Cyber Warfare and International Humanitarian Law

LAW

ELAY DERİN ULAŞ

Introduction

The principles of International Humanitarian Law are fully applicable when cyber operations reach the threshold of an armed conflict, yet the nature of cyber warfare profoundly challenges these norms. The principle of Distinction is complicated by the dual-use nature of civilian and military cyber infrastructure, such as power grids and communication systems, making it difficult to isolate legitimate military targets without causing unintended civilian harm. The principle of Proportionality is stressed by the unpredictable, cascading effects of cyber operations, which can rapidly spread across interconnected systems, hindering the accurate assessment of collateral damage. Finally, the principle of military necessity requires that cyber operations be indispensable for achieving a lawful military objective, excluding actions taken solely for political coercion or economic advantage.

Overview of International Humanitarian Law (IHL)

International Humanitarian Law is a branch of public international law that regulates the conduct of hostilities and seeks to minimize the humanitarian consequences of war. It provides a legal framework that aims to balance military necessity with the protection of human dignity. International Humanitarian Law applies in situations of armed conflict, whether international or non-international in nature. The core legal foundations of International Humanitarian Law are found in the Geneva Conventions of 1949 and their Additional Protocols of 1977, which together form the basis of modern humanitarian law. The Hague Conventions also contribute significantly by addressing the means and methods of warfare. These instruments establish binding rules for states and parties to a conflict, ensuring the humane treatment of civilians, prisoners of war, and the wounded. International humanitarian law consists of four basic principles. First, the principle of distinction: parties to a conflict must distinguish between combatants and civilians. Attacks must only be directed against military objectives. Second, the principle of proportionality, which prohibits attacks that might cause excessive harm to civilians in relation to the expected military objectives. Third, the principle of necessity, meaning that the use of force is limited to what is necessary to achieve legitimate military objectives. And lastly, the principle of humanity: parties must avoid unnecessary suffering and protect those not taking part in hostilities. All of these principles form the ethical and legal foundation that governs conflicts. International humanitarian law applies only during armed conflicts, not during internal disturbances or peacetime tensions. It binds all parties to a conflict regardless of which side initiated hostilities. Its rules are universal and non-reciprocal, meaning that violations by one party do not justify violations by another. In the 21st century, the scope of international humanitarian law has expanded to address emerging challenges such as cyber warfare, autonomous weapons, and information operations. The digitalization of conflict raises complex legal and

ethical questions about how traditional international humanitarian law principles apply in cyberspace, particularly in distinguishing civilian from military infrastructure.

Definition and Nature of Cyber Warfare

In the modern era, technological advancement has transformed the character of warfare. Conflicts are no longer confined to physical battlefields; instead, they increasingly extend into the digital domain. This new dimension of conflict, commonly referred to as cyber warfare, represents one of the most significant challenges to traditional international law and global security. Cyber operations have the potential to disrupt national infrastructure, compromise military capabilities, and threaten civilian populations without the use of conventional weapons. The term cyber warfare does not have a single, universally accepted definition under international law. Generally, it refers to the use of digital attacks by one state to damage, disrupt, or gain unauthorized control over another state's computer systems, networks, or digital infrastructure for strategic or military purposes. According to the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, a cyber operation qualifies as an "act of warfare" when it causes effects comparable to those of a traditional armed attack, such as loss of life, physical destruction, or significant disruption of essential services. Therefore, cyber warfare encompasses a range of activities, from espionage and sabotage to full-scale attacks against military or civilian infrastructure. Cyber warfare differs from traditional forms of conflict in several key aspects. Firstly, cyberattacks are carried out through invisible digital networks, often making it extremely difficult to identify the perpetrator or the origin of the attack. Also, cyber operations can occur instantaneously and can affect vast networks across borders within seconds. At the same time, many cyber targets, such as communication systems or power grids, serve both civilian and military purposes, blurring the distinction between combatants and civilians. In addition, compared to conventional military operations, cyberattacks are relatively inexpensive yet capable of causing substantial economic, political, or strategic damage. And lastly, the interconnected nature of cyberspace means that a single attack can have transnational or even global repercussions. In the present, states increasingly recognize cyberspace as a critical domain of warfare alongside land, sea, air, and space. Cyber capabilities are now integral to national defence strategies, enabling offensive and defensive operations without direct physical confrontation. Major global actors, including the United States, Russia, China, and members of NATO, have established dedicated cyber commands responsible for safeguarding national interests in the digital realm. The strategic importance of cyber warfare lies not only in its potential for destruction, however, also in its capacity for deterrence, intelligence gathering, and psychological influence, making it a vital tool in modern hybrid warfare.

