Transformation on the Battlefield: The Impact of Digital Technologies on International Humanitarian Law

1. Somayeh Sadat Miri Lavasani *: Assistant Professor, Department of Law, Payame Noor University, Tehran, Iran

*Correspondence: s.mirilavasani@pnu.ac.ir

Abstract

Digital technologies have brought profound changes to international humanitarian law, presenting both significant opportunities and complex challenges. On one hand, technologies such as big data, artificial intelligence (AI), armed drones, and autonomous systems have enhanced the efficiency and precision of military and humanitarian operations, while enabling the monitoring and documentation of violations through satellite imagery, reporting applications, and open data. Additionally, emerging technologies such as blockchain have contributed to increased transparency and accountability in the management and tracking of humanitarian aid. On the other hand, these technologies have also introduced serious challenges. Among these are the difficulty in distinguishing combatants from civilians within cyberspace, ambiguity in attributing legal responsibility to states and non-state actors, and the lack of transparency in the decision-making algorithms used in smart weapons. These challenges necessitate a reexamination of the existing rules and interpretations of international humanitarian law to ensure the preservation of human control and legal accountability. Institutions such as the International Committee of the Red Cross and the United Nations are actively working to develop new legal frameworks to better respond to these developments. Ultimately, the responsible use of digital technology to strengthen the principles of humanitarian law requires precise legislation, comprehensive education, and effective monitoring of legal implementation. These approaches are essential to ensuring that human dignity and the protection of civilians are upheld in the digital age, and that international humanitarian law remains a credible and functional legal system.

Keywords: humanitarian law; digital age; emerging technologies; law of armed conflict; means of warfare.

Received: 05 November 2024
Revised: 28 January 2025
Accepted: 06 February 2025
Published: 25 March 2025

Citation: Miri Lavasani, S. S. (2025). Transformation on the Battlefield: The Impact of Digital Technologies on International Humanitarian Law. *Legal Studies in Digital Age*, 4(1), 1-10.

1. Introduction

In the twenty-first century, digital technologies are transforming all dimensions of human life at an unprecedented pace—from daily interactions to the conduct of war and peace. One domain increasingly impacted by these developments is the legal framework governing armed conflict, commonly referred to in international legal discourse as *international humanitarian law* (IHL). While the primary aim of IHL is to reduce human suffering during war and to protect those who do not take direct part in hostilities, the emergence of new technologies such as artificial intelligence (AI), military drones, autonomous weapons, big data, and cyber warfare has raised serious and novel questions regarding the effectiveness, enforceability, and interpretation of the norms of this legal regime (Melzer, 2016).

International humanitarian law is a body of customary and treaty-based rules designed to regulate the conduct of hostilities and to ensure protection for civilians, prisoners of war, the wounded, and humanitarian personnel during armed conflicts. It rests on fundamental principles such as the *principle of distinction* between military and civilian targets, the *principle of proportionality* in the use of force, and the *prohibition of unnecessary suffering* (Sassòli, 2019). Foundational documents such as the 1949 Geneva Conventions and their Additional Protocols of 1977 and 2005 form the cornerstones of this legal system. Although IHL has successfully adapted to past technological changes, it remains unclear whether it possesses sufficient normative elasticity to address today's intelligent and complex technologies.

In recent decades, digital technologies have profoundly altered the nature of armed conflict. Among the most critical of these is artificial intelligence, which—with its high processing power and machine learning capabilities—plays a role in military decision-making, enemy behavioral pattern analysis, and even target selection (Schmitt, 2020). Military drones, capable of carrying out operations at high altitudes without a pilot on board, have entrenched the practice of remote warfare. In addition, autonomous weapons—which can independently select and fire on targets without direct human intervention—are among the most legally contentious innovations in modern warfare (Icrc, 2021).

Big data, derived through digital surveillance, social media, and advanced information analytics, allows military commanders to anticipate and manage enemy movements or the collective behavior of civilians (Boulanin & Verbruggen, 2017). Alongside these, cyber warfare has emerged as a novel form of conflict that poses grave threats to civilian infrastructures such as hospitals, water systems, and information networks—often without a clear distinction between military and civilian objectives (Lewis, 2018).

