https://doi.org/10.70265/DPOF9977

THE IMPACT OF THE USE OF NEW TECHNOLOGIES AND MEANS OF WARFARE ON THEIR REGULATION FROM THE PERSPECTIVE OF INTERNATIONAL HUMANITARIAN LAW

Luiza Raduslav, Cezar Vasilescu

Summary: *Emerging military technologies pose fundamental challenges for international humanitarian law. The study examines the hypothesis that these technologies create a significant normative vacuum, as the traditional principles of distinction, proportionality and precaution in attack were designed for conventional conflicts and require substantive reinterpretation. The study results question the adequacy of the existing legal framework.*

Keywords: *international humanitarian law; lethal autonomous systems; cyber warfare; drones; distinction principle; proportionality; normative vacuum; meaningful human control; Tallinn Manual 2.0.*

INTRODUCTION

The transformation of contemporary armed conflicts reflects the convergence between the technological revolution and the persistence of the phenomenon of war as a way of resolving interstate disputes. Although war, armed conflict in general, has been an organic part of the life of society since ancient times and has contributed to its shaping alongside political, ideological, economic, technical-scientific, cultural, and spiritual factors, its contemporary dimension is profoundly modified by the integration of disruptive technologies into military instruments.

Roger Trinquier noted in 1980 the importance of revolutions and wars in the history of peoples. Gaston Bouthoul (1950, p. 8), the founder of polemology, considered war, peace and conflict as an inseparable trilogy of the life of societies. These classical perspectives, although useful for understanding the continuity of the phenomenon, need to be supplemented by the recent technological developments that fundamentally modify the nature of armed conflict.

From a historical-legal perspective, war has been considered a licit phenomenon from Antiquity until the 20th century. Hans Kelsen (1881-1972) argued that the primacy of international law is the basis of pacifism and that its superiority can transform the territorial spaces of state entities

into legally delimited areas, thus making aggression anti-legal (Kelsen, 1944).

The contemporary context is marked by what the specialized literature calls the Revolution in Military Affairs (RMA), a concept that designates fundamental transformations in the ways of waging war, determined by major technological innovations. Scharre (2024, p. 7) notes that stage after stage, war has increased its destructive power, the effects on society being devastating.

The accelerated development of these technologies raises fundamental issues of legal compatibility that require systematic investigation.

1. RESEARCH HYPOTHESIS

Emerging military technologies (lethal autonomous systems, offensive cyber capabilities and unmanned aerial platforms) create a normative vacuum in international humanitarian law, as the traditional principles of distinction, proportionality and precaution in attack were designed for conventional conflicts and require substantive reinterpretation to respond to the specific characteristics of these new means of warfare. The decision-making autonomy of artificial systems, the operational distance between attacker and target, as well as the instantaneous cross-border effects of cyberattacks call into question the adequacy of the existing legal framework. Examining this hypothesis involves analysing the extent to which current IHL can be effectively applied to new technologies or whether specific legal instruments need to be developed.

2. CONCEPTUAL FRAMEWORK AND LITERATURE REVIEW

2.1. Terminological delimitations

Rigorous analysis of the interaction between emerging military technologies and IHL requires preliminary clarification of the key concepts used in this study. Lethal autonomous weapon systems, known in the literature under the acronym LAWS, represent a technological category whose degree of autonomy varies significantly. According to the US Department of Defense Directive 3000.09 (2023), the fundamental distinction is made between systems with semi-autonomous operation, which require human validation before executing each action, systems with supervised autonomous operation, in which the human operator can intervene to stop but the system operates independently after activation, and fully autonomous systems, which perceive, decide and act without any human intervention after activation.

In the field of offensive cyber operations, the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Schmitt, 2017) provides a reference definition of a cyber-attack as an offensive or defensive cyber

operation that can reasonably be expected to cause injury or death to persons or damage to property, according to Rule 92 on page 415. It is essential to emphasize that this Manual, although developed by a group of international experts under the aegis of the NATO Cooperative Cyber Defence Centre of Excellence, represents a doctrinal interpretation without legally binding force, constituting a useful guideline rather than a binding legal instrument for states.

