SAFEGUARDING CIVILIANS IN THE DIGITAL BATTLEFIELD: THE ROLE OF IHL IN REGULATING CYBER WARFARE AND ICT-DRIVEN THREATS

Nkechinyere Huomachi Worluh-Okolie, Ph.D. (JP), Senior Lecturer, Faculty of Law, Department of Public Law, Benson Idahosa University, Benin City, Nigeria. ORCID iD: 0009-0007-6794-7468. ORCID record is https://orcid.org/0009-0007-6794-7468

Joseph-Asoh, Chukwudemebi Okoye, PhD. Senior Lecturer, Faculty of Law, Department of Public Law, Benson Idahosa University, Benin City, Edo State, Nigeria.

ABSTRACT

This paper examines the applicability and effectiveness of International Humanitarian Law (IHL) in addressing the rising challenges posed by Information and Communication Technologies (ICTs) in armed conflicts. Utilizing a doctrinal research methodology, it analyzes core IHL instruments such as the Geneva Conventions, Additional Protocols, and customary principles, alongside emerging interpretations like the Tallinn Manual 2.0. The research highlights that while IHL prohibits indiscriminate attacks and mandates the protection of civilians, significant legal and practical gaps exist concerning cyber operations, digital espionage, and misinformation. These gaps are exacerbated by challenges in attribution, enforcement, and definitional ambiguity around cyber "attacks." The paper concludes that although IHL remains fundamentally relevant, evolving cyber threats require reinterpretation of existing norms, international cooperation, digital literacy, and the formulation of clear civilian data protection protocols. Ultimately, it calls for a reinvigoration of humanitarian protections to ensure that civilians remain safeguarded in both kinetic and digital domains.

Keywords: International Humanitarian Law, Cyber Warfare, Civilian Protection, Armed Conflict, Geneva Conventions.

1.0 Introduction

Safeguarding civilians is a fundamental objective of International Humanitarian Law (IHL), which aims to protect individuals who are not involved in hostilities from the consequences of armed conflict, ensuring their security and dignity. However, with the growing shift of warfare into the digital sphere, civilians are now exposed to unprecedented and complex threats.[1]

Advancements in technology have transformed the nature of contemporary warfare, presenting emerging threats that complicate the implementation of International Humanitarian Law. The rise of cyber warfare, AI-powered weapon systems, and widespread digital surveillance has increasingly obscured the distinction between military and civilian spheres, heightening concerns over the safety of non-combatants and the security of essential infrastructure.[2] Traditional IHL principles, such as distinction, proportionality, and military necessity were developed in the context of conventional warfare and now face interpretational challenges in the digital battlefield.[3]

Cyber operations can disrupt essential civilian services, including healthcare, electricity, and communication networks, without causing direct physical destruction. The 2010 Stuxnet attack on Iran's nuclear program and the 2017 WannaCry ransom ware incident illustrate the potential of cyber threats to destabilize critical systems and impact civilian populations.[4] Despite these risks, there remains no universally accepted definition of cyber-attacks under IHL, complicating enforcement and accountability efforts.

While the Geneva Conventions and Additional Protocols prohibit indiscriminate attacks and emphasize civilian protection, their applicability to cyber warfare remains contested. The International Committee of the Red Cross (ICRC) has emphasized that existing IHL rules must govern cyber operations, but gaps in interpretation persist.[5] Scholars argue that new legal frameworks or explicit state agreements are necessary to ensure adequate protections in the

[1] Kubo Mačák and Florentina Pircher, "Protecting civilians from harm caused by cyber operations during armed conflicts" <https://www.exeter.ac.uk/v8media/facultysites/hass/law/Macak__Pircher_-_Protection_of_civilians_against_cyber_harm_-_ECIL_WP_2025-1.pdf> accessed 11 April 2025

[2] M. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, (Cambridge University Press, 2017).

[3] Y. Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict*, (Cambridge University Press. 2021).

[4] E. Tikk-Ringas, "The Legal Challenges of Cyber Warfare" *Harvard Journal of International Law*,(2016) 58(4), 289-312.

[5] ICRC, "Cyber Warfare and International Humanitarian Law: The ICRC's Perspective" *International Committee of the Red Cross* (2019).

digital age.[6] Customary international humanitarian law, as compiled by the ICRC, supports the extension of IHL principles to cyber warfare and emerging technologies, even in the absence of specific treaties.[7]

Accordingly, this paper critically assesses the adequacy of IHL in responding to ICT-driven threats in armed conflict. It identifies key legal ambiguities, enforcement challenges, and the operational complexities surrounding cyber warfare. While existing legal frameworks provide essential foundational protections, they fall short in fully addressing the nuanced realities of technologically advanced conflict. The paper emphasizes the need for enhanced legal interpretation, proactive roles by states and international organizations, and innovative approaches to ensure that humanitarian norms are upheld in cyberspace. Ultimately, it calls for greater international cooperation, clearer definitions, and more robust mechanisms to protect civilians in both physical and digital theaters of war.

2.0 Background and Context

2.1 International Humanitarian Law

International Humanitarian Law is characterized by its function of regulating the use of force in armed conflicts. This regulation aims to achieve two main objectives: firstly, to protect those who are not directly involved in hostilities[8] or who have ceased their participation;[9] and secondly, to limit the use of violence to what is essential to achieve the objectives of the conflict, which is primarily to diminish the enemy's military capabilities, regardless of the causes being fought for.