The deployment of these technologies on the battlefield raises foundational questions about their compatibility with the entrenched principles of IHL. For instance: Can artificial intelligence uphold the principle of distinction? If a drone mistakenly targets civilians, who bears responsibility? And in a cyberattack that disables power to a hospital, which entity is held accountable? Such questions highlight not only the technical complexity of new technologies but also their profound implications for the ethical and legal foundations of IHL. Consequently, the central question of this article is formulated as follows: *What is the impact of modern digital technologies on the norms, interpretations, and implementation of international humanitarian law?* Addressing this question requires a precise analysis of how such technologies affect the core principles of IHL, the responses of international institutions, and the legal system's capacity for normative adaptation. The aim of this article is not to provide definitive answers but to map out the dimensions of this issue and offer a theoretical foundation for interdisciplinary dialogue in this critical field.

2. Materials and Methods

This study employs a descriptive-analytical method and relies on library-based resources for the writing and analysis.

3. Theoretical Foundations and Legal Frameworks

This section begins by elaborating on the fundamental principles of international humanitarian law.

3.1. Core Principles of International Humanitarian Law

International humanitarian law is grounded in a set of foundational principles whose purpose is to mitigate the harmful consequences of armed conflicts, protect victims of war, and regulate the use of force during hostilities. These principles form not only the theoretical underpinnings of this branch of international law but also serve as evaluative criteria for assessing the legality and proportionality of military actions. In the face of rapid technological advancements in modern warfare, reassessing these principles from both conceptual and operational standpoints has become more urgent than ever.

One of the cornerstone principles of IHL is the *principle of distinction*, which obligates parties to a conflict to distinguish at all times between military objectives and civilians. Only military targets may be attacked, and any assault intentionally directed at civilians or civilian objects is strictly prohibited (Sassòli, 2019). This principle is the bedrock of IHL, and without adherence

to it, the distinction between lawful warfare and indiscriminate killing collapses. In the digital age, the effective implementation of this principle is fraught with challenges, particularly when autonomous technologies or AI algorithms are involved in military targeting decisions.

The second core principle is the *principle of proportionality*. According to this rule, even when a military target is legitimate, the incidental harm inflicted on civilians or civilian property must not be excessive in relation to the concrete and direct military advantage anticipated (Dinstein, 2016). For example, a strike that destroys an enemy base but also kills hundreds of civilians may be deemed disproportionate. As big data and algorithmic analytics increasingly influence operational planning, calculating the proportionality between military benefit and human loss has become more intricate than ever.

The *principle of military necessity* is another foundational norm in IHL. It permits only those actions that are necessary to achieve a specific military objective and that comply with other rules of IHL (Roberts & Guelff, 2000). Military necessity cannot justify violations of other core principles, such as the prohibition of torture or the obligation to protect civilians; it must operate within a legally and ethically defined framework.

Closely related is the *principle of unnecessary suffering*, which prohibits the use of means and methods of warfare that cause superfluous injury or unnecessary pain (Icrc, 2005). This rule is especially relevant to the use of novel weaponry such as autonomous systems or neuro-control devices, which may have unpredictable effects on the physical and psychological well-being of human beings.

Together, these principles establish a normative architecture for limiting violence in war and safeguarding human dignity under extreme conditions. However, the advent of digital technologies and the transformation of modern warfare not only complicate the enforcement of these rules but also provoke fundamental questions regarding their interpretation, applicability, and adequacy in technologically advanced battlefields—questions that are crucial to the future viability of international humanitarian law.

3.2. Sources of International Humanitarian Law

As a branch of public international law, international humanitarian law (IHL) is based on multiple legal sources, including international treaties, customary international law, general principles of law, scholarly doctrine, and judicial practices. Understanding these sources is essential to grasp the scope, norms, and obligations of IHL—particularly in response to emerging challenges posed by technological advances in the military and digital domains. These sources not only provide binding legal frameworks but also play a decisive role in shaping legal responses to novel developments, such as cyber warfare or the deployment of artificial intelligence in armed conflict.