2.2. Literature review analysis

The issue of applying international humanitarian law to emerging military technologies has generated a substantial academic literature over the past decade, marked by intense debates about the adequacy of the existing regulatory framework. Paul Scharre's (2024) seminal work, Four Battlegrounds: Power in the Age of Artificial Intelligence, provides a comprehensive analysis of the impact of artificial intelligence on contemporary conflicts, arguing that the decision-making autonomy of weapons systems crosses what the author calls a moral and ethical Rubicon. Scharre examines not only the technical dimension of these systems, but also their strategic and normative implications, proposing a series of gradual regulatory solutions that balance the need for humanitarian protection with the strategic realities of global military competition.

In the field of cyber warfare, the Tallinn Manual 2.0 (Schmitt, 2017) represents the most ambitious attempt to codify the applicable norms, being the result of the work of an international group of experts who systematically analysed the applicability of IHL principles and rules to operations in cyberspace. The Manual addresses complex issues such as the qualification of cyberattacks as acts of war, the attribution of responsibility in the context of multi-actor operations, and the application of the principles of distinction and proportionality to dual-use infrastructures. The main criticism of this Manual, acknowledged by its authors themselves, is that, being a doctrinal document and not an international treaty, it reflects the interpretations of a limited group of experts and does not benefit from the democratic legitimacy of the interstate negotiation process.

The International Committee of the Red Cross (ICRC) has developed a distinct institutional position on lethal autonomous systems, promoting the concept of meaningful human control as a fundamental principle that should govern the use of these technologies. In its public positions from 2021 and 2023, the ICRC argues that maintaining human control is not just a legal requirement derived from existing IHL norms, but represents a fundamental ethical imperative that reflects the humanitarian values underlying this body of norms. The organization proposes that states adopt clear standards on the minimum level of human control required in different phases of the use of autonomous systems, from development and testing to operational deployment.

From the perspective of practical analysis of the use of emerging technologies in real-world conflicts, the Royal United Services Institute (RUSI, 2024) study on drone warfare in Ukraine provides essential empirical data on how these systems are transforming the tactical and operational dynamics of contemporary conflict. The RUSI research documents the widespread use of FPV (First Person View) drones and loitering munitions, highlighting both the tactical advantages they provide – increased accuracy, reduced cost, ability to saturate enemy defences – and the legal and ethical challenges they generate, particularly in terms of target verification and real-time collateral damage assessment.

Critical legal literature, however, raises serious doubts about the sufficiency of current approaches. Heyns (2016), in his report as UN Special Rapporteur on extrajudicial, summary or arbitrary executions, argues that lethal autonomous systems raise fundamental issues of legal responsibility that cannot be resolved by simply reinterpreting existing norms, but require new legal instruments that clearly define the obligations of states in the development, testing and use of these technologies. Anderson and Waxman (2017), analysing American state practice, suggest that current debates are often based on speculative scenarios rather than rigorous analysis of the actual technical capabilities of existing systems, leading to an overly polarized discussion between advocates of a total ban and those of full permissiveness.

The present study positions itself within this literature by adopting a perspective that combines normative legal analysis with an examination of available empirical data from contemporary conflicts. Its original contribution lies in systematically assessing the extent to which specific principles of IHL –distinction, proportionality, and precaution – can be operationalized in the context of each of the three major categories of emerging technologies, identifying both areas of compatibility and normative gaps that require legislative intervention or jurisprudential development.

3. EVOLUTION OF THE LEGAL FRAMEWORK FOR REGULATING COMBAT MEANS

3.1. Fundamental principles of IHL in the conduct of hostilities

International humanitarian law is built on three cardinal principles governing the conduct of hostilities, the application of which to new technologies is the central subject of this analysis. The principle of distinction, enshrined in Article 48 of Additional Protocol I to the 1977 Geneva Conventions, imposes a fundamental obligation to distinguish at all times between combatants and civilians, as well as between military and civilian objectives. This obligation presupposes the ability to identify and recognize the status of targeted persons and objects, which becomes

problematic in the case of systems operating autonomously or at a significant distance.