From this definition, several fundamental principles of IHL emerge:

---

[6] J. Kubo, “Cyber Operations and IHL: Bridging the Legal Gaps." *Journal of Conflict & Security Law*, (2020) 25(2), 135-157.

[7] ICRC, Customary International Humanitarian Law, Rule 144.

[8] International Humanitarian Law (IHL) indeed sets a high threshold for defining "participation" in armed conflicts. It doesn't consider mere causal contributions to the war effort as constituting participation. Instead, it focuses on the direct involvement in military violence or the implementation of the final element in the causality chain, which is the application of military force. This means that simply providing support, resources, or assistance to a party involved in a conflict may not necessarily be regarded as direct participation according to IHL. Rather, the law primarily concerns itself with individuals who are directly engaged in military activities or violence, such as combatants actively fighting in battles or carrying out military operations. By delineating participation in this manner, IHL aims to ensure that individuals who are not directly involved in armed conflict, such as civilians or non-combatants, are spared from the dangers and consequences of war as much as possible. This approach underscores IHL's fundamental commitment to protecting those who are not actively engaged in hostilities and minimizing the impact of armed conflict on civilian populations.

[9] For example, those who have surrendered (i.e., in international armed conflicts, prisoners of war) or can no longer participate (such as the wounded and sick).

a) *Distinction between civilians and combatants*: This principle requires parties to distinguish between individuals who are taking part in hostilities and those who are not, ensuring that civilians are not targeted during conflicts. In cyber warfare, the challenge arises in distinguishing between military and civilian infrastructure that may rely on interconnected digital systems. A cyberattack targeting a military command center could unintentionally affect civilian hospitals, power grids, or financial networks, blurring the lines of distinction.

b) *Prohibition of attacking those who are hors de combat*: Hors de combat refers to individuals who are incapacitated or no longer participating in hostilities, such as wounded soldiers or prisoners of war. Attacking such individuals is strictly prohibited under IHL.

c) *Prohibition of inflicting unnecessary suffering*: IHL prohibits the use of weapons or tactics that cause unnecessary harm or suffering to combatants or civilians.

d) *Principle of necessity*: This principle mandates that the use of force must be necessary to achieve legitimate military objectives and must not go beyond what is required to accomplish those objectives.

e) *Principle of proportionality*: According to this principle, the anticipated military advantage of an attack must be balanced against the potential harm to civilians or civilian objects. The use of force must not be disproportionate to the expected military gain.[10] In cyber-attacks, this is particularly challenging as the scale of damage caused by a cyber-operation may not always be immediately apparent, and the long-term consequences such as data manipulation or the disruption of essential services may be far-reaching.

f) *Precautions in Attack*: Parties must take all feasible precautions to avoid or minimize harm to civilians and civilian objects. In the realm of cyber warfare, this requires states to ensure that their cyber operations do not intentionally or negligently target civilian systems, such as medical facilities or infrastructure vital for civilian life.

These principles form the foundation of International Humanitarian Law and guide the conduct of parties involved in armed conflicts, aiming to mitigate the human suffering caused by

[10] ICRC, 'Fundamental Principles of IHL' <https://casebook.icrc.org/a_to_z/glossary/fundamental-principles-ihl#:~:text=the%20principle%20of%20distinction%20between,superfluous%20injury%20and%20unnecessary%20suffering> accessed 16 May 2024

warfare while also maintaining a level of military effectiveness necessary for achieving legitimate objectives.[11] In the digital age however, applying these principles becomes more complex, as cyber-attacks can be executed remotely and anonymously, making attribution difficult and increasing the potential for collateral damage.[12]

2.2 Technological Developments in Warfare

The integration of Information and Communication Technologies (ICTs) into military strategies has dramatically reshaped the landscape of modern warfare. Over the past few decades, the rapid evolution of ICTs has not only enhanced the operational capabilities of armed forces but also introduced novel methods of conducting hostilities that transcend traditional definitions of armed conflict.[13] Cyber operations,[14] autonomous weapons systems,[15] and digital surveillance mechanisms[16] have become integral to contemporary military doctrines, fundamentally altering the nature, scope, and reach of warfare.

This technological transformation presents unprecedented challenges for the application of International Humanitarian Law (IHL), which was primarily developed in the context of kinetic warfare. As the battlefield increasingly extends into cyberspace, new forms of civilian vulnerability have emerged ranging from cyber warfare, digital espionage and misinformation

[11]IHL Databases International Humanitarian Law Databases, Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949. Commentary of 2016 <https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949/article-63/commentary/2016> accessed 16 May 2024

[12] M.N. Schmitt, "Cyber Operations and International Law" *Journal of Conflict and Security Law* (2013) (3) (2) 19 - 28.

[13] Z. Veličković, D. Stanojević, & D. Kostić, *The Role of Modern Technologies in Military Conflicts of the 21st Century* < https://www.researchgate.net/publication/367000797> Accessed April 11, 2025.

