

Warfare in the Digital Age: Adapting the Laws of Armed Conflict to Cyber Operations

Kalyani Jayasekera *

General Sir John Kotelawala Defence University - Sri Lanka



0009-0005-7905-1576

Submission date: 23-10-2025

Acceptance date: 28-11-2025

Publication date: 01-03-2026

Abstract:

The rapid evolution of cyber technologies has transformed the nature of armed conflict, giving rise to cyber warfare as a prominent tool in modern military and strategic operations. This shift presents unique challenges for the application of International Humanitarian Law (IHL), a legal framework historically developed to govern conventional warfare. This article examines the intersection of IHL and cyber warfare, focusing on the difficulties of applying traditional principles such as distinction, proportionality, and precaution to the digital domain. By analyzing sources ranging from the Geneva Conventions and their Additional Protocols to the Tallinn Manual, as well as state practices and scholarly perspectives, the study highlights the complex legal and ethical questions posed by cyber operations. Particular attention is given to issues of attribution, civilian protection, and the evolving definition of “armed conflict” in cyberspace. The research argues that while IHL remains relevant, its implementation requires reinterpretation and adaptation to address the unique characteristics of cyber operations. Furthermore, the article underscores the urgent need for international dialogue, cooperative frameworks, and proactive state measures to codify and harmonize the application of IHL in cyberspace. The ultimate objective is to ensure that even in digital arenas, the humanitarian principles underpinning IHL continue to mitigate harm and uphold the protection of civilians.

Keywords: *Cyber Warfare; Civilian Protection; Attribution; Armed Conflict.*

Introduction:

In an era defined by rapid technological development and deep interconnectivity, cyber warfare has moved from the realm of theoretical possibility to a central concern of state security, humanitarian protection, and international law. While international humanitarian law (IHL) was

* Corresponding Author kalyajayasekera@gmail.com

drafted for kinetic conflict fighting with bullets, bombs, and tanks, the rising prominence of cyber operations in armed conflicts presents profound challenges. Existing rules must be stretched, reinterpreted, or potentially reformulated to deal with distinctive features of cyber warfare: its invisibility, its capacity for massive collateral effects, its capacity for anonymity, and its capacity to affect civilian infrastructure remote from the point of attack.

This article examines how IHL applies to cyber warfare, identifies the legal, ethical, and practical difficulties in that application, evaluates existing efforts to clarify or codify rules, and proposes ways forward. Key questions addressed include: when do cyber operations give rise to IHL (i.e. when is there an armed conflict, what counts as an attack), how do traditional principles like distinction, proportionality, and precautions work in cyber contexts, what are obligations regarding non-state actors, and how states are (or should be) contributing to regularizing norms.

IHL Framework and Cyber Warfare: Foundations

International humanitarian law is the body of law that regulates conduct during armed conflict. Its primary purpose is to alleviate human suffering, protect those who are not or no longer taking part in hostilities (such as civilians, wounded, medical personnel), and limit the means and methods by which warfare is conducted. Core treaties include the four Geneva Conventions of 1949 and their Additional Protocols (1977), while customary international law binds states whether they are party to specific treaties or not. IHL is grounded in principles such as *distinction* (between combatants/military objectives and civilians/civilian objects), *proportionality* (no excessive harm to civilians relative to the anticipated military advantage), *precautions* (measures to avoid or minimize civilian harm), *military necessity*, *humanity*, and *state responsibility*.

The emergence of cyber warfare has fundamentally altered the landscape of armed conflict, challenging traditional notions of battlefields, targets, and military engagement. Unlike conventional warfare, where hostilities are often visible and geographically bounded, cyber operations occur in a virtual space that transcends national borders and connects billions of systems worldwide. This digital domain allows actors to disrupt critical infrastructure, manipulate data, and disable communication networks, often without immediate physical destruction.