The principle of proportionality, regulated in Article 51, paragraph 5(b) of the same Protocol, prohibits attacks that would cause incidental loss of life among the civilian population, injury to civilians and damage to civilian objects excessive in relation to the concrete and direct military advantage expected. The application of this principle requires a complex, contextual and anticipatory assessment of the effects of an attack, an assessment that raises serious questions when delegated to an algorithm or when the operator is thousands of kilometers away from the theatre of operations. The precautionary principle, provided for in Article 57, requires that all possible measures be taken to avoid and, in any case, reduce to a minimum incidental loss of life among the civilian population. This principle implies an active responsibility for prior verification and validation of targets, a responsibility whose fulfilment becomes uncertain in the context of the use of technologies with a high degree of autonomy.

3.2. The mechanism for reviewing new weapons under Article 36

Additional Protocol I of 1977 introduces an essential normative innovation in Article 36 by establishing the obligation of states to review new weapons, means and methods of warfare in order to determine whether their use is compatible with applicable international law. The text of the article stipulates that in researching, developing, acquiring or adopting a new weapon, means or method of warfare, a High Contracting Party has the obligation to determine whether their use is prohibited, in certain or all circumstances, by the provisions of the Protocol or by any other applicable rule of international law.

This review obligation, known in state practice as Article 36 review, is a preventive mechanism designed to ensure that weapons comply with IHL before they are integrated into military arsenals. However, the practical implementation of this obligation varies significantly between states, with substantial differences in the review procedures, the assessment criteria used, the technical and legal expertise mobilized, and the degree of transparency of the process. These inconsistencies create the risk that the same technology may be considered legal in one jurisdiction and illegal in another, thus undermining the uniformity of application of IHL.

In the case of emerging technologies characterized by decision-making autonomy and adaptive capabilities, the application of the Article 36 review mechanism raises specific methodological challenges. Evaluating a traditional weapon system involves testing relatively stable and predictable characteristics – range, accuracy, destructive power. In contrast, machine learning-based systems may exhibit behaviors that were not explicitly programmed, but rather acquired through training on data sets, and these

behaviors may evolve depending on new data with which the system interacts.

This variability makes it difficult to certify ex-ante compliance with IHL, raising the question of whether the review should be a one-time process carried out before the adoption of the weapon or an ongoing process that monitors the behavior of the system during its operational use.

3.3. Historical precedents for regulating new military technologies

The history of international humanitarian law provides multiple examples of normative responses to the emergence of military technologies whose use raised major humanitarian problems. The 1868 St. Petersburg Declaration, which prohibited the use of certain explosive projectiles, represents the first international instrument to specifically regulate a category of weapons on the basis of their effects considered to be excessively injurious. This historical precedent is relevant to the contemporary debate because it demonstrates that states have recognized since the 19th century that not every technical means of defeating an adversary is permissible in war, even if it offers military advantages.

The 1925 Geneva Conventions on the Prohibition of Chemical and Biological Weapons, subsequently supplemented by the 1993 Chemical Weapons Convention and the 1972 Biological Weapons Convention, illustrate a comprehensive prohibition approach based on the inherent unacceptability of certain categories of weapons, regardless of the specific context of their use. These conventions do not allow for exceptions for uses considered precise or proportionate, but establish an absolute prohibition based on the impossibility of controlling the effects of these weapons and the moral repugnance they generate.

The 1997 Ottawa Convention on the Prohibition of Anti-Personnel Mines and the 2008 Oslo Convention on the Prohibition of Cluster Munitions are more recent examples of legal instruments that have banned certain weapons not on the basis of their chemical or biological nature, but because of their indiscriminate effects in practice and their long-term impact on civilian populations. These conventions were adopted through innovative diplomatic processes, outside the traditional framework of the Geneva Conference on Disarmament, demonstrating that new problems can require new institutional approaches.

