Contemporary Readings in Law and Social Justice
ISSN: 1948-9137, e-ISSN: 2162-2752
Vol 17(01), 2025
pp. 550 - 562

Governance and Regulation of Autonomous Weapons and Cybersecurity (2016–2024): The Influence of States, International Organizations, and Civil Society on International Humanitarian Law

[1]Carlos Alberto Aponte García, [2]Hermes Emilio Martínez Barrios, [3]Alexander Romero-Sánchez, [4] María Stephania Aponte García [5] María del Pilar García Valdés

[1]Universidad del Valle - Unidad Central del Valle del Cauca, Colombia,

https://orcid.org/0000-0002-0039-1772

[2] Universidad Popular del Cesar - Unidad Central del Valle del Cauca, Colombia

https://orcid.org/0000-0002-6932-157X

[3] Unidad Central del Valle del Cauca, Colombia, https://orcid.org/0000-0003-1928-7315

[4] Unidad Central del Valle del Cauca, Colombia. https://orcid.org/0000-0003-2642-2896

[5] Unidad Central del Valle del Cauca, Colombia, https://orcid.org/0009-0002-9605-155X

ABSTRACT: Between 2016 and 2024, the rapid development of emerging military technologies, such as lethal autonomous weapons, artificial intelligence applied to warfare, and cyber warfare, has posed significant challenges to International Humanitarian Law (IHL). This article critically analyzes the influence of States, international organizations, and civil society in shaping the legal and ethical frameworks addressing these issues. Using a qualitative, hermeneutic approach, it examines global actors' discourses, principles, and regulatory proposals. The study identifies three key findings: (i) a critical normative gap concerning autonomous systems and cyberconflicts; (ii) the need to reframe the notion of meaningful human control as a substantive legal safeguard; and (iii) the reluctance of technologically advanced States to accept binding frameworks. The discussion highlights the role of civil society as a normative co-designer and proposes a more inclusive, anticipatory, and adaptive global governance. Finally, the article provides recommendations to strengthen multilateral spaces, define clear principles, and promote proactive, ethical, and effective regulation of emerging military technologies.

Keywords: Lethal autonomous weapons; international humanitarian law; military artificial intelligence; meaningful human control; cyber warfare; normative governance.

Received: 25 May 2025 **Received:** 30 May 2025 **Accepted:** 26 Jun 2025

1. Introduction

Between 2016 and 2024, the rapid technological advancements characteristic of the Fourth Industrial Revolution have fundamentally transformed the landscape of international law, particularly in relation to the regulation of new forms of military equipment and conflict (Ávila García, 2024; García Vázquez, 2021). In this context, autonomous weapons, artificial intelligence applied to military domains, and cyberwarfare have emerged as critical challenges to the global legal order, prompting a reconfiguration of existing regulatory frameworks and fueling intense international debate (Podar & Colijn, 2025; Scharre & Lamberth, 2022).

This situation has attracted the attention and intervention of state actors, international organizations, and civil society representatives, whose positions, interests, and capacities have shaped discussions around the

legitimacy, legality, and regulation of these disruptive technologies (Ávila García, 2024; Kolijn & Podar, 2025).

This article is guided by the following research question: What has been the influence of states, international organizations, and civil society in the debate on the regulation of autonomous weapons, artificial intelligence, and cyberwarfare between 2016 and 2024? In addressing this question, the study seeks to understand how nations, international institutions, and broader society have contributed to the construction of legal, ethical, and political narratives surrounding the use of emerging technologies in warfare, as well as to the development of norms aimed at regulating and mitigating the risks associated with these tools.

In this context, a widening gap becomes evident between the pace of military technological innovation and the capacity of international law to anticipate and regulate its implications. While innovations continue to advance in areas such as algorithmic autonomy, combat AI, and offensive cyber operations, existing legal frameworks remain grounded in principles designed for more traditional forms of conflict (Scharre & Lamberth, 2022). This regulatory disconnect creates a legal and ethical vacuum that heightens the risk of illegitimate uses of force, weakens accountability mechanisms, as illustrated by the "responsibility gap" related to lethal autonomous weapons, and challenges the relevance of core principles of International Humanitarian Law (Taylor, 2022; Human Rights Watch, 2015).

Moreover, there is growing consensus among scholars, NGOs, and diplomats regarding the urgent need to ensure meaningful human control over autonomous systems to prevent the dehumanized use of violence (Santini et al., 2021). Therefore, it is imperative to examine how key actors, states, international organizations, and civil society, have engaged in recent regulatory debates, not only to understand current dynamics of power and governance but also to identify viable pathways toward a more effective, legitimate, and adaptive normative architecture for addressing 21st-century challenges.

The specific objective of this article is to determine the influence of states, international organizations, and civil society in the debate on the regulation of autonomous weapons, artificial intelligence, and cyberwarfare between 2016 and 2024. Accordingly, the study focuses on identifying the discourses, diplomatic actions, legal decisions, and advocacy mechanisms developed by various international actors within multilateral forums, disarmament dialogues, negotiated processes, and academic and scientific debates.