The primary source of IHL is found in international treaties and conventions that explicitly outline the duties of states and other parties engaged in hostilities. At the forefront of these are the four Geneva Conventions of 1949 and their two Additional Protocols of 1977 and 2005, which establish a comprehensive system for protecting civilians, the wounded, prisoners of war, and humanitarian personnel during wartime (Icrc, 2016). Protocol I pertains to international armed conflicts, while Protocol II introduces rules for non-international armed conflicts. Complementary treaties—such as the Chemical Weapons Convention, the Anti-Personnel Mine Ban Convention, and the Convention on Certain Conventional Weapons—further restrict the use of particular means and methods of warfare (Sassòli, 2019).

Customary international law constitutes the second fundamental source of IHL. These rules derive from the consistent and general practice of states, coupled with a belief in their legal obligation. Customary law is particularly relevant in cases where a state is not party to a specific treaty yet remains bound by the corresponding customary norms. The International Committee of the Red Cross (ICRC), through an extensive research project, has compiled a comprehensive body of customary IHL rules that now serve as a critical reference for analyzing diverse legal situations (Henckaerts & Doswald-Beck, 2005).

In addition to treaties and custom, *general principles of law* may fill normative gaps or aid in interpreting existing rules. Principles such as good faith, equity, and the prohibition of abuse of rights are applicable to IHL, especially when assessing state conduct involving novel technologies such as autonomous weapons or cyber operations (Dinstein, 2016).

Judicial decisions also constitute important interpretive sources. The International Court of Justice, ad hoc international criminal tribunals, and more recently, the International Criminal Court have played a significant role in clarifying the scope

and meaning of IHL norms. These rulings are particularly influential in identifying war crimes, defining individual responsibility, and regulating the lawful use of force (Cassese, 2008).

Finally, academic doctrine and legal scholarship function as subsidiary sources that assist in interpreting and developing the rules of IHL. The perspectives of legal experts are indispensable for analyzing emerging issues, particularly those related to the influence of digital technologies on the laws of war. In summary, the diversity and dynamism of IHL sources provide a legal framework that addresses both the traditional needs of armed conflict and the evolving technological challenges of the digital age—even as this framework is subjected to increasing strain in the face of such complexity.

3.3. The Position of New Technologies in the Existing Legal Framework: Gaps and Opportunities

Technological developments in areas such as artificial intelligence, big data, blockchain, and the Internet of Things (IoT) have presented new challenges to traditional legal systems. These technologies not only restructure human interactions but also call into question the conceptual foundations of many legal norms, such that aligning these norms with technological realities now requires rethinking foundational concepts, methodologies, and legal instruments (Brownsword, 2019).

One of the most prominent legal gaps in dealing with new technologies is the absence of clear frameworks for accountability and legal responsibility. For example, in the field of AI, assigning liability in cases where autonomous systems cause harm remains deeply problematic. In traditional legal structures, responsibility is often based on human fault or negligence. However, in machine-learning systems, there may be no clear human actor behind the outcome (Calo, 2016). This has prompted legal scholars to revisit concepts such as *agency*, *intent*, and *control*.

On the other hand, new technologies also offer considerable potential for enhancing legal systems. Blockchain technology, for instance, can significantly increase transparency and trust in legal transactions—especially in domains such as document registration, electronic voting, and intellectual property rights management (Werbach & Cornell, 2017). Similarly, the use of AI in arbitration and case analysis can accelerate adjudication and reduce human error.

A fundamental necessity in this context is to revisit traditional legal principles with the aim of aligning them with the logic of new technologies. Law must not merely react to technology; rather, it should proactively serve as a framework to guide and govern it. This affirmative approach requires the integration of interdisciplinary concepts and the application of data science, applied ethics, and systems engineering into the legislative process (Pagallo, 2013).

Ultimately, adapting legal systems to technological reality requires not only revising statutory laws but also transforming legal education, interpretive methodologies, and jurisprudential and philosophical approaches. The future of law lies not in opposition to technology, but in constructive engagement with it.

3.4. The Impact of Cyberspace on International Humanitarian Law

With the expansion of cyberspace and the digitalization of vast aspects of human life, armed conflicts have increasingly spilled into the virtual domain. In this context, international humanitarian law (IHL), as the legal framework governing armed conflict, faces emerging and complex challenges. Among the most pressing are cyberattacks with physical or psychological consequences and digital threats targeting civilian infrastructure—key intersections of cyber technologies and IHL (Schmitt, 2013). These two dimensions are explored below.