The relevance of these precedents for the regulation of emerging technologies lies in the various lessons they offer. First, they demonstrate that the international community has been able, in certain circumstances, to adopt bans or significant limitations on certain categories of weapons even in the absence of an actual humanitarian catastrophe, based on anticipatory risk assessments. Second, these precedents show that different types of weapons may require different types of normative responses –from outright bans to regulation of use or technical design standards. Third, they highlight

the importance of mobilizing civil society and public opinion in the process of adopting new norms, an element that is becoming increasingly relevant in the context of the debate on lethal autonomous systems.

4. ANALYSIS OF EMERGING TECHNOLOGIES: CHALLENGES FOR IHL

4.1. Cyber warfare and the issue of qualification as an armed conflict

In the international security environment is increasingly talking about cyber-attacks and wars that affect human security globally. The Romanian National Defence Strategy of the Country (Presidential Administration, 2020, p. 25) highlights that cyber-attacks launched by state and non-state entities on critical IT and communications infrastructures have become a top-ranking threat, their intensity, complexity and diversity being on an evolutionary trend, constantly increasing.

From an IHL perspective, cyber operations pose specific challenges that test the limits of the current legal framework. The first of these concerns the issue of attribution, namely the identification of the real aggressor, the physical location from which the attack was launched and its final beneficiary, given that cyber actors use sophisticated concealment techniques such as false flag operations, the use of proxy servers distributed across multiple jurisdictions, or the exploitation of compromised computer networks. This technical opacity makes it extremely difficult to apply IHL rules that require the clear identification of the belligerent parties.

The second major challenge is the application of the distinction principle in cyberspace, where infrastructures are often dual-use, serving both civilian and military purposes. A cyberattack on an electrical grid can simultaneously affect hospitals, schools and civilian homes on the one hand, and military command centres or air defence systems on the other. The technical capacity to limit the effects exclusively to the military component is often non-existent, which calls into question the possibility of respecting the distinction between military and civilian objectives.

The third problematic dimension concerns the assessment of proportionality in the context of cyber-attacks, where cascading effects on interdependent infrastructures can be difficult to predict ex ante. An apparently limited attack on an information system can generate chain consequences affecting related systems essential to the civilian population, from the supply of drinking water to the functioning of medical or transport safety systems. This structural unpredictability of the effects raises serious doubts about the attacker’s ability to assess with certainty the proportionality of his action to the military advantage sought.

4.2. Unmanned Aerial Platforms: The Case of the Ukraine Conflict

Drones are technical means without a human pilot on board, directed by their own autopilot or by connection to the ground command centre, used in observation and reconnaissance missions, but also for attacks with lethal payloads. The conflict in Ukraine, which began in February 2022 and continues to this day, has demonstrated a fundamental tactical transformation produced by the massive use of drones, both for strategic and operational reconnaissance, and for direct attacks on land and sea targets. The analysis carried out by the Royal United Services Institute (RUSI, 2024) highlights that FPV (First Person View) drones and loitering munitions have radically changed the dynamics of the contemporary battlefield, allowing the engagement of targets with increased precision at significantly reduced acquisition and operating costs compared to conventional weapons systems.

From a legal perspective, the use of drones raises specific issues related to the operator's effective control over the system. The ability of the operator located at a considerable distance to assess in real time compliance with the distinction principle depends crucially on the quality of the video transmission and other sensors, which can be affected by intentional or accidental electromagnetic interference, weather conditions, or the latency inherent in satellite communication systems. In such circumstances, the decision to engage a target is based on incomplete or degraded information, which significantly increases the risk of violating the distinction obligation.