Consequently, the principles of International Humanitarian Law (IHL) designed to limit the effects of warfare on civilians and combatants—face unprecedented tests in their application. The foundational rules of distinction, proportionality, and precaution, enshrined in treaties such as the Geneva Conventions and their Additional Protocols, must now contend with challenges such as distinguishing between civilian and military cyber assets, assessing harm in terms of data or functional disruption, and attributing cyber attacks to specific actors. The inherently intangible and interconnected nature of cyberspace complicates these legal principles, raising questions about how IHL can effectively govern operations that blur the line between civilian and military spheres.

Despite these challenges, IHL continues to offer a vital framework for regulating cyber warfare and mitigating humanitarian harm. The International Committee of the Red Cross (ICRC) and the Tallinn Manual on the International Law Applicable to Cyber Warfare have both underscored the relevance of IHL in the digital age, highlighting the necessity of adapting its rules rather than abandoning them. State responsibility remains a cornerstone of compliance, requiring governments to ensure that both state actors and affiliated non-state actors adhere to legal obligations, even in cyberspace. Moreover, the law must navigate the ethical and operational complexities of cyber operations, including the attribution of attacks, the protection of civilian infrastructure, and the prevention of excessive or indiscriminate damage. As cyber operations increasingly shape the conduct of modern conflicts, it becomes imperative for states, scholars, and international organizations to engage in proactive dialogue, establish codified guidelines, and interpret existing IHL norms in ways that address the unique characteristics of digital warfare. In doing so, the humanitarian principles underpinning IHL—primarily the protection of human life and dignity—can continue to guide conduct in the invisible yet consequential arenas of cyber conflict.

Applicability of IHL to Cyber Warfare

International Humanitarian Law (IHL) becomes applicable primarily in two circumstances: during international armed conflicts (IACs) and non-international armed conflicts (NIACs). When it comes to cyber operations, the consensus among states and scholars is that IHL applies only when such operations occur in the context of an armed

conflict. However, defining what constitutes an armed conflict in the cyber realm is far from straightforward. No international treaty explicitly categorizes cyber operations as an armed attack or defines the threshold for armed conflict in cyberspace. As a result, states must rely on customary international law and expert interpretations, most notably the Tallinn Manual(s). Experts generally agree that cyber operations may qualify as an armed attack if they cause death, physical destruction, or severe disruption akin to that caused by conventional kinetic attacks. Minor cyber intrusions that temporarily disrupt networks or systems may fall below this threshold, whereas large-scale operations targeting critical infrastructure or causing widespread damage are likely to be considered armed attacks. This delineation is crucial because it establishes the conditions under which IHL rules begin to govern conduct in cyberspace.

A related and equally complex issue concerns the distinction between the “use of force” and an “armed attack” under the UN Charter, which recognizes the inherent right of states to self-defence only in response to an armed attack. In cyberspace, this distinction is nuanced: smaller cyber incidents may constitute a use of force without triggering the legal consequences of an armed attack, while destructive or large-scale cyber operations would meet the threshold for an armed attack, thereby activating both IHL obligations and the right to self-defence. Another central challenge in applying IHL to cyber operations is attribution. For IHL obligations to bind an actor, it must be possible to reliably attribute the cyber operation to a state or a controlling entity. The technical nature of cyberspace—with its ability to obscure origins, use proxies, and involve multiple actors—complicates attribution, creating both legal and practical uncertainties. Without clear attribution, states may struggle to hold perpetrators accountable, classify operations as acts of a state, or determine the applicability of IHL. Consequently, while cyber operations fall under the scope of IHL in principle, these challenges underscore the difficulties of enforcing international humanitarian norms in the digital age.

What Counts as “Attack” under IHL in Cyber Contexts

Under International Humanitarian Law, the term “attack” traditionally refers to acts of violence directed against an adversary, whether during offensive or defensive operations, as codified in Article 49 of Additional Protocol I to the Geneva Conventions. In the context of

cyber warfare, however, defining what constitutes an “attack” presents unique challenges due to the intangible nature of digital operations. The Tallinn Manual on the International Law Applicable to Cyber Operations and its expert commentaries extend the notion of attack to cyber operations that are reasonably expected to cause death or injury to persons, or destruction or damage to objects. A particularly important debate concerns whether mere loss of functionality, without accompanying physical destruction, qualifies as “damage” or “destruction” under IHL. The Manual’s experts generally agree that significant impairment of functionality—such as disabling a civilian network, critical infrastructure, or medical information systems—can indeed meet the threshold of damage, as it may have direct or indirect effects on civilian safety and military operations. This interpretation reflects a broader understanding that the legal protections of IHL are designed to address both tangible and intangible harms that jeopardize human life or essential objects, ensuring that cyber operations are evaluated through the same humanitarian lens as traditional kinetic attacks.