[14] Cyber operations have emerged as a new frontier in armed conflict. These operations involve the use of digital means to disrupt, damage, or manipulate the functioning of critical infrastructure, such as power grids, communication systems, and financial institutions. See: M.N. Schmitt, "Cyber Operations and International Law" *Journal of Conflict and Security Law* (2013). High-profile incidents such as the Stuxnet attack in 2010, which targeted Iran's nuclear enrichment facilities, exemplify how cyberattacks can cause significant damage to both military and civilian targets without physical violence. See: J.R. Lindsay, "Stuxnet and the Limits of Cyber Warfare" *Journal of International Security Studies* (2013)

[15] Autonomous weapons systems (AWS) are another key technological advancement in modern warfare. These systems, which can operate independently of human control, are designed to select and engage targets without human intervention. While they hold the potential to reduce human casualties, they also raise significant ethical and legal concerns regarding accountability, proportionality, and distinction in armed conflict. See: R. Arkin, "The Ethics of Autonomous Military Systems" In S. H. R. B. S. A. A. Oswell (Ed.), *The Future of War: A History* (Springer).

[16] Digital surveillance has further expanded military reach by allowing real-time monitoring and tracking of both combatants and civilians. These technologies enable military forces to collect vast amounts of data, monitor enemy movements, and predict actions, thus enhancing military strategy. However, they also pose privacy risks and contribute to the erosion of civil liberties, especially in conflict zones. See: E. Bakker, & C. Rijken," The Impact of Digital Surveillance in Armed Conflict" *Journal of Digital Warfare* (2019).

campaigns to cyber-attacks on critical infrastructure such as hospitals, power grids, and communication systems.[17]

Cyber warfare refers to the use of digital attacks by one nation-state to disrupt the vital computer systems of another, with the intent of causing damage, disruption, or espionage. These attacks are often executed via malware, ransom ware, denial-of-service attacks, or other malicious code to damage infrastructure, steal sensitive data, or disrupt services.[18] It typically includes:

a. Denial-of-Service (DoS) attacks that disable government or military websites;

b. Malware infections that corrupt or extract sensitive data;

c. Cyber espionage aimed at stealing classified information;

d. Cyber sabotage, targeting utilities, banks, or transportation systems.

Cyber warfare blurs the line between war and peace because it often occurs during times of political tension rather than outright armed conflict.[19] It presents unique challenges to international law. The United Nations Charter, particularly Article 2(4), prohibits the use of force between states; however, it is unclear whether a cyber-attack qualifies as such. This ambiguity complicates state responses and accountability.[20]

Another conceptual dilemma arises when civilians participate in cyber hostilities, such as "hacktivists" during armed conflict. Such civilians may lose protection under Article 51(3) of Additional Protocol I, which states that civilians are protected "unless and for such time as they take a direct part in hostilities." However, determining when a digital action constitutes "direct participation" is contentious and not clearly codified.[21]

Cyber warfare is also addressed under International Humanitarian, where the key concern is whether cyber operations cause effects comparable to kinetic warfare such as destruction, injury, or death.[22]

[17]Z. Veličković, D. Stanojević, &D. Kostić, *Ibid*.
[18] *Oxford Dictionary of English*, 3rd edn (Oxford University Press, 2010) 362.
[19] M Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013).
[20]T. Rid, 'Cyber War Will Not Take Place' (2012) 35(1) *Journal of Strategic Studies* 5.
[21] N. Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, (ICRC, 2009).
[22]R. Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17(1) *Journal of Conflict and Security Law* 211.

2.3 Relevance of the Geneva Conventions and Additional Protocols

The Geneva Conventions of 1949 and their Additional Protocols of 1977 have long provided the primary legal framework for the conduct of armed conflict, particularly in safeguarding civilians, wounded soldiers, prisoners of war, and other persons not actively participating in hostilities. Protocol I extends protection in international armed conflicts, while Protocol II addresses non-international conflicts. Together, they codify critical principles of international humanitarian law (IHL), such as the distinction between civilian and military targets, the prohibition of indiscriminate attacks, and the protection of civilian infrastructure.[23]

However, the advent of cyber warfare presents complex and novel challenges that stretch the traditional application of these legal instruments. The Geneva Conventions were conceived in an era when armed conflict was defined primarily by physical violence and the occupation of territory.[24] Consequently, their provisions focus largely on physical harm and tangible objects, leaving a gap in how they address the unique characteristics of ICT-driven warfare, such as cyber-attacks on digital networks and data-based infrastructure. For instance, Article 53 of Additional Protocol I protects cultural objects and places of worship, yet it is silent on data repositories or digital communication systems, which, in today's interconnected society, serve critical civilian functions.[25]

The principle of distinction central to IHL requires parties to a conflict to differentiate between combatants and civilians, and between military and civilian objects. While clear in kinetic warfare, this principle becomes blurred in cyberspace where infrastructure often serves dual-use purposes, such as hospitals using the same communication networks as military facilities. The protection of such infrastructure under the Geneva framework is therefore under strain in the digital age.[26]

In this context, the Martens Clause, which appears in both the preamble of the 1899 Hague Convention II and in Article 1(2) of Additional Protocol I, becomes increasingly significant. It provides that in cases not covered by existing treaties, civilians and combatants remain under the protection of the principles of humanity and the dictates of public conscience.[27] This clause

[23] Geneva Convention I-IV (adopted 12 August 1949, entered into force 21 October 1950), 75 UNTS 31, 85, 135, 287; Protocol Additional to the Geneva Conventions of 12 August 1949 (Protocol I) (adopted 8 June 1977), 1125 UNTS 3.
[24] *Ibid*.
[25] Protocol I (n 1) art 53.
[26] Protocol I (n 1) art 1(2); see also Hague Convention II (1899), preamble.
[27] H. Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press 2012) 16–18.

offers a normative foundation to extend IHL protections to the cyber domain, particularly when cyber operations cause humanitarian consequences comparable to conventional attacks, even if they do not produce kinetic damage.

