Unity Journal
Vol.6, 284-296, Feb 2025
https://doi.org/10.3126/unityj.v6i1.75698
Prithvi Narayan Shah Research Center
Directorate General of Military Training, Nepali Army
Kathmandu, Nepal

ISSN - 2717-4751

Article history
Received: 09 Nov 2024
Accepted: 23 Jan 2025

Application of International Humanitarian Law in Changing Dimensions of Armed Conflict vis-à-vis Cyber Warfare

Ashutosh Pandey*

Abstract

Transcending the traditional methods of warfare, which were fought on land, sea, and airspace, the dazzling scientific progress of recent decades has given rise to unprecedented means and methods of warfare. The conventional weapons are being replaced by combat robots, drones, cyber-weapons, nanotechnologies, and Artificial Intelligence, among others. While the purpose of the old-school conflicts model was to weaken the opponent's military power through physical use of force, the modern-day conflicts model, be it international or non-international, deviates in methods of warfare by weakening enemy forces through the use of advanced science and technologies. Cyber warfare, under IHL, is a relatively new concept which relies on digital infrastructure to conduct hostilities on enemy forces, leading to the triggering of the definition of "attack" under Additional Protocol I and initiating the execution of Humanitarian Law. While there are numerous complex, unsolved, and unanswered questions, this paper aims to examine the applicability of existing IHL- related legal frameworks and principles to the cyber domain, elucidate the complexities involved in regulating such cyber operations under the purview of IHL, and the unique challenges that cyber warfare poses to the application of IHL in this digital realm, especially with regard to the non-kinetic nature of its attacking mechanism. While it is true that states have no common consensus regarding the regulation of war in the cyber domain, the assessment of primary and secondary sources like laws of war, textbooks, journal articles, commentaries, and notable cases affirms that IHL adjusts to the quickly evolving character of contemporary armed conflicts, such as cyber warfare.

Keywords: *War, science, cyber warfare, technology, armed conflict, international humanitarian law*

Introduction

With the establishment of the United Nations Organization (UNO) on 24 October 1945, countries across the globe have not witnessed the horrific scenes of large-scale war like World War I (1914-1918) or World War II (1939-1945). Considering the fact that the United Nations

* Law Graduate
Email ID : ashutosh.pandey2019@nalc.edu.np

Organization (UNO) has been successful enough to preempt World War III, there were various instances of small-scale armed conflicts around the world, among which some still exist. The Israeli-Palestinian Conflict, the Sierra Leone Civil War, the Afghanistan War, the Yemen and Syria Conflict, the latest Russian invasion of Ukraine in 2022, and Iran's missile attack in Israel in 2024 are some of the infamous ongoing conflicts which have time and again reminded mankind that wars can never be pleasant. With these two recent events of the Russian invasion of Ukraine and the bombing of Gaza, the end of June 2024 recorded 59 ongoing armed conflicts across the globe, both of international and non-international character (Rustad, 2024). Similarly, the Israel-Iran proxy war took a nasty turn and further escalated on 1st October 2024, when Iran launched 180 ballistic missiles at Israel in response to Israel's assassination of Hezbollah and Hamas leaders (Holmes, 2024). The escalation of these two recent armed conflicts has reminded the world that wars are always ugly and result in the death of people, destruction of property, and harm to the natural environment, making them unsuitable for human settlement. WW I was fought with rifles, mortars, flamethrowers, and machine guns, whereas these classical weapons were upgraded to high-tech guns, missiles, and atomic bombs in WW II. With scientific and technological advancements, countries have created modern weapons of mass destruction in the twenty-first century. These weapons can be nuclear, biological, or chemical, and are commonly referred to as WMD, which are more deadly, dangerous, and capable of causing a great deal of damage to people's lives, property, and natural environment (The Editors of Encyclopedia Britannica, 2017).

Once German scientist Albert Einstein stated, "I am unsure of the weapons that will be used in World War III, but World War IV will be waged with sticks and stones" (Calaprice, 2005, p. 173). The essence of this observation is that the advanced weapons that will probably have been used in WW III will have such a gruesome, large scale, and severe impact on living beings and mother nature that our era will be pushed back to the Stone Age where the human civilization began. Similarly, it also denotes how the means and methods of warfare, through time, have transitioned from traditional to technological. The discovery and development of unique tools and techniques of warfare, such as battle robots, artificial intelligence, nanotechnologies, laser weaponry, and observation and combat drones, have been made possible by the astounding scientific and technological advancements of the last few decades (Bernard, 2012, p. 458). The traditional wars were fought on land, sea and airspace; however, the scope of term “war” has been widened up, which incorporates the Cyber War, Trade War, Technology War, and Information War. The purpose of old-school traditional wars would be to kill enemy soldiers on the battleground and destroy the opponent’s military power as much as possible through the use of force, but the wars, in modern times, are fought even without the use of weapons or soldiers, and their sole motive would be to destroy the stability and economy of the enemy state.