Core IHL Principles in Cyber Warfare

Once IHL is applicable, the traditional principles must be interpreted and applied in light of cyber capabilities. Below are some of the main challenges and how they are being addressed or debated.

The principle of distinction requires that parties to a conflict distinguish at all times between combatants and non-combatants, and between military objectives and civilian objects. In cyber warfare, distinction is complicated by the abstract nature of many targets (software, networks, data) and by interconnected systems.

Civilian infrastructure that is essential for survival (drinking water, electricity, hospitals) may be partially or wholly networked in systems that also support military operations or data. For example, a power grid may also serve military command or control. Determining whether such systems are dual use, when civilian objects can be considered military objectives, and whether damage to civilian networks is permissible when they serve military functions are all contested issues¹.

¹ [International Review of the Red Cross+2ISPI+2](#)

Proportionality, under IHL, prohibits attacks in which incidental harm to civilians or civilian objects would be excessive in relation to the expected military advantage. Cyber operations introduce special difficulties in assessing the scale of expected harm vs. advantage.

Because harm may be non-physical, delayed, or spread geographically, estimating what is “excessive” is more complex. For instance, a cyber operation intended to disable enemy communications might also affect civilian hospitals, emergency systems, or public services far from the primary target. The ripple effects may not be immediately known. Therefore, decision-makers must design operations with due care and ensure that intelligence about likely effects is as accurate as possible¹.

IHL requires that parties take all feasible precautions in attack to avoid or minimize civilian harm. Cyber operations require precautions, too, but what counts as feasible in cyberspace is a matter of ongoing discussion.

Possible precautions include verifying targets, choosing tools that minimize collateral spread, avoiding tools with unpredictable behavior, ensuring reversible impact where possible, applying “scorched network” avoidance (i.e. making sure disruption is limited to what is intended), and confirming whether civilian systems may be affected. Use of “kill switches,” limiting self-propagation, and other technical safeguards are relevant².

International Humanitarian Law offers special protection to objects and services indispensable to civilian survival, including food, water, medical facilities, and humanitarian operations. Under Article 54 of Additional Protocol I to the Geneva Conventions, starvation of civilians as a method of warfare is prohibited, and Article 14 of Additional Protocol II extends protections to essential civilian objects in non-international armed conflicts. In the context of cyber warfare, these protections acquire new complexity, as attacks may target not only physical infrastructure but also the digital systems that enable their functioning. For instance, cyber operations that disrupt hospital information systems, manipulate medical data, or interfere with the logistics of humanitarian aid can have severe consequences for civilian survival, even if no physical destruction occurs.

¹ [International Review of the Red Cross+1](#)

² [International Review of the Red Cross+1](#)

The International Review of the Red Cross has emphasized that IHL principles, including distinction and proportionality, apply equally to cyber operations that threaten civilian objects, and the targeting of such systems is permissible only if they qualify as military objectives and the attack complies with all other IHL obligations. Scholarly analyses, such as those in ISPI reports, further highlight that the digital dimension of civilian services require states and parties to conflict to carefully assess the potential humanitarian impact before conducting cyber operations, ensuring that civilian harm is minimized and humanitarian access is preserved. This underscores the continuing relevance of IHL in adapting to the evolving cyber domain while maintaining protection for civilian life and essential services.

Legal and Doctrinal Efforts to Clarify Application

Over recent years, scholars, states, and international organizations have taken up efforts to clarify how IHL should be interpreted for cyber warfare. Some of these efforts are binding (treaty/customary law), others are non-binding but influential (manuals, state declarations).