Applicability of IHL to Cyber Operations

The rapid expansion of digital technologies and the growing reliance on cyberspace have fundamentally transformed the landscape of modern conflict. As states increasingly engage in cyber operations that may produce serious consequences, a key question arises: Does International Humanitarian Law apply to cyber warfare? This question lies at the heart of current international legal debates. While traditional armed conflicts are governed by well-established legal norms, the digital nature of cyber warfare presents challenges in determining when and how international humanitarian law should apply. International Humanitarian Law applies to situations of armed conflict, whether international or non-international. The applicability of international humanitarian law to cyber operations is therefore contingent on whether such operations meet the threshold of an armed conflict as defined by international law. According to Article 2 common to the Geneva Conventions, international humanitarian law applies to all cases of declared war or any other armed conflict between states, even if the state of war is not formally recognized. Thus, if a cyber operation results in consequences comparable to kinetic warfare, such as loss of life, injury, or destruction of property, it may constitute an armed conflict, triggering the application of international humanitarian law. The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations affirms this interpretation, stating that international humanitarian law applies to cyber operations when their effects are equivalent to those caused by conventional weapons. One of the major challenges in applying international humanitarian law to cyber operations is determining when a cyber activity reaches the level of an "armed attack." Most scholars and legal experts agree that mere cyber espionage, propaganda, or economic disruption do not, by themselves, meet the threshold of armed conflict. However, cyber operations that cause physical destruction, casualties, or disable critical infrastructure such as power grids, hospitals, or air traffic control systems are generally considered acts of armed conflict under international humanitarian law. The principle of attribution also plays a vital role. For international humanitarian law to apply, the cyber operation must be attributable to a state or an organized armed group, as private cybercrime falls under domestic or international criminal law rather than humanitarian law. International organizations and states increasingly recognize the importance of clarifying international humanitarian law's role in cyberspace. The United Nations Group of Governmental Experts and the Open-Ended Working Group have both affirmed that existing international law, including international humanitarian law, applies to cyberspace. Furthermore, several states have issued national position papers confirming that international humanitarian law governs cyber operations conducted during armed conflict. However, differences remain in interpreting how and when those rules apply, especially regarding proportionality and civilian protection.

Key IHL Principles: Distinction, Proportionality, Necessity

The principle of distinction is one of the most essential and universally recognized norms of international humanitarian law, codified in Article 48 of Additional Protocol I to the Geneva Conventions. It requires parties to a conflict to distinguish at all times between combatants and civilians, as well as between military objectives and civilian objects. Attacks must be directed only against legitimate military targets; operations that deliberately target

civilians or civilian infrastructure are strictly prohibited. In the context of cyber warfare, applying the distinction principle becomes particularly complex. Many cyber networks and infrastructures, such as communication systems, power grids, and satellites, are dual-use in nature, serving both civilian and military purposes. Distinguishing between lawful and unlawful targets in such interconnected systems is therefore one of the most pressing challenges in contemporary conflict regulation. Failure to uphold this principle may result in indiscriminate attacks, which constitute a serious violation of international humanitarian law and may amount to war crimes under international criminal law. The principle of proportionality complements distinction by seeking to balance military necessity with humanitarian protection. It is enshrined in Article 51 of Additional Protocol I, which prohibits attacks expected to cause incidental loss of civilian life, injury to civilians, or damage to civilian objects that would be excessive in relation to the concrete and direct military advantage anticipated. In the cyber domain, proportionality assessments are especially challenging due to the unpredictable and widespread effects of cyber operations. For instance, a cyber attack intended to disable a military network might inadvertently disrupt civilian hospitals, transportation systems, or financial institutions connected to the same infrastructure. Because such operations can cascade through interconnected systems, accurately evaluating proportionality in cyberspace demands advanced technical understanding and real-time risk assessment. Thus, commanders and decision-makers must ensure that cyber operations are carefully planned and executed to avoid disproportionate harm to civilian populations and infrastructure. The principle of military necessity limits the use of force to what is indispensable for achieving a legitimate military objective. It permits only those measures that are required to weaken the military capacity of the adversary, provided they are not otherwise prohibited by international humanitarian law. This principle is closely linked to both distinction and proportionality, ensuring that violence is not excessive or arbitrary. In the context of cyber warfare, necessity implies that cyber operations must be directly related to achieving a lawful military aim, and that any collateral damage must be avoided whenever possible. Operations carried out for purposes of political coercion, economic advantage, or psychological intimidation that lack clear military necessity would therefore fall outside the lawful boundaries of international humanitarian law. The principle also underscores the obligation to seek less harmful alternatives before resorting to destructive cyber actions, reinforcing the humanitarian restraint that underpins the entire framework of international humanitarian law. Although distinction, proportionality, and necessity are distinct legal concepts, they function interdependently within the international humanitarian law framework. Together, they form a system of checks and balances: distinction identifies legitimate targets, proportionality restricts the scale of force, and necessity ensures that force is used only when justified by military objectives. In the realm of cyber operations, their combined application is vital to preserving the protection of civilians and maintaining legal accountability in an increasingly complex and borderless domain of warfare.