Cyber Warfare is an emerging trend of complex methods of warfare wherein the parties to conflict use the digital domain to conduct cyber operations in order to destabilize their opponents. At times of war, the scope of cyber warfare may range from minor operations like data destruction or virus attacks to major operations like destabilizing the functioning of Air Traffic Controls and Hospital systems, the crucial infrastructure required for civilian population, or even infiltrating Nuclear Power Plants whose destruction can cause a horrific aftermath to human life, property, and the natural environment. While the developers of laws of war may not

have drafted the legislation for all sets of situations that may arise, including cyber warfare, the whole notion of IHL is to mitigate human suffering during armed conflicts. This article dives deep into the laws of war, the practice of sovereign states during war, jurisprudence developed by different international courts like the ICC, ICJ, and various international criminal tribunals like ICTY, ICTR, ECCC, and also the customary laws applicable at times of war to elucidate the applicability of such legal framework in the grey area of cyber warfare. While this article does not aim to provide answers to all questions relating to cyber warfare, it aims to address the complexities involved in regulating cyber wars under the legal regime of humanitarian law and how these unique digital challenges can be solved so as to uphold the notion of "even wars have limits."

Armed Conflicts and Laws of Armed Conflict (LOAC)

The regime of International Law uses the term “armed conflict” instead of “war” for various reasons, the primary being that war is political and formal in nature, whereas armed conflict is conceptually broader and more flexible with proper legal definition. While the concept of 'war' already existed since the development of human civilization and also in the oldest treaties of the IHL, the 1949 Conventions introduced the concept of “armed conflict” into this legal regime for the first time (Vite, 2009). This systematic codification and the jurisprudence developed by various international courts and criminal tribunals have commonly accepted that the situation of “armed conflict” exists whenever there is resort to armed force between states or protracted armed violence between state authorities and organized armed groups or between such groups within a state (Prosecutor v. Dusko Tadic, 1995, p. 32). This definition gives rise to two situations: either "International Armed Conflict," wherein two or more sovereign states use force against each other, or "Non-International Armed Conflict," wherein conflicts of internal nature exist within the territorial jurisdiction of the state between armed groups or armed groups and the state itself. This classification of armed conflict into two distinct branches helps to determine the scope of protections available to various actors under international law. It also helps establish the jurisdiction of the Hague-seated International Criminal Court, temporary ad hoc criminal tribunals, like the ICTY or ICTR, established by the United Nations Security Council, or a national court established by an agreement between a state and the United Nations, like the ECCC Khmer Rouge Tribunal, whose only concern is to prosecute the wrongdoings at times of such armed conflicts (Gilani, 2021).

On one hand, International Armed Conflict (IAC) is a situation of “armed hostilities” (Prosecutor v. Jean-Pierre Bemba Gombo, 2009, p. 78) which exists whenever a state uses armed force against another state or its territory, whether through its armed forces or other actors acting on behalf of the State (Triffterer & Ambos, 2016). This is the traditional form of wars like WW I and WW II where states used force against each other, and in this regard, Common Article 2 of the Geneva Convention I states that the convention shall apply to "cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them" (Prosecutor v. Jean Pierre Bemba Gombo, 2009, p. 76). By today, all the countries across the globe have ratified the Geneva Conventions, and hence, while referring to "High Contracting Parties," it simply means all the countries around the world. This implies that if two or more states

participate in armed hostilities, whether may it be declared in the form of war or an undeclared situation of hostile acts, there exists the situation of International Armed Conflict. This scenario does not take into account the intensity of conflict or number of victims, meaning that it exists as soon as a hostile act occurs and there is involvement of armed forces of two states acting on behalf of their government.

On the other hand, Non-International Armed Conflict (NIAC) came into the legal regime only after 1949 through Common Article 3 of the Geneva Conventions. This situation exists whenever there is protracted violence between governmental authorities and organized armed groups or between such armed groups within a state (Prosecutor v. Thomas Lubanga Dyilo, 2012, pp. 242-245). It is distinct from the former category of conflict, provided that this situation as a whole should be protracted in order to distinguish it from riots, isolated and sporadic actions, or cases of internal disturbances within a nation, and such armed hostilities should meet two necessary legal requirements of "intensity" and "organization" (Prosecutor v. Fatmir Limaj et. al, 2005, p. 35). To categorize a situation as a Non-International Armed Conflict, there must be a significant level of intensity in the conflict, and the armed group should be sufficiently organized to carry out military operations. Under legal jurisprudence, the former criterion is assessed on the basis of the attacks spread over territories, over a period of time, attracted the attention of the United Nations Security Council and the mobilization and the distribution of weapons among both parties to the conflict (Prosecutor v. Germain Katanga, 2014, p. 451) and the latter criterion is determinative through the armed group's internal hierarchy, internal rules and regulations, the command structure, the availability of military equipment, and the group's ability to plan a military operation and execute it (Prosecutor v. Ramush Haradinaj et. al, 2008, pp. 32, 33).