The issue of legal liability for errors committed in the use of drones adds another dimension of complexity. Determining who bears legal liability if a drone mistakenly attacks a protected civilian target requires clarifying the role and obligations of each actor involved in the decision-making and operational chain. Liability may lie with the operator who actually carried out the attack, the commander who authorized the mission without sufficiently verifying its parameters, the intelligence officer who provided erroneous data about the target, or even the manufacturer of the technology if a technical failure contributed to the error.

4.3. Lethal Autonomous Systems: The Responsibility Dilemma

The use of fully autonomous weapons generates what Scharre (2024, p. 325) calls the crossing of a moral and ethical Rubicon in the evolution of combat means. The fundamental problem is not of a purely technical nature, but concerns the delegation to an artificial system of the decision to take human life, thus eliminating direct human judgment and responsibility at the critical moment of the attack.

From the strict perspective of IHL, lethal autonomous systems create what the specialized literature has called the accountability gap, namely a vacuum of legal responsibility that occurs when violations of the norms are committed by non-human entities. When an autonomous system mistakenly attacks a protected civilian objective, the attribution of legal responsibility

becomes extremely problematic. The manufacturer of the artificial intelligence algorithm can argue that the system was used in operational conditions different from those for which it was designed and tested. The military commander who authorized the deployment of the system can claim that he had reasonable confidence in its certified technical capabilities.

The US Department of Defense (2023, p. 330) maintains a position that seems to resolve these dilemmas by stating that the laws of war do not require weapons to make legal distinctions, even if the weapon can be characterized as being capable of making technical distinctions, the responsibility for compliance with IHL remaining entirely with the person using the weapon. This interpretation, while legally valid in the context of traditional weapons where the human operator maintains direct and continuous control over use, does not resolve the practical and moral problem of effective control in the case of fully autonomous systems.

5. REGULATORY VACUUM AND LEGAL SOLUTIONS

5.1. Limitations of the existing legal framework

The current legal framework of IHL presents significant gaps in relation to the emerging technologies analysed, gaps that derive primarily from the lack of specific definitions for the new concepts that these technologies introduce into the vocabulary of armed conflicts. Terms such as cyber-attack, lethal autonomous system or effective control are not explicitly defined in existing IHL treaties, which leaves room for divergent interpretations between states and complicates the uniform application of the rules.

The inadequacy of classic tools for evaluating new weapons becomes evident when we try to apply the test offered by the Martens Clause, the classic clause that invokes the laws of humanity and the demands of public conscience as the ultimate benchmark in determining the legality of a weapon or method of warfare. This clause, formulated at the end of the 19th century, presupposes the existence of a relatively stable and shared moral consensus on what constitutes acceptable conduct in war.

5.2. Regulatory proposals

The literature and emerging state practices suggest several possible ways to address the identified normative gap. Scharre (2024, pp. 492-500) proposes a gradual approach that would categorically prohibit lethal autonomous systems designed to directly target people, while maintaining the permissibility of the use of systems designed to destroy material targets, provided that human oversight of their operation is maintained.

The International Committee of the Red Cross promotes the implementation of the principle of meaningful human control over decisions to use lethal force. This principle does not equate to direct manual control over every function of the weapon system, but assumes that critical decisions

regarding target selection and authorization of attack remain the exclusive prerogative of human judgment.

CONCLUSION

The analysis of the interaction between emerging military technologies and international humanitarian law allows us to validate the hypothesis from which we started this study. The data examined confirm that emerging military technologies (lethal autonomous systems, offensive cyber capabilities and unmanned aerial platforms) indeed create a significant normative vacuum in international humanitarian law. This vacuum is manifested not so much by the total absence of applicable norms, but by the inadequacy of existing legal instruments for the effective and uniform application of the fundamental principles of IHL to the specific characteristics of these technologies.

The traditional principles of distinction, proportionality and precaution in attack, while remaining valid as conceptual foundations of IHL, were indeed conceived in the context of conventional conflicts in which the human operator maintains direct and continuous control over the weapon and can directly observe the effects of his actions. The decision-making autonomy of artificial systems disrupts this direct relationship between the operator and the effects of the use of the weapon, creating uncertainties about when and how IHL principles should be applied.