Legal and Ethical Challenges in Cyberspace

The evolution of digital technology has created a new and complex domain of conflict. While cyber operations offer states strategic and defensive advantages, they also raise profound legal and ethical challenges. The unique nature of cyberspace complicates the application of traditional international law and humanitarian principles. These challenges have generated significant debate among policymakers, military strategists, and legal scholars regarding how to regulate cyber warfare in a way that ensures accountability, legitimacy, and human protection. One of the most critical legal challenges in cyberspace is the issue of attribution, identifying the actor responsible for a cyber attack. Unlike conventional warfare, where the origin of an attack can often be traced to a specific territory or force, cyber operations can be easily disguised, rerouted, or conducted through third-party systems. This anonymity makes it difficult to determine state responsibility, a core concept under international law. According to the Articles on the Responsibility of States for Internationally Wrongful Acts, a state may only be held accountable for actions that are attributable to it. However, in cyber operations, attackers may use proxy networks, botnets, or non-state hackers, blurring the line between state and non-state involvement. This uncertainty undermines deterrence, complicates lawful retaliation, and increases the risk of escalation based on misattribution. A major question concerns when a cyber operation constitutes the "use of force" or an "armed attack" under the United Nations Charter and International Humanitarian Law. While international humanitarian law applies to situations of armed conflict, not every cyber incident reaches this threshold. Cyber espionage, data theft, or temporary disruptions may not qualify as armed attacks, yet large-scale cyber operations that cause loss of life, injury, or destruction of critical infrastructure may meet this standard. The difficulty lies in the lack of physical damage in many cyber attacks, which complicates the interpretation of what constitutes "force" in the digital environment. Consequently, the absence of clear legal thresholds leaves room for subjective state interpretations and inconsistent enforcement. Another pressing challenge relates to the protection of civilians and dual-use infrastructure. Modern societies depend on interconnected digital systems for healthcare, transportation, energy, communication, and finance. Many of these systems serve both civilian and military purposes, making it difficult to distinguish lawful targets from protected civilian assets. A cyber attack on a military communication system, for example, could inadvertently disrupt hospitals, emergency services, or water supply networks connected to the same infrastructure. Such unintended consequences directly challenge the international humanitarian law principle of distinction and raise moral concerns about the proportionality and foreseeability of harm to civilian life. The increasing role of non-state actors presents additional legal complications. These actors often operate beyond the control of any government, yet their actions can have transnational consequences. Existing legal frameworks are primarily state-centered, making it difficult to hold non-state cyber actors legally accountable under current international law. Furthermore, private technology companies now possess capabilities comparable to state cyber units, influencing the dynamics of warfare and blurring lines of responsibility. The absence of comprehensive international mechanisms to regulate or prosecute cyber offenses exacerbates the accountability gap in this

domain. Beyond legal questions, ethical dilemmas also arise in the conduct of cyber warfare. The ability to cause widespread harm remotely, without physical confrontation, can desensitize decision-makers to the human consequences of their actions. Cyber operations may disproportionately affect civilians, particularly vulnerable populations dependent on digital services. Additionally, the use of automated and autonomous cyber systems raises moral questions about delegating lethal or destructive decisions to machines. Ensuring human oversight, moral judgment, and ethical restraint in such systems remains a significant global concern. The absence of a comprehensive international treaty specifically governing cyber warfare underscores the urgent need for global cooperation. Existing frameworks provide interpretative guidance but lack binding authority. A unified international approach is necessary to establish norms of responsible behavior, define legal thresholds, and enhance transparency and accountability in cyberspace.