3.4.1. Cyberattacks and Attribution of Responsibility under IHL

Cyberattacks, when they reach a certain threshold of intensity, may be considered equivalent to armed attacks and fall under the regulatory scope of IHL. However, establishing the necessary threshold for applying the laws of armed conflict, and attributing legal responsibility to perpetrators in a complex and unstable cyber environment, is highly challenging. The first issue is attribution—many cyber operations are launched via anonymous networks, proxies, or non-state actors (Tsagourias & Buchan, 2015). This undermines the principle of state responsibility for the conduct of its forces or proxies.

Under international law, the "effective control" standard is used to establish state responsibility for non-state actors' conduct. However, in cyber operations, demonstrating effective control is exceptionally difficult, especially when attack vectors—such

as malware or ransomware—spread through decentralized and anonymous channels (Dinstein, 2020). Consequently, some scholars have proposed expanding the attribution standards to include notions such as "overall control" or even "technological cooperation relationships," though these concepts have yet to achieve recognition in international jurisprudence (Milanovic, 2015).

Furthermore, the principles of *distinction* and *proportionality*—cornerstones of IHL—encounter significant difficulties in cyber contexts. Evaluating human harm and collateral damage before a digital attack occurs is rarely feasible. For instance, a cyberattack disabling hospital power systems, even without causing physical destruction, may result in civilian deaths. Such scenarios demand a reassessment of how cyber operations align with humanitarian principles (Schmitt & Vihul, 2017).

3.4.2. Digital Threats to Civilian Infrastructure and the Duty of Protection

Within IHL, the principle of distinction between military and civilian targets, along with the obligation to protect civilian infrastructure, is fundamental. However, in cyber warfare, civilian infrastructure is highly vulnerable and often targeted due to its integration with digital systems such as electricity, water, health services, and transportation—all of which contain exploitable cyber vulnerabilities (Margulies, 2019).

Such attacks, even absent traditional military conflict, may cause humanitarian disasters. The 2010 Stuxnet malware incident, although targeting military assets, demonstrated how digital attacks can affect vital infrastructure. Other potential scenarios include cyberattacks on power plants or hospital control systems, which could result in lethal consequences (Tikk & Kerttunen, 2020). This necessitates expanding the concept of “attack” under IHL to encompass cyber actions with serious human or infrastructural consequences.

States also bear a duty to safeguard their civilian infrastructure from digital threats—not only during conflict but also in peacetime. Cybersecurity provisions for health, education, and relief systems are part of states’ preventive responsibilities under IHL and the principle of precaution (Greenwood, 2020).

Additionally, some scholars advocate for an *enhanced protection* principle, suggesting that critical facilities such as hospitals and essential infrastructure should receive a higher level of legal protection. In cyberspace, this translates to a complete prohibition of attacks against systems vital to civilian survival, even if these systems host limited military functionality (Kube & Kühn, 2021).

Overall, cyberspace—with its layers of ambiguity regarding attribution, legal responsibility, and civilian protection—constitutes one of the most formidable challenges facing IHL in the 21st century. While traditional legal frameworks remain the starting point for analysis, technological transformations demand the development of new legal structures or at least updated interpretations to address the realities of cyber warfare. Enhancing transparency, creating collective attribution mechanisms, and establishing digital protection protocols for civilians are among the most pressing initiatives for the international community.

3.5. Big Data and Electronic Surveillance

The emergence of digital technologies—particularly big data and electronic surveillance tools—has fundamentally altered the role of information in armed conflict. On one hand, the analysis of vast data sets has become central to the identification and precise targeting of military objectives. On the other hand, the extensive use of personal data in this context raises serious concerns regarding privacy violations during wartime. Both dimensions are discussed below.

3.5.1. Data Use in Target Identification and Intelligence Operations

Big data analytics—processing massive volumes of digital information from diverse sources such as social media, satellite imagery, and intercepted communications—are increasingly utilized in military operations. These tools assist in identifying individuals, predicting enemy behavior, locating targets, and optimizing strikes. Some armed forces, such as those of the United States and Israel, actively rely on data-driven algorithms for targeting decisions (Bode & Huelss, 2018).