Legal scholars and institutions have begun addressing this gap through interpretive mechanisms. The *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, produced by the NATO Cooperative Cyber Defence Centre of Excellence, is one such effort. It affirms that the rules of IHL apply to cyber operations conducted during armed conflict, including the principles of distinction, proportionality, and precautions in attack.[28] According to Rule 92 of the Manual, a cyber-attack that disables critical civilian infrastructure may be deemed unlawful if it results in excessive harm to civilians relative to the anticipated military advantage.[29]

Despite these evolving interpretations, practical challenges remain. One major issue is attribution that is, accurately identifying the origin and perpetrators of a cyber-attack. Many operations are conducted by non-state actors or by state proxies under a veil of anonymity, complicating the assignment of legal responsibility. Additionally, the inherently borderless and decentralized nature of cyberspace makes enforcement of IHL more difficult than in traditional settings.

Although the Geneva Conventions and their Additional Protocols were not originally designed for the digital battlefield, their fundamental humanitarian principles remain relevant. Through evolving interpretations, particularly supported by the Martens Clause and contemporary commentaries like the *Tallinn Manual 2.0*, there is a legal and moral basis for applying IHL to cyber warfare. However, to ensure effective protection of civilians in the digital age, the international legal community must continue clarifying these norms and considering the development of complementary instruments tailored to cyber threats.

3.0 Application of IHL Principles in Contemporary Cyber Warfare

The International Committee of the Red Cross[30] defines Cyber Warfare as the operations against a computer or computer system through a data stream, when used as a means and methods of warfare in the context of an armed conflict as defined under IHL. It also describes

[28] Michael N. Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) 445–450. (Rules 92–94)
[29] *ibid* Rule 92.
[30] ICRC, "International Humanitarian Law and The Challenges of Contemporary Armed Conflicts", 32*nd* *International Conference of The Red Cross and Red Crescent*, EN 321C/15/11 (2015) pp41-42.

cyber warfare as "the use of cyber means by a state to cause injury, death or damage to property in this course of an armed conflict or during peacetime.

Hence cyber operation is now referred to as the 5th domain of warfare in which a belligerent state, be it between their selves or against non-state actors, use it as a battlefield to conduct their hostile act. Thus the domain of warfare has expanded beyond the physical realms of land, sea, air, and outer space, in today's interconnected world and with the development of technology, the cyberspace has become a unique domain of warfare, therefore attacks carried out on cyberspace can amount to armed conflict.[31] According to North Atlantic Treaty Organization (NATO),[32] cyber operation refers to cyber-attacks that are carried out as a part of a military operation and are intended to cause physical damage or destruction, or to disrupt military operations.

This paper will examine the application of these foundational IHL principles to cyber warfare in turn:

3.1 Cyber Operation and Principle of Distinction

Under the principle of distinction, IHL stipulates that parties to an armed conflict are obligated to distinguish at all times between the civilian population and combatants, and between civilian objects and military objectives. The purpose of this distinction is because combatants or military objectives are the only lawful targets for an attack while it is unlawful in IHL to make civilians and civilian objects targets of an attack. This basic rule of distinction is enshrined in AP I Article 48. In its Nuclear Weapons Advisory Opinion, the ICJ held that the principle of distinction is 'the cardinal principle contained in the text constituting the fabric of humanitarian law.'[33] Accordingly, cyber operations must only be directed at military objectives, and where attacks are directed at civilian infrastructures it would amount to a breach of this principle.

Under international humanitarian law the only object that can be lawfully attacked is military object which will contribute to their military advantage if captured, destroyed or neutralized.[34]Thus any attack to an object not classified under a military object is deemed a civilian object and such attacks are prohibited. [35] In the context of the cyber domain of warfare,

[31] J. Hampel, "The Invisible War: How Cyberspace Is Shaping Global Conflicts" https://www.linkedin.com/pulse/invisible-war-how-cyberspace-shaping-global-conflicts-hempel-xlsoc. [Accessed 27th December, 2024].
[32] NATO's Glossary of Terms and Definitions, p 2-C-11.
[33] Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 256 (July 8)
[34] Art 52(2) AP I
[35] *Ibid*

a lawful cyber-attack is deemed as one which only attacks military cyber infrastructures which would confer a definite military advantage.[36]

The main difficulty in applying this principle to cyber warfare lies in the fact that most cyber infrastructure on the cyberspace is dual use, serving both civilian and military purposes. The currently prevailing position is that dual use objects are military objectives because of the military purpose they serve.[37] When applied to cyberspace, this position implies that cyber infrastructure which is of dual use to both the civilian population and the military should be classified as military objectives and, could be susceptible to attack. For instance, the cables, nodes, routers, and satellites on which so many civilian systems depend would all be deemed military objectives because they have the dual function of transmitting military information.[38] Thus, with so many objects in the cyber realm considered military objectives, the principle of distinction becomes largely devoid of protective value. Even civilian cyber infrastructure that is not dual use, protected from direct attack might nevertheless be vulnerable to harm because of the interconnectedness of cyberspace.[39]

In order to avoid this outcome, IHL places a prohibition on indiscriminate Cyber-attacks[40]. Belligerent parties during cyber warfare are prohibited from employing cyber weapons that are indiscriminate by nature, such as malware computer programs that replicate without control (for instance viruses, worms) and whose harmful effects could not be limited as required by IHL. Furthermore, a belligerent intending to mount a cyber-attack would have to first verify that in the given circumstances, the cyber weapon employed can be and is in fact directed at a military objective and that its effects can be limited as required by IHL.