Despite both of these armed conflicts being atrocious and violent in nature, they are still conducted within the ambit of laws. Even wars have rules, and not everything is fair in times of war. While there is a fair legal distinction between the two categories of conflicts, there is an absence of a central authority under international law to classify a situation as an armed conflict, so it is one of the primary duties of conflicting parties to determine the applicable legal framework to determine the legality of the conduct of their military operations (How is the term "Armed Conflict" defined in International Humanitarian Law?, 2024, p. 5). Jus in bello, also known as International Humanitarian Law (IHL), refers to such principles governing the methods of armed conflict in order to minimize human suffering to the greatest extent possible. Influenced by religious texts, the Battle of Solferino, and post-World War II criminal trials held in Nuremberg and Tokyo, the Geneva Conventions, the Hague Conventions, their Additional Protocols, various Weapon Conventions, and Military Manuals drafted by various nations to regulate their military together, along with customary international humanitarian law, form the modern-day "Law of Armed Conflict or Laws of War" (Pandey, 2024, p. 272). These rules are relevant to all involved parties in both international and non-international conflicts, since the sole aim of these rules is to make armed conflicts as humane as they can be.

Fifth Domain of Warfare: Introduction, History, and a Modern-Day Reality

After surpassing the conflicts on land, sea, air, and space, humans have started to enter into a new, yet complex and crucial, battlefield of the digital realm. It is one of those examples

where the human mind is said to have limitless and supreme power. While the advancement in science and technology has been a boon to mankind, it is also a bane as these complex technologies are rapidly being applied across a range of military domains, including strategy, defense systems, advanced weapons, and combat tactics, for the purpose of wars. Combat drones, advanced missiles, nuclear & hydrogen weapons, satellites, and lethal autonomous systems are all notable examples of advancements in science and technology in the field of warfare, and upon scrutinising these technologies, they have one thing in common: the use of computer networks and digital infrastructure. Cyberspace has proliferated in almost all aspects of human life in developed countries and is increasingly doing so in the developing world (Rajagopalan & Patil, 2024), and attacking this digital space, at times of war, will lead to some serious consequences and military advantage. Hence, with this realization, countries across the globe have shifted their attention and resources to foster their cyber arms and cyber defence and prepare for the era of cyber war.

While the earliest recorded conflict, like the Battle of the Megiddo, was fought in 1457 BC (Watkins, 2017, p. 10), the world had not witnessed the attacks in the digital domain until the very beginning of the 21st century. The first instances of attacks in the cyber domain came to light when the computer systems of the USA (Bodmer, Kilger, Carpenter, & Jones, 2012) and Estonia (Traynor, 2007) were targeted in 2003 and 2007, respectively. Designated as "Titan Rain" (Taylor, 2007), the 2003 cyberattacks were carried out against the United States Department of Defence and organizations within it, including the Army, Navy, and Space Installations Unit. Similarly, in 2007, after the famous statue of the Bronze Soldier was removed from the center of Tallinn, the capital of Estonia, after gaining independence from the Soviet Union, cyberattacks were launched on Estonia's government and corporate cyber infrastructures. (Sohail, 2022, p. 3). In both of these attacks, government websites were attacked, services denied, and sensitive information was stolen, making it disruptive rather than destructive. While these series of coordinated attacks were looked upon closely by many nations and military planners, it did not divert much attention of international law experts (The Economist, 2007). The debate on cyber warfare among the international legal community only sparked in 2008, during the Russo-Georgian war, when Georgian government sites were attacked with the message “win+love+in+Russia” (Markoff, 2008). This attack was distinctive in nature provided that though Russian officials denied its involvement, it was the first case in the history of warfare that planned and coordinated cyberattacks were concurrently synchronized with other major battle actions in other warfighting domains (Hollis, 2011, p. 2) meaning that while the wars on land, air, and sea were ongoing, the fifth domain of cyberwar came into action alongside. Another classic example of cyber warfare is Operation Olympic Games wherein attacks were directed against the centrifugal apparatus installed for the purification of Uranium in the nuclear facility of Iran (Kamiński, 2020, p. 64). Similarly, cyber operations as a means of modern warfare were also employed during the armed conflicts in Afghanistan (Shane Harris, 2009), Iraq (Markoff & Shanker, Halted ‘03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk”, 2009), Libya (Schmitt & Shankar, 2011) and Syria (Watson, 2011). The 2022 invasion of Ukraine by Russia (Duguin & Pavlova, 2023, p. 6) and the Israel – Iran conflict, both also accompanied by destructive cyber-enabled operations (The Times of Israel, 2024).