Yet, aligning this process with core IHL principles, especially distinction and proportionality, presents serious challenges. Raw data may be inaccurate, incomplete, or tainted by algorithmic bias. Consequently, targeting based on such information may inadvertently harm civilians or civilian objects. Moreover, data analysis replacing human judgment may exclude the ethical and contextual considerations necessary for life-or-death decisions (Crootof, 2016).

Furthermore, when decision-making is based on data whose collection and processing remain opaque—particularly when governments or militaries withhold details about the algorithms or criteria used—it impairs legal accountability and violates the principle of responsibility (Schmitt, 2020).

3.5.2. Privacy Concerns in Armed Conflict

Although privacy has traditionally been framed within the domain of human rights law, it is increasingly becoming a concern within IHL. In modern conflicts, military and intelligence agencies collect vast amounts of personal civilian data, including phone calls, geolocation, digital interactions, and even biometric traits like facial recognition or voice samples. Often, this data is harvested without individual consent or awareness (Kleffner, 2021).

While IHL does not explicitly address the right to privacy, its foundational principles—such as the principle of humanity and the prohibition of unnecessary suffering—offer a normative basis for protecting civilian privacy. Excessive surveillance, particularly in occupied or militarized zones, can result in continuous monitoring, psychological distress, and disruption of daily life—all of which contradict the spirit of IHL (Lubell & Pejic, 2020).

Moreover, the transfer of personal data between states or coalition forces without legal safeguards raises serious concerns. In some cases, such data sharing has led to the arrest or even execution of suspects based on unverifiable information (Wright & Raab, 2014).

Given these legal gaps, some jurists have proposed incorporating general human rights norms—such as the right to privacy enshrined in Article 17 of the International Covenant on Civil and Political Rights—into IHL, especially in contexts involving digital surveillance and information technologies (Benvenisti, 2013).

Although big data and electronic surveillance may enhance precision and effectiveness in military operations, they pose severe legal and ethical risks to international humanitarian law. Mistrust of flawed data, the exclusion of human judgment, and the erosion of civilian privacy are among the most significant threats. Therefore, updated interpretations of IHL are urgently needed to regulate data use responsibly and to develop new protective mechanisms for civilians within digital conflict environments.

4. Challenges of International Humanitarian Law in the Face of Digital Technologies

One of the most pressing challenges in the intersection of digital technologies and international humanitarian law (IHL) is the difficulty of distinguishing between combatants and civilians in cyberspace. The complexity and opacity of the cyber domain blur traditional lines of distinction. Unlike conventional warfare—where physical targets are visible and identifiable—cyber operations are often indirect, immaterial, and conducted through data or software attacks, making it difficult to ascertain the role of individuals or groups (Schmitt, 2013). For instance, a computer system may be used simultaneously for military and civilian purposes, or a cyberattack may be launched through networks used primarily by civilians, thereby increasing the risk of unintended civilian harm. These complexities make it fundamentally difficult to apply and enforce IHL principles in the cyber context.

Another key obstacle is the attribution of legal responsibility to states and non-state actors. Cyberattacks are frequently carried out by non-state groups, hacker collectives, or proxies, making it difficult to assign accountability to a specific government (Tsagourias & Buchan, 2015). Under international law, attribution is based on the principle of "effective control," which is particularly hard to prove in cyberspace due to the immaterial and covert nature of attacks (Dinstein, 2020). This complicates legal accountability and allows many harmful cyber operations to go unpunished, revealing serious enforcement gaps in IHL.

A further concern is the opacity of decision-making algorithms in smart weapons, which undermines the integrity and fairness of these technologies. Intelligent weapons using AI to identify and strike targets operate based on complex algorithms that are often incomprehensible and uncontrollable by humans (Crootof, 2016). This "black box" nature of the technology limits the ability to evaluate the correctness of decisions and may result in critical misjudgments regarding target legitimacy. Moreover, the lack of transparency impedes accountability—making it unclear whether responsibility lies with the system's designer, the commanding officer, or the system itself. Such ambiguity raises serious concerns about compliance with IHL principles such as distinction and proportionality.