Perhaps the most comprehensive attempt is the *Tallinn Manual* (first edition, 2013) and its successor, *Tallinn Manual 2.0* (2017). These works represent the views of expert groups about how existing international law (including IHL, UN Charter, sovereignty, state responsibility) applies to cyber operations. Tallinn Manual 2.0 contains 154 “black letter rules,” many of which relate to responsibilities in peace and conflict, conduct of hostilities, attribution, and the threshold of attack. While non-binding, these manuals are widely cited and have helped shape state practice and expert debate¹.

Many states, through national war manuals, diplomatic statements, and practice have acknowledged that IHL applies to cyber operations that amount to attacks or hostilities. For example, the United States War Manual recognizes that when cyber operations rise to attacks, the law of war rules on conduct must apply, including principles such as distinction and proportionality². Several states in international forums (e.g. AALCO,

¹ [ISPI+3Atlantic Council+3icdt.osu.edu+3](https://ispi+3atlantic.council+3icdt.osu.edu+3)

² <https://aauihl-clinic.org/>

UN fora) have voiced concern about critical civilian infrastructure and have called for norms of behavior in cyber space consistent with IHL¹.

ICRC reports have similarly reaffirmed that IHL does apply to cyber operations during armed conflict, and that states need to interpret IHL in light of new means and methods and take active measures to ensure civilian protection in cyber warfare².

While existing frameworks and efforts are valuable, significant gaps and challenges remain. These are legal, technical, doctrinal, and political.

Ambiguity in “Attack” and Thresholds of Armed Conflict

A central challenge in applying IHL to cyber operations lies in the ambiguity surrounding what constitutes an “attack” and when a cyber operation crosses the threshold into an armed conflict. Traditional IHL frameworks, including Articles 2 and 49 of the 1949 Geneva Conventions and Article 51 of Additional Protocol I, were drafted with kinetic operations in mind, defining armed conflict and attacks primarily in terms of physical violence and destruction. In the cyber domain, however, operations may cause severe disruption to critical infrastructure, such as hospital systems, financial networks, or power grids, without inflicting direct physical damage or loss of life. These scenarios create legal uncertainty, as state practice varies regarding the threshold at which a cyber operation triggers IHL obligations. The Tallinn Manual on the International Law Applicable to Cyber Operations attempts to address this gap by defining a “cyber attack” as any cyber operation reasonably expected to cause injury, death, or damage comparable to kinetic effects. Nonetheless, there is no universally accepted treaty definition, and states remain constrained to interpret customary law and expert guidance when determining whether a cyber operation constitutes an armed attack. This lack of clarity complicates decision-making for military commanders, challenges the consistent application of proportionality and distinction principles, and raises broader questions about the applicability of IHL in highly digitalized conflict environments.

¹ <https://www.aalco.int/>

² [ICRC+2International Review of the Red Cross+2](#)

Attribution Difficulties

Attribution in cyber operations presents a formidable challenge to the application and enforcement of IHL. Many core obligations under IHL, including the principles of distinction, proportionality, and precautions, presuppose that the attacking actor can be identified and held accountable. Article 8 of the Draft Articles on Responsibility of States for Internationally Wrongful Acts, reflecting customary international law, provides that conduct of a person or group shall be considered an act of a state if the individual or group is acting on the instructions of, or under the control of, that state. However, cyber operations are frequently conducted through non-state actors, proxy groups, or anonymized networks, making reliable attribution extremely difficult. This creates both practical and legal uncertainty: without clear attribution, it is challenging to classify an operation as part of an armed conflict or to hold states responsible for violations. The problem is compounded by the potential for states to deny involvement or assert plausible deniability, effectively undermining accountability. The International Review of the Red Cross has noted that these attribution difficulties impede enforcement of IHL and complicate efforts to deter unlawful cyber operations, as the lack of identifiable responsibility may weaken the deterrent effect of legal prohibitions. Consequently, states are urged to develop robust mechanisms for assessing and demonstrating attribution, and to adopt measures ensuring that cyber operations comply with IHL obligations even when indirect actors are involved.