Recently, on 17th and 18th September, pagers and radio devices operated by Hezbollah members as a safe means of communication detonated in multiple cities in Lebanon and Syria, resulting in 30 fatalities. Although no state or militant group has claimed responsibility for the attacks, they have largely been attributed to the state of Israel (Hamzeh, 2024). UN experts have condemned this attack by whoever has done it, stating that it violates the principle of the laws of war. The indiscriminate nature of the attack, targeted haphazardly, led to the killing of two children below 11 years of age, who were civilians. On top of that, the IHL prevents the use of "booby traps." Booby traps are those devices which look harmless but are designed to kill or injure, that function unexpectedly when a person performs an apparently safe act (Melzer, 2016, p. 114). In the pager explosion case, people were using the device as a means of communication and performing a safe act of receiving the call, but it led to an explosion. In such a scenario, not only the members of the Hezbollah group but also other civilians using those pagers, at that very particular moment, could also be seriously injured or killed. Be this attack termed as a "cyber-attack" (Gilani I., 2024) or an assault via supply chain (Lin, 2024), it raises serious concern in the international community that even low-tech devices can cause kinetic physical damage. If a pager can be turned into a weapon, then what about day-to-day instruments like smartphones, hearing aids, and pacemakers? If one could disable the working of a pacemaker with just one touch of a button sitting in any part of the world and kill millions of people, humans can only imagine how sophisticated the modern methods of warfare can get. Gone are the days when worldwide interconnectivity was of great utility because interconnectivity now also means that it can be targeted from anywhere in the world, regardless of the border (International Committee of the Red Cross, 2011, p. 36).

Cyber Warfare: Does International Humanitarian Law Apply?

To avoid confusion regarding the applicability of IHL in Cyber Warfare, first it is crucial to demarcate a clear boundary between cyber warfare in the sense of cyber operations and cyber warfare conducted in the context of armed conflicts. Some cyberattacks can be destructive enough but would not come under the ambit of the laws of war, only because they were not associated with or conducted in the context of an armed conflict. Hence, the term “Cyber Warfare”, in this research article, describes only those cyber operations conducted in or amounting to an armed conflict, be it international or non-international. From a more detailed technical perspective, such "cyber operations" entail creating and sending computer code from one or more systems to target systems that may aim to infiltrate a computer network to gather, export, destroy, modify, or encrypt data, or to initiate, change, or otherwise influence processes managed by the compromised system. (Dreoge, 2012, p. 538). The 2008 Georgian cyber-attacks played a decisive role in making analysts and scholars think of the nexus between International Humanitarian Law and attacks in the cyber domain (Tikk, Kaska, & Vihul, 2010, p. 83). It is long established that International Humanitarian Law (IHL) is applicable right from the moment an armed conflict begins and continues to exist after hostilities have ceased until a general peace agreement is reached, in case of an international conflict, or until a peaceful settlement is reached, in case of a non-international conflict. (Separate Opinion of Judge Simmar, Democratic Republic of the Congo v. Uganda, 2005, p. 177). But while the drafters of laws of war had only anticipated governing methods and means of warfare involving the use of kinetic force in the physical world, they were yet unknown about the dynamic nature of the

battlefield. However, general IHL rules and principles regulate all conduct of armed hostilities, including the use of all weapons, and are thus applicable to cyber warfare as well (Diamond, 2014, pp. 69, 70). The authenticity of this statement is tested under a three-pronged analysis.

Firstly, whenever a situation of non liquet arises, especially in the field of humanitarian law, international legal experts refer to the Martens Clause. The insertion of the Martens Clause in the Geneva Conventions and Hague Conventions primarily made IHL of an evolving nature capable of dealing with and adapting to the changing dimensions of warfare (Sohail, 2022, p. 4), and the Hague World Court also acknowledged the positive aspect of its functioning, stating that it has proved to be an effective means of addressing the rapid evolution of military technology (Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, 1996, p. 18). So, when IHL aims to minimize suffering at times of war, it would be illogical and unjust to argue that IHL would not apply to cyber warfare, as it would totally nullify the whole humanitarian objective of jus in bello.

Secondly, the Additional Protocol I to the Geneva Conventions, under Article 35, indicates that the parties to conflict do not have an absolute right to choose the methods or means of warfare and hence must prohibit the employment of methods which can cause superfluous injury or unnecessary suffering. Consequently, in the development and adoption of a new means or method of warfare, Article 36 has set out an obligation on states to determine whether those means or methods of warfare are legal (Jevglevskaja, 2015, p. 112). So, in order to validate this clause, the concept of cyber warfare must fall well within the regime of IHL.

Thirdly, the Tallinn Manual developed by the North Atlantic Treaty Organization (NATO), despite its non-binding nature, acts as the only detailed descriptive document which demonstrates how IHL may be applied to cyber warfare and cyber conflicts (Pascucci, 2017, p. 419). The manual provides that, after fulfilment of some criteria, cyber operations do constitute an attack, and IHL applies. Under Rule 30, the drafters of the manual defined 'cyber-attack', for the purpose of application of IHL, as a cyber-operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects (NATO CCD COE, 2013, p. 92). Hence, the answer to the threshold question of whether the laws of war would apply to the digital regime is concluded with a positive affirmation, thereby upholding the notion of IHL that wars should be made as humane as possible.