Ultimately, the structural misalignment between emerging technologies and existing legal obligations under IHL poses a significant threat to the preservation of fundamental humanitarian norms. Technologies like armed drones, autonomous weapons, and complex data systems are often developed and deployed in ways that fall outside or challenge the scope of current IHL frameworks (Heyns, 2013). Traditional IHL is grounded in human-centric norms and judgment; however, modern smart technologies increasingly remove humans from the decision-making loop. This necessitates a fundamental revision and updating of legal instruments to ensure that principles such as civilian protection, accountability, and human control remain intact in technologically mediated warfare (Scharre, 2018). Facing digital technologies in IHL thus requires developing novel legal concepts, clarifying responsibilities, and establishing precise and flexible regulations to address the intricacies of cyberspace and modern warfare. Furthermore, international cooperation in creating comprehensive regulatory frameworks and robust oversight mechanisms is essential to prevent abuse and safeguard humanitarian norms.

5. Opportunities of Digital Technology for Enhancing IHL

Digital technologies have created unprecedented opportunities for enhancing international humanitarian law, particularly in improving civilian protection and the efficiency of humanitarian operations. One of the most important capacities of these technologies is the ability to monitor and document violations using satellite imagery, mobile applications, and open data. These tools enable rapid and accurate observation and documentation of events in conflict zones, which can play a key role in proving war crimes and increasing legal accountability (Kleinfeld et al., 2017). For instance, high-resolution satellite images can detect urban destruction or encroachments on protected zones, while mobile apps allow civilians to report violations directly, and open data provides independent analytical capacity and greater transparency.

In addition, digital technology significantly enhances the efficiency of humanitarian aid and emergency response. Cloud-based data management systems, geospatial tools, and AI applications help humanitarian organizations better allocate resources and optimize aid distribution (Guberek et al., 2019). These technologies reduce resource waste, speed up crisis response, and improve coordination among diverse actors. For example, in recent humanitarian crises, digital data analysis has helped identify urgent aid zones and facilitated the rescue of thousands of lives.

Another transformative application is the use of blockchain in tracking humanitarian aid. Blockchain, as a decentralized and immutable ledger, allows precise and transparent recording of transactions, thereby increasing trust in aid distribution processes (Tapscott & Tapscott, 2017). It prevents misuse, corruption, and loss of resources during aid transfers, offering donors and recipients greater assurance. Some international and non-governmental organizations are now using blockchain to track financial and material aid, ensuring that it reaches those in genuine need.

Finally, digital technology provides innovative tools for education and promotion of IHL. Virtual reality, serious games, online courses, and social media platforms have expanded access to humanitarian legal knowledge and raised public awareness (Björkdahl & Buckley Zistel, 2017). These tools are especially valuable in training military personnel, human rights activists, and the general public, equipping them to understand IHL principles and take effective action during crises. For example, digital platforms can offer interactive conflict simulations that provide more tangible and experiential learning than traditional methods.

Overall, digital technology holds immense potential for supporting IHL and improving the performance of institutions committed to humanitarian principles. However, responsible use of these tools and acknowledgment of their limitations are critical to ensuring they are effectively aligned with the foundational values of IHL.

6. Institutional and Procedural Developments in Response to Digital Challenges

Institutional and procedural developments have played an increasingly important role in responding to digital technology challenges, particularly within the realm of international humanitarian law. The International Committee of the Red Cross (ICRC) has been one of the most active institutions in this space, articulating clear positions on autonomous and intelligent weapon systems. The ICRC emphasizes that such systems must remain under meaningful human control and that decisions related to targeting and lethal force must never be delegated entirely to machines (Icrc, 2018). It further underscores the importance of respecting IHL principles such as distinction, proportionality, and precaution, while calling for the development of new legal rules to respond to the complexities of emerging technologies (Icrc, 2020).

At the international level, the United Nations has undertaken extensive diplomatic efforts to establish new legal frameworks. Meetings of the Group of Governmental Experts (GGE) on Lethal Autonomous Weapons Systems and cyber warfare exemplify such efforts, aimed at addressing current legal gaps and developing rules to limit the use of dangerous technologies in armed conflict (Unga, 2019). While no binding global consensus has yet been reached, ongoing multilateral dialogue paves the way for the eventual adoption of new treaties and protocols (Schmitt, 2020).