For instances, a cyber-attack by a group of threat actors going by the name Sandworm executed this attack by targeting the power grid of Ukraine's capital city, this group employed a malware called the Black Energy 3, which greatly affected the national power grid of Ukraine especially western Ukraine. This incident occurred on 23rd December 2015, plunging the city- about one-fifth of Kyiv into darkness. Such attack was purposely driven toward hampering the Ukraine

[36] Z. Chang, "Cyberwarfare and International Humanitarian Law", *Creighon International and Comparative Law Journal,* (2017). Vol 9, No 1
[37] TALLINN Manual, Commentary on Rule 39, para 1
[38] N. S. Maliha, *Cyber Warfare: Challenges In The Application Of International Humanitarian Law To Virtual Conflict* avaliable at https://www.researchgate.net/publication/343979992_Cyber_Warfare_Challenges_In_The_Application_Of_International_Humanitarian_Law_To_Virtual_Conflict/link/. [Accessed 17th January 2025].
[39] *Ibid*
[40] Art 51(4) AP I

government however this greatly affected many civilian infrastructure such as bank and hospitals located in western Ukraine, and this was due to the inability of the attack by the non-state actor to discriminate and distinguish.[41]

3.2 Cyber Operation and Principle of Proportionality

This principle is employed when fighting a just war. It comes into effect when it becomes impossible to not have civilian casualties when an attack is launched against a military object used for dual purposes. In such cases, a lawful attack on a military target may result in collateral damage and also result in incidental loss of civilian lives. The principle of proportionality is encapsulated in Art 51(5) (b) of Additional Protocol 1 and customary international law. This principle prohibits attacks 'which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination of both, which would be excessive in relation to the concrete and direct military advantage anticipated'[42] It further provides that belligerents should are mandated to cancel or suspend an attack if it becomes apparent that the objective is not a military one or is subject to special protection or that the attack may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects which would be excessive in relation to the concrete and direct military advantage anticipated.'[43]

The principle of proportionality aims at striking an acceptable balance between direct and concrete military advantage on one hand and civilian loss or injury on the other hand. While carrying out an attack on a military objective, belligerents must weigh the military advantage they seek to achieve against the level of damage that could affect the civilian population. Where the incidental loss and injury to civilians outweighs the expected military advantage, then such attack is prohibited. But where the military advantage expected is proportionate or greater, compared to the little civilian casualties, such attack will not be prohibited. In the context of cyber operation, cyber-attacks which are not proportionate and expected to cause collateral damage to civilian infrastructure when directed at a military objective is highly prohibited by IHL.

However, there are some challenges while applying this principle: one of which would be to determine whether the incidental damage to civilian objects that may be expected is excessive

[41] Birchwood University "Cyber Attack in Ukraine" <https://www.birchwoodu.org/top-10-real-world-case-studies-on-cyber-security-incidents.> Accessed 3rd January , 2025
[42] Art 51(5)(b) AP I; CIHL, Rule 14
[43] Art 57(2)(b) AP I

in relation to the military advantage anticipated.[44] To be sure, the exercise of weighing the expected harm to civilians or civilian objects against anticipated military advantage is always problematic, but in the case of cyber warfare the problems are exacerbated by the difficulty to assess with any accuracy what scope of incidental damage can be expected. This is so because cyber warfare is a new domain of warfare and so little is known about the impact of cyber operations, and because the interconnected nature of cyberspace makes it particularly difficult to foresee all of the possible effects of such operations. Again, the weight a cyber-attack may have on the civilian population may vary depending on certain circumstances. Therefore, a legally planned cyber-attack by belligerent may be prohibited because of the uncertainty of its impact.

For example, in 2021 The Colonial Pipeline ransom ware attack greatly affected civilian infrastructure and highlighted the vulnerability and interconnectedness of critical infrastructure to cyber threats. Dark Side, a ransom ware group, targeted the largest fuel pipeline in the United States, causing fuel shortages and widespread disruption along the East Coast and as such it cannot be said that such attack is in line with the principle of proportionality.[45]

3.3 Cyber Operation and the Principle of Precaution

IHL requires belligerents to take precautions in attack, as well as precautions against the effects of attack. The principle is provided for in Article 57 AP I. Precautions in attack are mandated by a general rule, applicable to all military operations, 'whereby constant care must be taken to spare the civilian population and civilian objects.'[46]IHL require belligerents who plan or decide upon an attack to do everything feasible to verify that targets are military objectives and not civilian objectives[47] and to take all feasible precautions in the choice of means and methods of warfare with a view to avoiding and in any event minimizing incidental harm to civilians.[48] Belligerents are further required to cancel or suspend an attack if it becomes apparent that it will entail a breach of the principle of proportionality.[49]

---

[44] D. Eitan 'Applying International Humanitarian Law to Cyber Warfare', *Law and National Security: Selected Issues, containing: Applying International Humanitarian Law to Cyber Warfare.* https://www.academia.edu/8214779/Law_and_National_Security_Selected_Issues_Containing_Applying_International_Humanitarian_Law_to_Cyber_Warfare [Accessed 4th January, 2025].