Prima facie, the applicability of IHL would be relatively easier to establish if the cyber operations were conducted concurrently with an existing armed conflict compared to amounting those cyber operations as initiation of an armed conflict itself (Diamond, 2014, p. 71). However, complications arise in both of these cases under two major headings: with regard to the non-kinetic nature of cyber operations and to establish sufficient grounds to assert that the methods of cyber warfare were conducted by or on behalf of a party to an armed conflict. However, this paper aims to only scrutinize the first aspect of the non-kinetic nature of the attack and not the attribution part.

Cyber Warfare: A Non-Kinetic "Attack" with Kinetic Consequences

The major feature of cyber warfare is that it is conducted in the digital realm with no use of actual physical force or weapons. In a rather strict sense, the attacker, the victim, and the weapon, all three are just digital systems and data. Under such circumstances, how can cyber

operations, those conducted in or amounting to an armed conflict, be considered an "attack" under the IHL? To determine this aspect, the term "attack" plays a protagonist role as it forms the basis of several general principles and special prohibitions in terms of the application of IHL (Sohail, 2022, p. 5). The Additional Protocol I of the Geneva Conventions, under Article 49 (1), has defined "attacks" as acts of violence against the adversary, whether in offense or in defense. This indicative factor of 'acts of violence' should have a liberal and flexible approach to uphold the notion of IHL. This implies that to elucidate the term 'act of violence' in the regime of cyber warfare, the consequences of the cyber operations must be taken into account rather than the violent nature of such operations. But, in my view, this rationale needs to be further modified and should consider the design, target of such a cyberattack and its intended consequences. Accordingly, cyber operations by means of viruses, worms, etc., that result in physical damage to persons or damage to objects that goes beyond the computer program or data attacked could be qualified as 'acts of violence,' that is, as an "attack" in the sense of IHL (International Committee of the Red Cross, 2011, p. 37). For instance, destroying a dam with the use of bombs or disabling its Automatic Reservoir Monitoring and Control (ARMAC) system through cyber-attack will have the same violent effect of massive flash floods causing destruction of civilian life, property, and the natural environment. Similarly, the use of asphyxiating or poisonous gases during an armed conflict will have the same violent consequences as altering the functioning of a pesticide plant through cyber operations, both leading to mass civilian casualties. In such scenarios, concluding that just because the cyberattack on those infrastructures was not violent or did not involve the use of kinetic force, it should not be deemed as an 'attack' under the rules of IHL, would be totally irrational, provided that the violent effects in both cases are identical.

It is well settled that, in the case of an ongoing international armed conflict, methods of cyber warfare causing violent consequences are prohibited by IHL (Schmitt M., 2020, p. 173). The challenge arises, in the absence of existing armed conflict, when assessing whether a cyber-operation initiated by a state would amount to an international armed conflict. For this assessment, two criteria of attribution and resorting to armed force must be taken into consideration (Dreoge, 2012). The first criterion of attribution makes it clear that the cyber operations must be attributable to the state, meaning that they must have been conducted by state actors or their military, and the second criterion regards the cyber operations must have the same effects as kinetic resort to armed force. The cumulative fulfilment of these two standards would trigger an international armed conflict (Dinniss, 2012, p. 131). We know that international armed conflict, through the physical use of force, does not take into account the intensity, meaning that it exists as soon as the slightest hostile act occurs and there is the involvement of armed forces of two states acting on behalf of their governments. Similarly, in my view, the cyber operations also do not take into account the intensity as soon as it is confirmed that the attack originated from the state actor acting on behalf of the state. This connotes that while IAC has a very low threshold, it is the attribution that plays a major role. For instance, if the Operation Olympic Games directed against the centrifugal apparatus installed for the purification of Uranium in the nuclear facility of Iran would be attributable to a state, with precision, it would lead to the triggering of an international armed conflict even if the attacks were not violent in nature and did not cause any violent effects. This is because the legitimacy of Operation Olympic Games should depend on what it was designed for, what it

targeted, and if the operations were successful, what consequences Iran would see. Due to the cyberattack, Iran's centrifuges experienced around 900 machines being taken out of service, the target was a nuclear facility and if the attacks were unknown to Iran, it could cause deadly consequences leading to nuclear breakdown. To support this view, the ICRC and many state parties have taken the position that a cyber-operation that "disables" an object is also an attack even when it does not cause physical damage (International Committee of the Red Cross, 2024, p. 49).

On the other hand, in the case of non-international armed conflict, the complexity increases with the requirement of fulfilment of "organization" and "intensity" standards. It is well settled that for a non-international conflict to exist, there must be the involvement of at least one-armed group which is properly organized, and the attacks or violence between warring parties must be intense enough to surpass the threshold criterion to qualify such confrontations as NIAC.