The hypothesis that these specific features require a substantive reinterpretation of IHL principles or even the development of new legal instruments is also validated by the analysis carried out. Reinterpretation alone, without normative complementation, proves insufficient to respond to the identified challenges. The current legal framework provides general principles that remain applicable, but the lack of specific rules on the definition of cyber-attacks, acceptable autonomy standards for lethal systems, mandatory Article 36 assessment procedures for new technologies, or mechanisms for attributing liability in the case of autonomous systems makes the practical application of these general principles inconsistent and uncertain.

The study thus highlights the need for a dual approach that combines the reinterpretation of existing principles through state doctrine and practice with the development of specific legal instruments that clarify the technical and procedural aspects of the use of new technologies. This dual approach should focus on clarifying fundamental concepts through precise legal definitions, establishing verifiable technical standards for assessing the compliance of autonomous systems with IHL, establishing mandatory and standardized procedures for reviewing new weapons under Article 36, and creating clear mechanisms for attributing legal responsibility in the case of the use of highly autonomous systems.

The analysis in this paper confirms the warnings of scholars such as Scharre (2024) on the moral and ethical risks of autonomous weapons, Heyns (2016) in his report as UN Special Rapporteur on legal accountability gaps, and the authors of the Tallinn Manual 2.0 (Schmitt, 2017) on the challenges of applying IHL in cyberspace. Although emerging technologies may, in principle, be compatible with the purposes of IHL aimed at protecting certain categories of persons and property, their uncontrolled use without an appropriate regulatory framework can have effects that seriously contravene the fundamental principles of this law. The RUSI (2024) study on the use of drones in Ukraine demonstrates that the tactical transformations generated by these technologies are already an operational reality, not a future speculation, which emphasizes the urgency of developing clear legal standards.

Future research should focus on developing verifiable and operational technical standards for assessing the compliance of autonomous systems with IHL, as well as on analysing the emerging jurisprudence of international courts on liability for the use of new military technologies. Only through such a comprehensive approach, which combines legal rigor with a deep understanding of technical realities, will it be possible to develop an effective normative framework that ensures respect for fundamental humanitarian values in armed conflicts of the future.

BIBLIOGRAPHY:

Trinquier, R. (1961). *La guerre moderne*. Éditions de la Table Ronde, Retrieved December 02, 2025, from https://francegenocidetutsi.org/TrinquierLaGuerreModerne.pdf.

Bouthoul, G. (1950). *Les guerres: Éléments de polémologie*. Payot.

Kelsen, H. (1944). Peace through law. *University of North Carolina Press.*

Scharre, Paul. (2024). *Four Battlegrounds: Power in the Age of Artificial Intelligence. New York: W.W. Norton & Company.*

U.S. Department of Defense. (2023). *Autonomy in weapon systems (DoD Directive 3000.09),* Retrieved December 28, 2025, from *https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf.*

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations* (2nd ed.). Cambridge University Press. https://doi.org/10.1017/9781316822524.

Heyns, C. (2016). *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions* (UN Doc. A/HRC/23/47). United Nations Human Rights Council.

Anderson, K., & Waxman, M. C. (2017). *Law and ethics for autonomous weapon systems: Why a ban won't work and how the laws of war can*. Stanford University, Hoover Institution.

The Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), adopted June 8, 1977, Retrieved December 03, 2025, from https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf

President of Romania. (2020). *National Defence Strategy 2020-2024: "Together, for a safe and prosperous Romania in a world marked by new challenges"*. Retrieved December 04, 2025, from https://www.presidency.ro/files/userfiles/National_Defence_Strategy_2020_2024.pdf.

U.S. Department of Defense, Office of General Counsel. (2023). *Department of Defense law of war manual*, Retrieved December 06, 2025, from https://www.defense.gov/News/Releases/Release/Article/3382481/dod-releases-updated-law-of-war-manual/.