[45] Security Scorecard, " "The Wannacry ransomware attack"inhttps://securityscorecard.com/blog/top-cyberattacks-on-us-government/. [Accessed 4th January, 2025].

[46] Art 57(1) AP I

[47] Art 57(2)(a)(I) AP I

[48] Art 57(2)(a)(ii) AP I

[49] Art 57(2)(b) AP I

In application to cyber warfare a party planning to implement a cyber-attack is mandated to do everything feasible to gain the information necessary to verify that the projected target is a military objective and to ascertain the attack to cause excessive harm. Belligerents would also need to take all necessary precautions to ensure that critical civilian infrastructure will be protected as much as possible from the effects of cyber-attacks For instance, by ensuring that necessary data is safely stored and effectively backed up and by providing for timely repair of civilian systems that come to harm.[50]

3.4 Cyber Operation and Principle of Necessity and Humanity

Military Necessity means a military advantage that must be achieved by a party to an armed conflict. IHL does not frown at the intention of states or belligerent parties to win a war. However, in any operations or activities that will be carried out in line with military necessity, there must be a balance against humanitarian consideration. The principle of military necessity requires that a party to an armed conflict may only resort to those means and methods that are necessary to achieve the legitimate purpose of a conflict, i.e., 'to weaken the military forces of the enemy'.[51] This provision applies to all domains of warfare including the cyberspace. It does not, however, permit belligerents to take measures that would otherwise be prohibited under IHL,[52] and a rule of IHL cannot be derogated from by invoking military necessity unless this possibility is expressly provided for by the rule in question.[53] For example, cyber operations that do not constitute attacks under IHL but that would nonetheless seize or destroy enemy property such as freezing access to data stored in the cyber infrastructure controlled by the other party to the conflict may be justified on the grounds that such seizure or destruction would be 'imperatively demanded by the necessities of war'.[54] By contrast, IHL mandates that medical facilities be respected and protected at all times[55], which precludes the reliance on military necessity to justify a cyber-operation against a hospital during an armed conflict.

The principle of humanity imposes certain limits on the means and methods of warfare, and requires that those who have fallen into enemy hands be treated humanely at all times.[56] It seeks to limit unnecessary suffering, superfluous injury, and destruction during armed conflict; its purpose is to protect life and health and to ensure respect for the human being. This principle

[50] *Ibid*
[51] St. Petersburg Declaration (1868), preamble
[52] United States, Military Tribunal at Nuremberg, *Hostages case*, Judgment, 1948, pp. 66–67
[53] ICRC AP Commentary, para. 1389.
[54]Article 23(g) Hague Regulations (1907).
[55] Article 18 AP I.
[56] N. Melzer, "International Humanitarian Law: A Comprehensive Introduction", *ICRC*, 2022, p. 19.

precludes the assumption that anything that is not explicitly prohibited by specific IHL rules is therefore permitted[57]. For instance, using disinformation to mislead the enemy is not as such prohibited, as long as it does not infringe any specific rule of IHL and is not perfidious[58]. Conversely, spreading false information designed to cause panic among the civilian population in times of armed conflict would conflict with the principle of humanity. This is because such actions, even if not covered by a particular rule of IHL[59], would be reasonably expected to lead to significant harm to civilians, which would be contrary to the demands of humanity. Therefore, parties in cyber warfare must ensure that when carrying out an attack in the cyber space, the principle of humanity must be duly observed while their military necessity is in view.

4.0 Impact of Cyber Operations

Cyber operations, when used as means or methods of warfare in armed conflicts, pose significant risks to civilians and civilian infrastructure, potentially causing both direct and indirect harm. Unlike traditional kinetic warfare, cyber operations can cross borders silently, disrupt essential services remotely, and have both immediate and long-term consequences. These operations, whether targeted deliberately or misdirected unintentionally, can severely disrupt societal functions, incapacitate public institutions, and harm civilians directly and indirectly.

4.1 Impact of Cyber Operations on Civilian and Civilian Infrastructure

It is thus essential to appraise the impact of cyber operation on civilians and to understand how international humanitarian law protects civilians, civilian infrastructure, and civilian data against cyber harm. The international community recognizes that just as any other means and methods of warfare, cyber operations may seriously affect civilian infrastructure and thus result in devastating humanitarian consequences. There is a real risk that cyber tools may either deliberately or by mistake cause large-scale and diverse effects on critical civilian infrastructures, such as essential industries, telecommunications, transport, governmental, and financial systems. This is due to the interconnectivity of cyber space and such cyber tools will have diverse effects on civilian and civilian objects.[60]

[57] ICRC AP Commentary, para. 55.
[58] Article 38 (2) Additional Protocol I.
[59] Article 33 Fourth Geneva Convention (1949); Article 51(2) AP I.
[60] ICRC, "Cyber operations during armed conflict" in https://www.icrc.org/en/document/cyber-warfare. [Accessed 10th February, 2025].

The impact a cyber-attack has towards the civilian population while carrying out cyber operations can be very severe in the sense that it can lead to injury, damage and even death in the civilian population.