For the former part of the "organization" criterion, the jurisprudence laid down by the International Criminal Tribunal for the Former Yugoslavia takes into account a number of factors, like the presence of a command structure, the ability of an armed group to carry out military operations in an organised manner, the ability to recruit and train new members, the level of discipline within the armed group and the group's capacity to speak with one voice (Prosecutor v. Boskoski and Tarculovski, 2008, pp. 91, 92). In the case of cyber warfare, the hackers who conduct cyber operations, even though they are part of an organized armed group, do not necessarily meet in a physical space or get recruitment and training like armed soldiers or maintain discipline and hierarchy within the armed group. In such a case, traditionally, they would not qualify as a part of an armed group, and hence IHL would not apply. However, in my view, as the methods of warfare get sophisticated, so should the interpretation of IHL rules and principles in order to limit the effects of armed conflict. This implies that the group of hackers or the group of people conducting cyber operations within an armed group must be considered as meeting the organization criterion. Comparing with members of conventional armed groups, hackers also do meet in the digital space. They are well trained and recruited through digital platforms in the armed group to conduct cyber operations. Though they do not use sophisticated weapons like machine guns and tanks, they do conduct lethal cyber operations through the use of deadly viruses, worms, and algorithms, which can cause an equivalent level of kinetic damage. While the domain of warfare is wide enough to fit in the cyberspace, the scope of law and principles of IHL must also be interpreted flexibly in order to achieve the humanitarian norms. Hence, when there is an existing NIAC, the cyber operations conducted by the members of an armed group must be regulated by IHL. But the problem arises when the physical presence of such an armed group is totally null, meaning that the armed group has no combatants to fight on land, but only in digital space. In such a case, it would be very ambiguous to interpret the application of laws of war to such armed groups, wherein they are not actually physically armed but just digitally armed.

Now for the latter part of the "intensity" criterion, to determine whether the conflict was of sufficient intensity, the ICTY considered factors like the extent of material destruction, seriousness of attacks, extent of government forces mobilization, spread over geographical area, period of time, types of weapons used, and an upsurge in armed clashes over a period of

time (Prosecutor v. Ramush Haradinaj et. al., 2008, pp. 27, 28). To date, no cyber operations have reached the 'intensity' threshold and the Tallinn Manual also acknowledges the fact that cyber operations single-handedly can trigger a non-international armed conflict, but only in exceptional cases (NATO CCD COE, 2013, p. 78). Cyber operations, which are sporadic, despite causing serious injury or destruction, do not suffice the intensity criterion (NATO CCD COE, 2013, p. 77). The threshold in NIAC is relatively very high as compared to IAC for a cyber-operation to trigger IHL, and hence only the rarest case might sneak its way to the top.

Conclusion

While the first digital computer was invented in 1945, the concept of war in cyberspace evolved just around the same time, in the last few decades. Efforts are being made in the international arena to govern the method of cyber warfare and how this digital regime can be brought under the purview of IHL. The Tallinn Manual, developed by NATO, is the only comprehensive document developed by 20 experts, but it lacks binding effect as it is not made by state consensus. The Tallinn Manual does not reflect the opinion of states but of those 20 experts in the field of digital regime. However, sovereign states have started to develop their own form of cyber war guidelines, like the USA publishing its Department of Defence's Cyber Strategy and the French Ministry of the Armies releasing their own version of International Law Applicable to Operations in Cyberspace. States like the United Kingdom, Australia, Estonia, New Zealand, and the Netherlands have also aligned with and endorsed the Tallinn Manual to govern the conflicts in cyberspace. Although there is no comprehensive legal instrument or convention regulating cyberwarfare, certain customary laws and principles of humanitarian law–such as distinction, proportionality, humanity, and military necessity–must be respected and upheld by all states, regardless of the domain in which they clash. President of Microsoft Corporation, Brad Smith, in 2017, called for the extension of a ‘Digital Geneva Convention’ to protect civilians and civilian objects from the deadly consequences of cyberattacks (Smith, 2017). Amidst the existing armed conflicts, states should be more interested in benefitting from interconnectivity rather than making it a battle zone to cause destruction. The methods of warfare have advanced, and so should the rules of war, so as to maintain the notion of 'Even wars have Rules.'

References

Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons (International Court of Justice July 8, 1996). Retrieved from https://iilj.org/wp-content/uploads/2016/08/Legality-of-the-Threat-or-Use-of-Nuclear-Weapons-1996.pdf

Bernard, V. (2012). Science cannot be placed above its consequences. *International Review of the Red Cross, 94*(886), 458.

Bodmer, S., Kilger, M., Carpenter, G., & Jones, J. (2012). *Reverse Deception: Organized Cyber Threat Counter-Exploitation.* New York: McGraw Hill Publishers.