The role of state responsibility and individual accountability in the context of new technologies is also of growing importance. While IHL traditionally emphasizes state responsibility for the conduct of national or proxy forces, digital and autonomous systems complicate this attribution (Dinstein, 2020). As a result, the legal spotlight is increasingly directed at individual accountability—particularly that of commanders and decision-makers—to ensure compliance with humanitarian principles (Crootof, 2016). These responsibilities include careful oversight of technological applications, assurance of human control, and liability for violations, all of which are vital for upholding ethical and legal standards in modern warfare.

7. Conclusion

Digital technologies have significantly reshaped the structure and function of international humanitarian law (IHL), introducing both novel challenges and valuable opportunities to this legal system. Historically, IHL was developed based on assumptions aligned with the characteristics of traditional armed conflicts, which were predominantly physical and human in nature. However, the advent of digital technologies—such as autonomous weapons, cyberattacks, big data, and artificial intelligence—has challenged these foundational assumptions. As a result, core principles like the distinction between combatants and civilians, accountability, and transparency in operations are being reinterpreted in new and complex ways.

One of the most profound effects of digital technology on IHL is the increasing difficulty in distinguishing military actors from civilians in cyberspace. While this principle remains fundamental to civilian protection, the immaterial and invisible nature of cyber operations and intelligent systems makes accurate target identification increasingly complex. Additionally, digital technologies have introduced ambiguity in determining legal responsibility. Many attacks and operations are now carried out by non-state actors or autonomous systems, complicating efforts to attribute them to specific states or individuals.

On the other hand, these same technologies have enhanced transparency and operational efficiency in the implementation of IHL. The use of satellite data, reporting applications, blockchain for aid tracking, and digital educational tools provides better monitoring capabilities, enables faster crisis response, and increases public awareness. These tools can help strengthen accountability and promote respect for civilian rights.

Nevertheless, technological advancements have also highlighted the need to revisit and update certain IHL rules and interpretations. Traditional principles—rooted in human judgment—must now be adapted to account for automated and intelligent technologies in order to preserve human oversight and legal accountability. New legal frameworks must be developed to address gaps in the attribution of responsibility in digital environments and to regulate the legal status of complex technologies. In this regard, it is recommended that multilateral actions and international cooperation be accelerated to legislate and revise existing IHL provisions.

Drafting new treaties and protocols that clearly define the scope and permissible use of emerging technologies is essential. At the same time, building global monitoring capacities and accountability mechanisms must be prioritized to ensure effective and transparent enforcement of humanitarian rules. Beyond legislation, promoting education and raising awareness about the

implications of digital technologies on IHL is also critical. This should include training for military personnel, legal institutions, humanitarian organizations, and civil society actors so that all stakeholders can contribute to upholding humanitarian principles.

Ultimately, digital technology can be a powerful tool for reinforcing and supporting IHL—provided that legal frameworks, policies, and legal cultures are modernized and employed in a responsible and humane manner. These measures can help ensure that, even in the digital age, human dignity and civilian protection remain paramount and that IHL continues to serve as an effective and credible body of law.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all who helped us through this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Benvenisti, E. (2013). Sovereigns as Trustees of Humanity: On the Accountability of States to Foreign Stakeholders. *The American Journal of International Law*, *107*(2). https://doi.org/10.5305/amerjintelaw.107.2.0295

Björkdahl, A., & Buckley Zistel, S. (2017). *The Oxford Handbook of Gender and Conflict*. Oxford University Press.

Bode, I., & Huelss, H. (2018). Autonomous weapons systems and changing norms in international relations. *Review of International Studies*, *44*(3). https://doi.org/10.1017/S0260210517000614

Boulanin, V., & Verbruggen, M. (2017). *Mapping the development of autonomy in weapon systems*. Stockholm International Peace Research Institute.

Brownsword, R. (2019). *Law, Technology and Society: Reimagining the Regulatory Environment*. Routledge. https://doi.org/10.4324/9781351128186

Calo, R. (2016). Robotics and the Lessons of Cyberlaw. *California Law Review*, *103*(3).

Cassese, A. (2008). *International criminal law*. Oxford University Press.

Crootof, R. (2016). War Torts: Accountability for Autonomous Weapons. *University of Pennsylvania Law Review*, *164*(6).