Cyber operation has a high rate of affecting critical civilian infrastructure in this sense refers to systems that are vital and indispensable to the functioning of the society and its economy. Such civilian infrastructure includes infrastructures for the health care sector, electricity, water, sanitation, transportation systems, communication systems, financial systems. These systems are so important that their failure could cause significant harm to public safety, national security, economic stability and the environment. It was noted that the more digital dependencies were ingrained in the health care system, the more difficult it might become to operate when and if these dependencies stop functioning. Depending on the type and number of facilities affected and the severity of future cyber-attacks, it could be made impossible to treat patients.[61] Examples of cyber-attacks that affected the health care sector[62] include the WannaCry ransomware in 2017, the 2016 ransomware campaign against a hospital in Hollywood (which seriously impeded patient care for several days), and the 2016–17 attack in Singapore. The investigation into the Singapore attack revealed that the infection lasted for more than ten months, and that the data of some 1.5 million users (including 16,000 medical prescriptions) were exhilarated. The impact of the attacks is that it prevented the medical facilities from operating normally by hampering system and data availability.[63]

Other notable examples of where critical infrastructure that have been impacted by cyber-attacks includes Not Petya which affected the financial systems such as banks, ATMs and point of sales across Ukraine. The civilians were unable to carry out financial transactions. The Ukraine power grid attack which affected the electricity supply of the civilians. Also, where the US and Israel launched the Stuxnet virus, it had devastating impacts on the Iranian nuclear program. What this seeks to prove is that in an event where cyber-attacks are being launched at critical civilian infrastructure, it can lead to devastating consequences which affect the general civilian population.[64]

[61] L. Gisel and L. Olejnik (eds), ICRC Expert Meeting: The Potential Human Cost of Cyber Operations, ICRC, Geneva, 2019.
[62] *Ibid.*
[63] *Ibid*
[64] *Ibid.*

4.2 Impact of Cyber Warfare on Combatants

Firstly, to what extent do cyber operations directly affect combatants, given their distinct nature when compared to traditional methods of warfare? Unlike conventional military operations—which are typically confined to clearly defined temporal and geographic boundaries and executed using tangible weapons such as rifles, bombs, aircraft, tanks, and naval vessels—cyber operations are often trans boundary, continuous, and intangible. Their effects may be delayed, dispersed, or even indirect, raising questions about their immediate impact on combatants as opposed to civilian populations and infrastructure. This evolution, referred to as cyber warfare, is a game-changer. It changes how we assess our enemies.[65] Hence the nature of Cyber warfare is distinct from the traditional concepts of warfare in the sense that it does not occur in the traditional domain and it does not utilize the traditional weapons of warfare.

Therefore cyber warfare does not affect combatant in the battlefield in the normal sense of warfare, however due the nature of cyber operation it has disastrous effect on the adversary forces, cyber operation is a multidimensional virtual space which parallel the physical world created by the growing network of computing and communication technologies, thus cyber-attack that affect the cyber spectrum will also affect the state of the physical world.[66] A cyber-attack includes any unauthorized cyber act aimed at violating the security policy of a cyber-asset and causing damage, disruption or destruction of the services or access to the information of the said national cyber asset. It is the intentional use of a cyber-weapon against an information system in a manner that causes a cyber-incident.[67]

The use of cyberspace by actors to carry out attacks brings about some challenges. Firstly, the cyber space is characterized by a dual-use character. This implies that the tools which are essential to the proper functioning of modern society and tools that are used by the civilians can also be used by the military forces. As a result, it is often difficult for one to distinguish between the civilian population and the military population in cyberspace.[68]

Secondly, cyber operation can be carried out by actors from any location on the world. With the complex nature of cyberspace, these actors can be anonymous. They can use techniques

[65] Marie O'Neill Sciarrone," Cyber Warfare: The New Front," in https://www.bushcenter.org/catalyst/modern-military/sciarrone-cyber-warfare. [Accessed 10th February, 2024].
[66] *Ibid.*
[67] Yuchong L., Qinghui L., "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments" https://www.sciencedirect.com/science/article/pii/S2352484721007289. [Accessed 14th June 2024]
[68] M. Piatkwoski, "The Definition of the Armed Conflict in the Conditions of Cyber Warfare". Polish Political Science Yearbook (2017) Vol. 46, No. 1, pp. 271-280.

such as routing attacks through multiple compromised systems or using stolen credentials to make it difficult to identify the source of the attack.

Thus, when anonymity is used by actors on the cyberspace, it makes attribution very difficult. Hence it becomes difficult for belligerent states involved in such an attack to attribute blame to a particular state actor due to the interconnectivity of the cyber spectrum.[69]

5.0 Recommendations for Safeguarding Civilians and Civilian Infrastructure in Cyber Warfare

1. Develop and Implement Cyber-Specific Rules of Engagement Consistent with IHL

States should formulate clear rules of engagement for cyber operations that explicitly integrate IHL principles, ensuring that military cyber operators are trained to apply distinction, proportionality, and precaution in their planning and execution of cyber missions. This includes technical safeguards to isolate military targets and prevent the spread of malware to civilian systems.[70]

2. Strengthen Legal Review Mechanisms for Cyber Weapons

In accordance with Article 36 of Additional Protocol I, states should establish or strengthen weapons review processes to assess the legality of cyber capabilities before their deployment. This legal review should consider the potential for indirect or cascading harm to civilians, particularly where dual-use infrastructure is likely to be affected.[71]

3. Harden and Isolate Critical Civilian Infrastructure

Governments must take proactive technical steps to enhance the cyber resilience of essential civilian infrastructure, particularly in the healthcare, water, energy, and financial sectors. This includes: segmentation of civilian and military networks; deployment of redundant systems and offline backups; implementation of end-to-end encryption, firewalls, and intrusion detection systems.[72] Such efforts not only reduce vulnerability but also help to ensure continuity of essential services during cyber conflict.