International Efforts and the Tallinn Manual

As cyber warfare continues to evolve, the international community has recognized the urgent need to clarify how existing international law applies to cyber operations. The absence of a specific treaty governing cyberspace has led to efforts by states, international organizations, and expert groups to develop interpretative frameworks and non-binding guidelines. Among these, the Tallinn Manual stands as the most comprehensive attempt to analyse and codify how international law regulates cyber activities. The Tallinn Manual originated from a project initiated by the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, following the 2007 cyber attacks on Estonia. These attacks, which targeted government websites, banks, and media institutions, highlighted the vulnerabilities of modern digital infrastructures and the absence of a clear legal framework to address such incidents. In response, a group of international legal experts and practitioners developed the Tallinn Manual on the International Law Applicable to Cyber Warfare and later expanded it into the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. The project's primary objective was to interpret how existing international law applies to state behavior in cyberspace. The Tallinn Manual 1.0 focused on the application of international law to cyber activities that occur during armed conflicts, addressing issues such as the definition of "armed attack," combatant status, and the protection of civilians. The later Tallinn Manual 2.0 broadened this scope to include cyber operations below the threshold of armed conflict, such as espionage, information operations, and state-led cyber intrusions. The manual is structured into rules and commentaries covering a wide range of legal domains, including sovereignty, use of force, state responsibility, and human rights law. While the manual is not a legally binding document, it provides authoritative guidance for states, policymakers, and military planners by interpreting existing norms in the cyber context.

Future Perspectives and Recommendations

The continuous evolution of technology and the growing dependence on digital infrastructure have made cyberspace an integral component of modern international relations and national defense. As cyber operations become more sophisticated and frequent, the question of how to regulate their use under international humanitarian law will lie not only in applying existing legal frameworks to cyberspace but also in adapting and strengthening them to address the unique characteristics of the digital domain. This section explores potential future directions, legal developments, and policy recommendations that can enhance global cybersecurity governance while ensuring that humanitarian principles remain central to all cyber operations. One of the most pressing needs is the development of binding international agreements that specifically address cyber warfare. While the Tallinn Manual, UN GGE, and OEWG provide interpretative guidance, they do not have the force of law. A future Cyber Warfare Convention, modeled on the Geneva Conventions, could codify specific obligations for states regarding the use of cyber means and methods of warfare. Such a convention would represent a critical evolution in international law, closing the current normative gap between traditional armed conflict and modern cyber operations. It could establish legally binding standards that delineate acceptable state behavior in cyberspace, providing greater predictability, accountability, and humanitarian protection. To be effective, a cyber warfare convention should define the thresholds for the use of force and armed attack in digital contexts, ensuring consistency with Article 2 and Article 51 of the United Nations Charter. It would also need to regulate state responsibility, outlining when a cyber operation can be attributed to a state, as well as the obligations of states to prevent malicious activities launched from their territory. Moreover, such a framework could codify the protection of civilian infrastructure, prohibiting cyber operations against hospitals, power grids, water systems, and other essential services whose disruption would cause disproportionate humanitarian harm.

Conclusion

Despite international humanitarian law's continued relevance, the digital domain creates significant legal uncertainties, particularly concerning attribution and defining the precise threshold at which a cyber operation constitutes the use of force or an "armed attack." These ambiguities create an accountability gap, underscoring the urgent need for clarity. To effectively preserve the protection of civilians and maintain accountability in this borderless domain, it is essential to establish a new, binding legal framework, potentially through a cyber warfare convention. Such a convention should clearly define the use-of-force thresholds and explicitly codify the protection of critical civilian infrastructure against cyber operations that would otherwise cause disproportionate humanitarian harm.

References

- Geneva Conventions of 1949 and Additional Protocols
  https://www.icrc.org/en/law-and-policy/geneva-conventions-and-their-commentaries
- Additional Protocol I (1977)
  https://www.icrc.org/sites/default/files/document/file_list/additional-protocols-geneva-conventions-1949-icrc-eng.pdf
- Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations
  https://ccdcoe.org/research/tallinn-manual/