-attacks with plausible deniability, especially as in many cases nations can credibly claim that the attacks may have started on their territory but were not initiated by their governments nor did the government authorize any group to initiate such an attack. Many cyber-attacks will not be harmful to civilian populations or to their objects, and many may not even cause permanent damage to physical objects. Another research finding is that it is hard to determine which conflict is international and non-international when it comes to Cyber Warfare. Here again, IHL is unable to determine the nature of the attack to exercise jurisdiction over it. The next research finding is that in Cyber Warfare proportionality cannot be determined or evaluated. Likewise, there are issues with the principle of distinction, and proportionality. This leads to the conclusion that IHL is unable to regulate absolutely Cyber Warfare.

Conclusion

Cyberwar refers to an attack on computer systems by means of the digital world, Even if the data center included government records, firing a missile against it would not be deemed Cyber Warfare. and using hackers to spy on or steal data would not be considered cyber warfare in itself, but rather cyber espionage, which is carried out by practically all nations of the world. This chapter has concluded this research that a new treaty is required to focus on the control of Cyber Warfare.

For Sure, there are a lot of grey areas here (Cyber Warfare is basically one huge grey area), but labeling every hack as an act of Cyber War is at best ineffective, and at worst, it is scaremongering that could lead to dangerous development.

During my research on Cyber Warfare, Analyzing the existing situation of cyberspace and then discussing Cyber Warfare and the events that have occurred appeared to be difficult. Particularly, the potential for cyber warfare to occur in the international community, the limitations that existing international laws have imposed on cyber warfare, and, most importantly, the possible drawbacks of these laws. The focus of this research is, however, to collect relevant Cyber Warfare information and map it into a framework hence the governance aspects are still not covered.

The data collected could assist in understanding the boundaries that are crossed in cyber warfare and the misuse of cyberspace that is triggered by or results from international conflicts. Whereas superpower governments such as the United States and China appear to be working toward the formation of a new type of major power relationship, cyberspace collaboration should be a key component of that endeavor. Following the land, sea, air, and outer space as battlefields, cyberspace is becoming one of them.

The Internet has become a vital and crucial component of every state, society, and individual's daily life. Furthermore, it has gained momentum for future development. However, along with the conveniences that the Internet has provided, it has also brought with it a growing number of potential threats and concerns to the world computer system. Cyber Warfare incidents from the past were researched for this article, included are a number of prominent and publicized Cases of Cyber Warfare that involve states. Each case was investigated, analyzed, and documented using a framework similar to that used in kinetic warfare in the field of international conflict management. Each case study follows a general framework that begins with a brief background of the conflict in order to understand the parties involved. This research has shown to a large extent that the current IHL framework is insufficient to combat the threat of cyber warfare. therefore, a new treaty focusing on cyber-warfare must be established.

References

Askin, K. D, (1997). *War Crimes Against Women: Prosecution in International War Crimes Tribunals Volume 1 of War Crimes Against Women*. Martinus Nijhoff Publishers.

Barber, R. J. (2010). The proportionality equation: Balancing military objectives with civilian lives in the armed conflict in Afghanistan. *Journal of Conflict & Security Law*, 15(3), 467-500.

Bartels, R. (2009), Timelines, borderlines and conflicts: the historical evolution of the legal divide between international and non-international armed conflicts. *International Review of the Red Cross,* 91(873). 35-67.

Baxter, R. R, (1980). International Law in "Her Infinite Variety." *The International and Comparative Law Quarterly*, 29(4), 549-566.

Bendiek, A., & Metzger, T. (2015). *Deterrence Theory in the Cyber-Century. Lecture Notes in Informatics (LNI),* Gesellschaft für Informatik, Bonn

Benvenisti, E. (2010). The Legal Battle to Define the Law on Transnational Asymmetric Warfare, 20 *Duke Journal of Comparative & International Law*, 20(3), 339-359.

Bothe, M., Partsch, K. J., & Solf, W. A. (1982). *New rules for victims of armed conflicts: commentary on the two 1977 protocols additional to the Geneva Conventions of 1949.* Martinus Nijhoff Publishers.

Cannizzaro, E. (2006). Contextualizing proportionality: jus ad bellum and jus in bello in the Lebanese war. *International Review of the Red Cross*, 88(884), 779-792.