Diamond, E. (2014). Applying international humanitarian law to cyber warfare. *Law and National Security: Selected Issues*, 69. Retrieved from https://www.jstor.org/stable/resrep08957.8

Dinniss, H. H. (2012). *Cyber Warfare and the Laws of War.* Cambridge: Cambridge University Press.

Dreoge, C. (2012). Get off cloud: Cyber warfare, International Humanitarian Law and the Protection of Civilians. *International Review of the Red Cross*, 533.

Duguin, S., & Pavlova, P. (2023). *The Role of Cyber in the Russian War against Ukraine: Its Impact and the Consequences for the Future of Armed Conflict.* Brussels: Directorate General for External Policies of the European Union.

Gilani, I. (2024, September 18). *Deadly Cyberattack in Lebanon Reveals the New Face of Warfare.* Retrieved from Frontline: https://frontline.thehindu.com/news/lebanon-hezbollah-cyber-attack-pager-explosions-warfare-israel-gaza/article68654302.ece

Gilani, N. (2021, August 12). *The Classification of Conflicts in International Humanitarian Law.* Retrieved from DLP Forum: https://www.dlpforum.org/2021/08/12/the-classification-of-conflicts-in-international-humanitarian-law/

Hamzeh, W. (2024, September 19). Pager and walkie-talkie attacks on Hezbollah look like war crimes – international legal expert. Retrieved from *The Conversation*: https://theconversation.com/pager-and-walkie-talkie-attacks-on-hezbollah-look-like-war-crimes-international-legal-expert-239408

Hollis, D. (2011). Cyberwar case study: Georgia 2008. *Small Wars Journal*, 2.

Holmes, O. (2024, October 2). Iranian Strikes on Israel: What Happened and Why did Iran Attack? Retrieved from *The Guardian*: https://www.theguardian.com/world/2024/oct/02/iranian-strikes-on-israel-what-happened-why-did-iran-attack-missiles-damage-what-next

ICRC Geneva. *How is the term "Armed Conflict" defined in International Humanitarian Law?* Retrieved from International Committee of the Red Cross Onion Paper 2024. https://www.icrc.org/sites/default/files/document_new/file_list/armed_conflict_defined_in_ihl.pdf

International Committee of the Red Cross. (2011). International Humanitarian Law and the challenges of contemporary armed conflicts. *31st International Conference of the Red Cross and Red Crescent* (pp. 1-53). Geneva: ICRC. Retrieved from https://www.rulac.org/assets/downloads/2011_Contemporary_Challenges_report.pdf

International Committee of the Red Cross. (2024). *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts.* Geneva: ICRC. Retrieved from https://rcrcconference.org/app/uploads/2024/09/34IC_10.6-IHL-Challenges-Report-EN.pdf

Jevglevskaja, N. (2015). Legal Review of New Weapons: Origins of Article 36 of AP I. *Finnish Yearbook of International Law*, 109-140. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3803709

Kamiński, M. A. (2020). Operation "Olympic Games." Cyber-sabotage as a tool of American intelligence aimed at counteracting the development of Iran's nuclear programme. *Security and Defense Quarterly, 20*, 64. Retrieved from https://securityanddefence.pl/pdf-121974-52879?filename=Operation%20_Olympic.pdf

Lin, H. (2024, October 2). *Reflections on the Lebanon Pager Attack.* Retrieved from LawFare: https://www.lawfaremedia.org/article/reflections-on-the-lebanon-pager-attack

Markoff, J. (2008, August 12). Before the gunfire, cyberattacks. Retrieved from *The New York Times*: https://www.nytimes.com/2008/08/13/technology/13cyber.html

Markoff, J., & Shanker, T. (2009, August 1). Halted 03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk. Retrieved from *New York Times*: https://www.nytimes.com/2009/08/02/us/politics/02cyber.html

Melzer, N. (2016). *International Humanitarian Law: A Comprehensive Introduction.* Geneva: ICRC. Retrieved from https://www.jep.gov.co/sala-de-Prensa/Documents/4231_002-IHL_WEB_13.pdf

NATO CCD COE. (2013). *Tallinn Manual on the International Law applicable to Cyber Warfare.* New York: Cambridge University Press. Retrieved from https://csef.ru/media/articles/3990/3990.pdf

Pandey, A. (2024). Protection of natural environment and cultural property during armed conflict: An international humanitarian law perspective. *Unity Journal, 5*, 272. Retrieved from https://www.nepjol.info/index.php/unityj/article/view/63222/47777

Pascucci, C. P. (2017). Distinction and proportionality in cyber war: Virtual problems with a real solution. *Minnesota Journal of International Law*, 419-460.