Dual-use Assets and Civilian vs Military Objects

The dual-use nature of many modern networked systems presents a significant challenge under IHL, particularly in distinguishing between civilian and military objects. Dual-use assets are those that serve both civilian and military functions, for example, power grids, communication networks, or transportation systems that support civilian life but also contribute to military operations. Under Article 52 of Additional Protocol I, attacks may only be directed at military objectives, defined as objects which by their nature, location, purpose, or use make an effective contribution to military action, and whose destruction offers a definite military advantage. Civilian objects, conversely, enjoy protection against attack, and any incidental harm to them must not be excessive in relation to the anticipated military advantage, in accordance with Article 51(5)(b)

on proportionality. Cyber operations against dual-use systems complicate this assessment, as the military relevance of a network may be intertwined with vital civilian functions, and damage may manifest indirectly or with temporal delay, affecting civilian populations in unforeseen ways. The obligation to take precautions, codified in Article 57 of Additional Protocol I, requires parties to the conflict to verify that targets are military objectives, choose means and methods of attack that minimize civilian harm, and adjust or cancel operations if anticipated civilian damage is excessive. In cyberspace, these requirements are particularly complex because the effects of an operation may propagate unpredictably, potentially disrupting civilian infrastructure while achieving a military objective, raising critical questions about proportionality and lawful targeting. The ICRC has emphasized that when dual-use objects are targeted, states must rigorously evaluate both the military necessity and potential civilian impact, ensuring that cyber operations remain consistent with the core principles of distinction, proportionality, and precaution.

Technological Unpredictability and Collateral Effects

Cyber operations pose unique challenges due to the technological unpredictability inherent in digital tools and networks. Malware or other offensive cyber capabilities may spread beyond their intended targets, potentially causing cascading disruptions to civilian infrastructure, essential services, or critical data systems. Such unpredictable effects complicate compliance with IHL obligations, particularly the principles of proportionality and precaution. Article 57 of Additional Protocol I requires that parties to a conflict take “all feasible precautions” to avoid or minimize incidental harm to civilians and civilian objects, including assessing the potential effects of an attack before it is launched. In the context of cyber operations, this obligation necessitates careful analysis of the likely second- and third-order consequences, even though reliable intelligence regarding the propagation or unintended effects of software or malware is often unavailable. Furthermore, Article 51(5)(b) prohibits attacks that may be expected to cause excessive civilian harm in relation to the anticipated military advantage, emphasizing that even non-kinetic operations must be evaluated for their potential to produce disproportionate effects. The unpredictable nature of cyber tools thus heightens the risk of violating these core IHL norms, as the intended military effect may be easily outweighed by unintended damage to

civilian systems or populations. The ICRC has repeatedly noted that the inherent uncertainty of cyber capabilities demands rigorous pre-attack assessments and continuous monitoring to ensure that operations remain within the legal boundaries established by IHL, reinforcing the need for careful operational planning and adherence to precautionary measures.

Non-State Actors and Civilian Participation

Non-international armed conflicts (NIACs), which involve hostilities between states and organized non-state armed groups or among such groups within a single state, introduce particular doctrinal challenges under IHL, especially in the context of cyber operations. One key complexity concerns civilians who directly participate in hostilities, such as hackers or organized groups engaging in offensive cyber operations. Under IHL, civilians are afforded protection from attack unless and for such time as they take a direct part in hostilities, as established in Article 51(3) of Additional Protocol I to the Geneva Conventions. However, the law provides limited guidance on what constitutes “direct participation” in cyberspace, leaving ambiguity regarding whether a civilian operating a computer network to disable enemy infrastructure temporarily loses immunity from attack. The ICRC has highlighted this challenge, emphasizing that while civilians involved in cyber operations may forfeit protection during their engagement, the threshold for direct participation must be strictly interpreted to avoid undermining the fundamental principle of distinction between combatants and civilians. Additionally, Article 13 of Additional Protocol II reinforces the protection of persons who are not taking part in hostilities in NIACs, and customary IHL principles extend similar safeguards, requiring that any targeting of civilians, including those engaged in cyber activities, must be proportionate and discriminate. The involvement of non-state actors in cyber operations further complicates attribution and accountability, as their actions may be loosely connected to a state or an organized armed group, raising questions about state responsibility under Article 8 of the Draft Articles on Responsibility of States for Internationally Wrongful Acts. Consequently, the participation of civilians in cyber operations challenges traditional IHL frameworks and underscores the need for doctrinal clarification and evolving legal interpretation in the digital age.