Dinstein, Y. (2016). *The conduct of hostilities under the law of international armed conflict*. Cambridge University Press. https://doi.org/10.1017/CBO9781316389591

Dinstein, Y. (2020). *The Conduct of Hostilities under the Law of International Armed Conflict*. Cambridge University Press.

Greenwood, C. (2020). The Law of Armed Conflict and the Use of Force. In C. Warbrick & C. Greenwood (Eds.), *International Law and the Classification of Conflicts*. Oxford University Press.

Guberek, T., D'Ignazio, C., & Taylor, L. (2019). Data for humanitarian action: challenges and opportunities. *International Review of the Red Cross*, *101*(911).

Henckaerts, J. M., & Doswald-Beck, L. (2005). *Customary international humanitarian law: Volume I–Rules*. Cambridge University Press. https://doi.org/10.1017/CBO9780511804700

Heyns, C. (2013). *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions*.

Icrc. (2005). *Customary international humanitarian law: Volume I–Rules*. Cambridge University Press.

Icrc. (2016). *Commentary on the First Geneva Convention*. Cambridge University Press.

Icrc. (2018). *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*. ICRC.

Icrc. (2020). *Autonomous Weapons Systems: Technical, Military, Legal and Humanitarian Aspects*. ICRC.

Icrc. (2021). *Autonomous weapon systems: Implications of increasing autonomy in the critical functions of weapons*. International Committee of the Red Cross.

Kleffner, J. (2021). The Application of International Humanitarian Law to Cyber Operations. In *Research Handbook on International Law and Cyberspace*. Edward Elgar Publishing.

Kleinfeld, R., Peksen, D., & Waltz, J. (2017). Satellite Imagery and the Detection of Mass Atrocities. *Journal of Peace Research*, *54*(2).

Kube, H., & Kühn, A. (2021). Cyber Attacks on Civilian Infrastructure: Legal Challenges under IHL. *German Yearbook of International Law*, *63*(1).

Lewis, J. A. (2018). *Cybersecurity and cyberwarfare: What Everyone Needs to Know*. Oxford University Press.

Lubell, N., & Pejic, J. (2020). Human rights obligations and armed conflict: The interplay between international humanitarian law and international human rights law. *International Review of the Red Cross*, *102*(913).

Margulies, P. (2019). Sovereignty and Cyber Attacks: Technology's Challenge to the Law of Armed Conflict. *Maryland Journal of International Law*, *34*(2).
Melzer, N. (2016). *Interpretive guidance on the notion of direct participation in hostilities under international humanitarian law*. International Committee of the Red Cross.
Milanovic, M. (2015). Attribution and the Law of Targeting. In E. Wilmshurst (Ed.), *International Law and the Classification of Conflicts*. Oxford University Press.
Pagallo, U. (2013). *The Laws of Robots: Crimes, Contracts, and Torts*. Springer. https://doi.org/10.1007/978-94-007-6564-1
Roberts, A., & Guelff, R. (2000). *Documents on the Laws of War*. Oxford University Press.
Sassòli, M. (2019). *International Humanitarian Law: Rules, controversies, and solutions to problems arising in warfare*. Edward Elgar Publishing. https://doi.org/10.4337/9781786438553
Scharre, P. (2018). *Army of None: Autonomous Weapons and the Future of War*. W. W. Norton & Company.
Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press. https://doi.org/10.1017/CBO9781139169288
Schmitt, M. N. (2020). The Principle of Distinction and New Warfare Technologies. In E. Wilmshurst (Ed.), *International Law and the Classification of Conflicts*. Oxford University Press.
Schmitt, M. N., & Vihul, L. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press. https://doi.org/10.1017/9781316822524
Tapscott, D., & Tapscott, A. (2017). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Portfolio.
Tikk, E., & Kerttunen, M. (2020). *The Role of the UN in Addressing Cyber Threats: Towards a Cyber Stability Framework*. Finnish Institute of International Affairs.
Tsagourias, N., & Buchan, R. (2015). *Cyber War and International Law*. Cambridge University Press.
Unga. (2019). *Report of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems*.
Werbach, K., & Cornell, N. (2017). Contracts Ex Machina. *Duke Law Journal*, *67*(2).
Wright, D., & Raab, C. (2014). *Privacy and Surveillance: The Multidisciplinary Perspective*. Springer.