Prosecutor v. Boskoski and Tarculovski, IT-04-82-T. International criminal tribunal for the Former Yugoslavia July 10, 2008. Retrieved from https://www.refworld.org/jurisprudence/caselaw/icty/2008/en/61641

Prosecutor v. Dusko Tadic, IT-94-1-A. International criminal tribunal for the former Yugoslavia October 2, 1995. Retrieved from https://www.refworld.org/jurisprudence/caselaw/icty/1995/en/61438

Prosecutor v. Fatmir Limaj et. al, IT-03-66-T. International criminal tribunal for the former Yugoslavia November 30, 2005.

Prosecutor v. Germain Katanga, ICC-01/04-01/07-3436. International criminal court March 7, 2014. Retrieved from https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2015_04025.PDF

Prosecutor v. Jean-Pierre Bemba Gombo, ICC-01/05-01/08-424. International criminal court June 15, 2009. Retrieved from https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2009_04528.PDF

Prosecutor v. Ramush Haradinaj et. al, IT-04-84-T. International criminal tribunal for the former Yugoslavia April 3, 2008. Retrieved from https://www.refworld.org/jurisprudence/caselaw/icty/2008/en/61839

Prosecutor v. Ramush Haradinaj, Idriz Balaj and Lahi Brahimaj, IT-04-84-T. International Criminal Tribunal for the Former Yugoslavia April 3, 2008. Retrieved from https://www.refworld.org/jurisprudence/caselaw/icty/2008/en/61839

Prosecutor v. Thomas Lubanga Dyilo, ICC-01/04-01/06-2842. International criminal court March 14, 2012. Retrieved from https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2012_03942.PDF

Rajagopalan, R. P., & Patil, S. (2024). Future warfare and critical technologies: Evolving tactics and strategies. *ORF and Global Policy Journal*, 46. Retrieved from https://swfound.org/media/207797/future-warfare-and-critical-technologies_feb-2024.pdf

Rustad, S. A. (2024). *Conflict Trends: A Global Overview, 1946–2023*. Peace Research Institute Oslo (PRIO). Retrieved September 5, 2024, from https://www.prio.org/publications/14006

Schmitt, E., & Shankar, Y. (2011, October 17). U.S. debated cyber warfare in attack plan on Libya. Retrieved from *The New York Times*: https://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?hp;

Schmitt, M. (2020). International humanitarian law and the conduct of hostilities. In B. Saul, & D. Akande, *The Oxford Guide to International Humanitarian Law* (p. 173). Oxford: Oxford University Press.

Separate Opinion of Judge Simmar, Democratic Republic of the Congo v. Uganda (International Court of Justice December 19, 2005).

Shane, H. N. (2009). The cyber war plan. *National Journal* .

Smith, B. (2017). The need for a digital Geneva Convention. *RSA Conference.* San Francisco.

Sohail, H. (2022). Fault lines in the application of international humanitarian law to cyber warfare. *Journal of Digital Forensics, Journal of Digital Forensics, Security and Law*, 3. Retrieved from ttps://commons.erau.edu/jdfsl/vol17/iss1/8

Taylor, R. N. (2007, September 5). Titan rain - how Chinese hackers targeted Whitehall. Retrieved from *The Guardian*: https://www.theguardian.com/technology/2007/sep/04/news.internet

The Economist. (2007, May 24). Cyber Warfare is becoming scarier. Retrieved from *The Economist*: https://web.archive.org/web/20081209081836/http://www.economist.com/world/international/displaystory.cfm?story_id=E1_JNNRSVS

The Editors of Encyclopaedia Britannica. (2017, November 27). *Weapon of Mass Destruction*. Retrieved from https://www.britannica.com/technology/weapon-of-mass-destruction

The TImes of Israel. (2024, October 15). *Iran Cyberattacks Against Israel Surged After Gaza War Started, Microsoft Reports*. Retrieved from The TImes of Israel: https://www.timesofisrael.com/iran-cyber-attacks-against-israel-surged-after-gaza-war-started-microsoft-reports/

Tikk, E., Kaska, K., & Vihul, L. (2010). *International Cyber Incidents: Legal Considerations*. Tallinn: Cooperative Cyber Defence Centre of Excellence (CCD COE). Retrieved from https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf

Traynor, I. (2007, May 17). Russia accused of unleashing cyberwar to disable Estonia. Retrieved from *The Guardian*: https://www.theguardian.com/world/2007/may/17/topstories3.russia

Triffterer, O., & Ambos, K. (2016). Rome Statute of the International Criminal Court: A Commentary. In M. Cottier, *Elements of War Crime* (p. 305).

Vite, S. (2009). Typology of armed conflicts in International Humanitarian Law: Legal concepts and actual situations. *International Review of the Red Cross, 91*, 72. Retrieved from https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/irrc-873-vite.pdf

Watkins, J. (2017). *The Greatest Battles in History: An Encyclopedia of Classic Warfare From Megiddo To Waterloo.* London: Amber Books Ltd.

Watson, I. (2011, November 22). *Cyberwar Explodes in Syria.* Retrieved from CNN: https://edition.cnn.com/2011/11/22/world/meast/syria-cyberwar/;

-◆◆◆-