Lack of Binding Treaty or Uniform Customary Norms Specific to Cyber

While IHL treaties apply, none were drafted with cyber warfare in mind specifically. There is no treaty that explicitly addresses cyber-attacks or cyber warfare. Customary law is developing, but state practice is patchy and opinions diverge. Non-binding frameworks (like the Tallinn Manual) help but do not carry legal force.

Ethical Implications

Even beyond legal compliance, cyber warfare raises ethical questions. The potential for wide, sometimes hidden harm to civilians (e.g., through loss of healthcare services, water, power, or economic harm), raises serious concerns under ethical theories of war (just war, utilitarianism, deontological duty). Morally, states must ask not only what they *may* do under law, but what they *should* do to limit harm, ensure transparency, and uphold human dignity. Ethical norms may in some cases demand more than what minimal legal compliance requires.

International Humanitarian Law (IHL) applies to both international armed conflicts (IACs) and non-international armed conflicts (NIACs), as established by the Geneva Conventions of 1949 and their Additional Protocols of 1977. Specifically, Common Article 2 of the Geneva Conventions provides that the Conventions apply “to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties,” thus covering traditional interstate conflicts. For non-international armed conflicts, Common Article 3 and Additional Protocol II extend humanitarian protections to situations where hostilities occur between state forces and organized armed groups, or among such groups within a single state. In the context of cyber operations, the legal challenge is determining when such operations constitute an armed conflict. No treaty explicitly defines a cyber attack as an armed attack, and states must rely on customary international law and expert interpretations, such as those presented in the Tallinn Manual on the International Law Applicable to Cyber Warfare. The Manual, although non-binding, interprets that a cyber operation may amount to an armed attack if it causes death, serious physical damage, or disruption equivalent to that produced by

conventional military force, thus triggering the applicability of IHL principles.

The distinction between the “use of force” and an “armed attack” under Article 2(4) and Article 51 of the UN Charter is particularly relevant in cyberspace. Article 2(4) prohibits the threat or use of force against the territorial integrity or political independence of any state, while Article 51 recognizes a state’s inherent right to self-defence if an armed attack occurs. Minor cyber intrusions, such as temporary disruptions of civilian networks, may constitute a use of force but not an armed attack, whereas large-scale operations that disable critical infrastructure or cause significant civilian harm are likely to meet the threshold of an armed attack, thereby activating both IHL obligations and the right of self-defence. Furthermore, IHL imposes obligations on parties to a conflict to distinguish between civilian and military objects (Article 48, Additional Protocol I) and to take precautions against incidental harm to civilians (Article 57, Additional Protocol I). In the cyber context, civilian data, networks, and infrastructure may be inadvertently affected by attacks targeting military objectives, making compliance with these principles particularly challenging. Additionally, attribution under customary international law, reflected in Article 8 of the Draft Articles on Responsibility of States for Internationally Wrongful Acts, is crucial: for IHL to bind the actor, the cyber operation must be attributable to a state or a controlling entity. The difficulty of attributing cyber operations, due to their ability to mask origins, employ proxies, or involve non-state actors, creates legal uncertainty, potentially undermining accountability and enforcement.

While many cyber operations remain covert and attribution is inherently difficult, several incidents and state practices illustrate both the challenges of applying IHL to cyber warfare and the gradual emergence of evolving norms. A notable example is the cyberattacks against Estonia in 2007, which targeted government websites, banks, and media outlets. Although these operations did not rise to the level of an armed conflict, the incident drew international attention to the vulnerability of critical national infrastructure in cyberspace. The aftermath of the attacks catalyzed discussions on responsible state behavior and contributed significantly to the development of the Tallinn Manual, which provides guidance on how existing international law, including IHL, can be applied to cyber operations during armed conflict.