Carter, A. B. (1984). *Directed Energy Missile Defense in Space–A Background Paper*. Washington, D. C.: U.S. Congress, Office of Technology Assessment, OTA-BP-ISC-26,

Castel, J. G., & Castel, M. E. (2016). Canadian State Immunity Act and the Absolute Immunity of Foreign States Committing or Supporting Acts of Terrorism or Violating International Humanitarian Law. *Advocates' Quarterly*, 45(1), 81-101.

Chengeta, T. (2016). *Measuring autonomous weapon systems against international humanitarian law rules*. JL & Cyber Warfare.

Chesterman, S. (2002). *Just war or just peace? humanitarian intervention and international law*. Oxford University Press on Demand.

Chinkin, C. (1994). Rape and sexual abuse of women in international law. *European Journal of International Law*, 5(3), 326-341.

Clark, I. Kaempf, S., Reus-Smit, C., & Tannock, E. (2018). Crisis in the laws of war? Beyond compliance and effectiveness. *European Journal of International Relations*, 24(2), 319-343.

Cullen, A. (2010). The concept of non-international armed conflict in international humanitarian law. Cambridge University Press.

Diamond, E. (2014). *Applying International Humanitarian Law to Cyber Warfare.* The Institute for International Security Studies.

Dinstein, Y. (2012). The principle of distinction and cyber war in International Armed Conflicts. *Journal of Conflict and Security Law*, 17(2), 261-277.

Droege, C, (2012). Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians*. International Review of the Red Cross,* 99(886), 533-578.

Droege, C. (2012). Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross*, 94(886), 533-578.

Evans, C. (2005). The double-edged sword: religious influences on international humanitarian law. *Melbourne Journal of International Law*, 6(1), 1-32.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival,* 53(1), 23-40.

Fenrick, W. J. (1982). The Rule of Proportionality and Protocol in Conventional Warfare. *Military Law Review*, 98, 91-100.

Focarelli, C. (2008). The responsibility to protect doctrine and humanitarian intervention: too many ambiguities for a working doctrine. *Journal of Conflict and Security Law,* 13(2), 191-213.

Goodman, R, (2013). The power to kill or capture enemy combatants. *European Journal of International Law,* 24(3), 819-853.

Hollis, D. B. (2007). Why States Need an International Law for Information Operations. *Lewis & Clark Law Review*, 11(4), 1023-1061.

Lupovici, A. (2011). Cyber warfare and deterrence: Trends and challenges in research. *Military and Strategic Affairs*, 3(3), 49-62.

Lysaght, C. (1983). *The Scope of Protocol II and Its Relation to Common Article 3 of the Geneva Conventions of 1949 and Other Human Rights Instruments*. American University Law Review, 33.

McGhee, James E. (2017). Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy. *Journal of Law & Cyber Warfare*, 2(1), 64-103.

Melzer, N. (2011). *Cyberwarfare and International Law*. UNIDIR Resources.

Mosteanu, N. R. (2020). Artificial Intelligence and Cyber Security a Shield Against Cyberattack As A Risk Business Management Tool Case Of European Countries. *Quality-Access to Success*, 21(175),148-156.

Mueller, K. P., Castillo, J. J., Morgan, F. E., Pegahi, N., & Rosen, B. (2006). *Striking first: preemptive and preventive attack in US national security policy*. Rand Corporation.

Rid, T. (2013). Cyber War and peace, *Foreign Affair*, 96(6), 77-87

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & security*, 49, 70-94.

Rose, G., & Oswald, B. (2016). *Detention of Non-State Actors Engaged in Hostilities: The Future Law*. Nijhoff: Brill.

Schmitt, M. N. (2016). Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance. *Virginia Journal of International Law*, 50(4), 795-839.

Voigt, C. (2008). State responsibility for climate change damages. *Nordic Journal of International Law,* 77(1-2), 1-22.

Wallace, D. A., & Jacobs, C. W. (2019). Conflict Classification and Cyber Operations: Gaps, Ambiguities and Fault Lines. *University of Pennsylvania Journal of International Law*, 40(3), 643-693.

Yates, J. A. (2013). *Cyber Warfare: An Evolution in Warfare Not Just War Theory. Marine Corps Command and Staff Coll Quantico Va*. Master's Thesis. Submitted to the USMC Command and Staff College. USA: Marine Corps University.