---

[69] *Ibid.*
[70] Y. Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict*, (3rd edn, Cambridge University Press, 2016), p. 110.
[71] ICRC, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare*, (ICRC, 2006), p. 7.
[72] M. Schmitt, (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, (Cambridge University Press, 2017), pp. 245–247.

4. Promote International Norms and Confidence-Building Measures

States should actively participate in international fora such as the UN Open-Ended Working Group (OEWG) and the GGE to develop non-binding norms that reinforce the protection of civilians in cyberspace. Confidence-building measures may include: advance notification of potentially harmful cyber operations; voluntary commitments not to target civilian infrastructure; information-sharing and cooperation on cyber incident response.[73]

5. Recognise Civilian Data as Civilian Objects

Given the growing strategic and humanitarian value of civilian data, such as health records and financial information, states should begin to interpret IHL protections to extend to digital civilian objects. This includes refraining from the deletion, manipulation, or exfiltration of sensitive civilian data during cyber operations, which could result in irreversible harm to affected populations.[74]

6. Enhance Public-Private Cooperation

As much of the world's digital infrastructure is owned or operated by private entities, states must engage with private sector actors to establish cyber security protocols that align with IHL obligations. This involves: joint contingency planning; sharing real-time threat intelligence; clarifying the roles and responsibilities of private companies during armed conflict.[75]

7. Educate and Train Military and Civilian Actors on Cyber IHL

To ensure IHL compliance in cyberspace, there must be widespread training for both military personnel and civilian stakeholders, including policy makers, legal advisors, and IT specialists. Training should focus on: understanding the legal status of civilian objects and data; identifying cyber operations that could constitute war crimes; applying ihl principles in networked environments.[76]

6.0 Conclusion

The evolving nature of armed conflict, particularly with the integration of cyber operations, has significantly heightened the risks faced by civilians and civilian infrastructure. Unlike

[73] United Nations, Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135, 2021, paras. 34–39.
[74] M. Taddeo, and L. Floridi, "The Ethics of Cyber Conflicts," *Philosophy & Technology* (2014), vol. 27, pp. 1–14.
[75] ICRC, *The Human Cost of Cyber Operations: Key Issues and Findings*, (ICRC, Geneva, 2021), p. 9.
[76] N. Melzer, *International Humanitarian Law and Cyber Operations*,(ICRC, Geneva, 2021), p. 21.

traditional warfare, cyber operations transcend physical boundaries and can indiscriminately affect interconnected systems that societies depend upon for survival, healthcare, electricity, finance, communication, and water supply. These operations may be executed remotely, silently, and in milliseconds, but their consequences are often devastating, widespread, and enduring. It is precisely because of this complex and unpredictable nature of cyber warfare that the protection of civilians and civilian objects must not only be preserved but actively reinforced. Their vulnerability in the digital battle space is not theoretical; it is real, as evidenced by numerous cyber-attacks that have disabled hospitals, disrupted power grids, and endangered lives. Therefore, IHL's core humanitarian purpose to shield those not participating in hostilities from the ravages of war must be rigorously upheld and adapted to ensure that the digital front does not become a legal and ethical vacuum.

While the Geneva Conventions and their Additional Protocols do not specifically mention cyber operations, the fundamental principles of distinction, proportionality, and precaution remain fully applicable and binding. These principles must now be interpreted in the light of the peculiarities of cyberspace, its borderlessness, dual-use infrastructure, and potential for mass disruption. As such, there must be a deliberate effort to ensure that cyber means and methods of warfare are developed, reviewed, and deployed in compliance with existing legal obligations under Article 36 of Additional Protocol I, and in accordance with evolving interpretations of international humanitarian norms.

Moreover, the increasing dependence of civilian populations on digital infrastructure calls for a re-examination of what constitutes civilian objects in armed conflict. Civilian data, digital health records, and networked systems have become lifelines in modern society and should be explicitly recognised as objects entitled to protection under IHL. As the Tallinn Manual 2.0 suggests, the legal framework must continue to evolve to address the intangibility and complexity of digital warfare, while maintaining the humanitarian imperative at its core.

States must also adopt proactive policy and technical measures to mitigate civilian harm. These include isolating civilian infrastructure from military networks, investing in cyber-resilience for essential services, conducting legal reviews of cyber weapons, and fostering cooperation between governments and private sector entities that manage critical infrastructure. In addition, international cooperation must be strengthened through multilateral dialogue, confidence-building measures, and the progressive development of binding cyber norms that explicitly protect civilians in armed conflict.

Ultimately, the protection of civilians and civilian infrastructure in cyberspace is not merely a legal obligation; it is a moral and humanitarian imperative. Failure to adapt IHL to the realities of cyber warfare risks rendering its protective guarantees ineffective in modern conflict. The laws of war must therefore be both preserved and reinterpreted to ensure that, even in the digital realm, the dignity, safety, and rights of non-combatants remain inviolable.