The Estonia case underscores the difficulties of distinguishing between peacetime cyber incidents and operations that could trigger IHL protections, particularly when civilian systems are disrupted.

State practice has also demonstrated an acknowledgment of the applicability of IHL to cyber operations. The United States, for instance, has integrated IHL considerations into its cyber operations doctrine, as reflected in the U.S. Cyber Command doctrine and the U.S. War Manual. These publications recognize that certain offensive or defensive cyber operations, particularly those conducted during armed conflict, are subject to the principles of distinction, proportionality, and precautions under IHL. On the multilateral front, forums such as the Asian-African Legal Consultative Organization (AALCO) have provided platforms for states to deliberate on the protection of essential civilian infrastructure, including power grids, water systems, and healthcare services, emphasizing the need for consistent application of IHL in cyberspace. Complementing these efforts, the International Committee of the Red Cross (ICRC) has played a pivotal role by producing reports, engaging in expert dialogues, and conducting bilateral discussions with states to ensure that cyber operations in conflict adhere to IHL principles. These initiatives collectively illustrate that while cyber warfare presents unique legal and operational challenges, states and international organizations are gradually working toward establishing norms that uphold civilian protection and accountability in the digital domain.

Conclusion

Cyber warfare presents new, serious challenges to the framework of international humanitarian law, but also opportunities for legal, normative, and technical innovation. While many features of cyber operations anonymity, non-kinetic effects, interconnected civilian infrastructure strain traditional assumptions of IHL, existing law, as interpreted through expert manuals and state practice, already offers a foundation. The principles of distinction, proportionality, precautions, and protection of civilians continue to apply, even though their implementation may require adaptation.

For IHL to remain relevant and effective, states and other actors must act to clarify definitions, build consensus, share information, establish best practices, and ensure compliance. Ethical considerations must guide legal reform, seeking not only what is permissible, but what

is responsible. Unless the international community takes proactive steps, the legal protections IHL affords could be eroded by developments in cyber tools and operations that outpace existing norms.

Bibliography:

Books and Manuals

- Ohlin, Jens, Kevin Govern, Jeffrey Finkelstein, and Robert Bussolati. *Cyber Operations and State Responsibility in International Law*. Oxford: Oxford University Press, 2015.
- Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.
- Schmitt, Michael N. "Cyber Operations and the Law of Armed Conflict: The Tallinn Manual and Beyond." In *The Handbook of International Humanitarian Law*, edited by Dieter Fleck, 3rd ed. Oxford: Oxford University Press, 2013.

International Legal Instruments

- Additional Protocol I to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, 1977.
- Additional Protocol II to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, 1977.
- Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 1949.
- Geneva Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, 1949.
- Geneva Convention (III) Relative to the Treatment of Prisoners of War, 1949.
- Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War, 1949.
- United Nations. *Charter of the United Nations*. 26 June 1945. 1 UNTS XVI.

Reports and Articles

- Gisel, Laurent, and Tilman Rodenhauser. "Application of International Humanitarian Law to Cyber Operations." *International Review of the Red Cross* 101 (2019): 537.
- International Committee of the Red Cross. *Cyberwarfare and International Humanitarian Law: The ICRC's Position*. 2013. <https://www.icrc.org/en/document/cyberwarfare-and-international-humanitarian-law-icrcs-position>. Accessed 9 October 2025.
- International Committee of the Red Cross. *International Humanitarian Law and Cyber Operations during Armed Conflicts*. ICRC, 2019. <https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations>. Accessed 9 October 2025.
- ISPI. "Cybersecurity and International Law: Balancing Security and Humanitarian Protection." 2020. <https://www.ispionline.it/en/publication/cybersecurity-and-international-law>. Accessed 9 October 2025.

Websites and Online Sources

- Asian-African Legal Consultative Organization (AALCO). "Proceedings on Cybersecurity and IHL." <https://www.aalco.int/>. Accessed 9 October 2025.
- icdt.osu.edu. "Cyber Operations, Armed Conflicts, and International Law." <https://icdt.osu.edu/cyber-law>. Accessed 9 October 2025.