2. Theoretical and Conceptual Framework

This study is structured around five core concepts that contextualize the analysis of emerging military technologies within the framework of contemporary international law. These concepts, International Humanitarian Law, Lethal Autonomous Weapon Systems, Cyberconflicts, Meaningful Human Control, and International Responsibility, provide the normative and analytical foundation for examining how legal frameworks are transforming in response to military technological autonomy.

First, International Humanitarian Law (IHL) comprises the set of rules governing the conduct of hostilities during armed conflict (Zurek, Kwik & van Engers, 2023). It is grounded in universal principles such as distinction, proportionality, military necessity, and precaution. The application of IHL to autonomous technologies presents new legal and operational challenges, particularly regarding the ability of non-human systems to comply with these principles.

Second, Lethal Autonomous Weapon Systems (LAWS) are devices designed to select and engage targets without direct human intervention. This capability raises fundamental questions about their compatibility with IHL and about the effective allocation of responsibility (Ardiansyah, 2025). Although their development continues to progress, there is still no binding legal regime specifically regulating these systems, which has led to intense international debate over whether prohibitions or restrictions should be established.

The third key concept is that of cyberconflicts and cyberwarfare, which involve the use of offensive digital

capabilities, often difficult to attribute, that can produce effects comparable to conventional force. As such, they introduce a new operational category in international law (Lin, 2012; Madubuike-Ekwe, 2021). The ambiguous nature of cyberspace, its dual civilian–military use, and the critical interconnection between civil and military infrastructures complicate the practical application of IHL, as they erode the principles of distinction and proportionality by blurring the line between military and civilian targets (Lin, 2012; Gisel, Rodenhaüser & Dörmann, 2020; Dörmann et al., 2021). Additionally, the lack of effective mechanisms for verification and attribution constitutes a significant obstacle to accountability and the establishment of credible legal boundaries under IHL (Lin, 2012; Shakarian et al., 2014).

Fourth, Meaningful Human Control (MHC) has been proposed as a minimum normative principle to ensure that decisions regarding the use of force remain under effective human supervision. This control extends beyond symbolic operator presence and entails situational awareness, contextual understanding, predictive capacity, informed decision-making, and traceability of responsibility (Kwik, 2022; Santoni de Sio & Van den Hoven, 2022). MHC aims to safeguard the ethical and legal judgment of humans from being displaced by opaque algorithms or lethal automation.

Finally, international responsibility represents one of the greatest normative challenges in the context of autonomous technologies. The classical doctrine of "responsible command" weakens in scenarios involving systems that do not fit into conventional military hierarchies or respond to direct human orders. This has led to proposals such as "electronic responsibility," which seeks to adapt accountability frameworks to contexts where human agency is mediated or diluted (Spadaro, 2022).

Bringing together these five concepts not only helps identify existing regulatory gaps but also outlines theoretical avenues that could guide the evolution of international law in the face of emerging military technologies.

3. Methodological Perspective

This study is grounded in a rational-idealist epistemology (Romero-Sánchez et al., 2025), which recognizes that legal and political knowledge regarding emerging technologies—such as autonomous weapons and cybersecurity, is constructed through reflective, interpretative, and normative processes. Rather than seeking an objective and universal truth, this approach prioritizes the understanding of the discourses, values, and power relations that shape International Humanitarian Law (IHL) within global governance contexts. As De Berríos and Briceño de Gómez (2009) argue, this epistemological stance views knowledge as a rational and idealist construction, wherein the cognizant subject plays an active role in interpreting social and legal realities.

Methodologically, the research aligns with the interpretive paradigm (Romero-Sánchez et al., 2024), which assumes that social and legal phenomena must be understood through the meanings and representations constructed by actors in a globalized world. A qualitative research approach provides key methodological tools to analyze the complexity of the phenomenon by interpreting discourses, documents, treaties, declarations, and specialized studies (Aponte-García et al., 2025). The hermeneutic method thus becomes central to uncovering the argumentative logic and ideological positions embedded in the perspectives of the various actors involved (Romero-Sánchez & Aponte-García, 2024).

The scope of the research is exploratory, as it examines still-developing phenomena such as the international regulation of autonomous weapons and cybersecurity, in order to identify patterns, legal gaps, relevant actors, and ethical-legal tensions (Salcedo et al., 2022). Rather than seeking to validate universal hypotheses, the study aims to generate situated knowledge that broadens the critical understanding of the challenges these technologies pose to IHL between 2016 and 2024.

The literature review or state-of-the-art analysis (Martínez et al., 2024) serves as the primary tool for data collection and analysis, focusing on high-quality academic literature and institutional documents published in recent years (Martínez et al., 2022; Romero-Sánchez et al., 2024). The review includes United Nations reports, declarations from the Convention on Certain Conventional Weapons (CCW), NATO statements, and official positions from countries such as the United States, Russia, China, France, and Germany, as well as

reports from organizations such as the International Committee of the Red Cross (ICRC), Human Rights Watch, Stop Killer Robots, and the Stockholm International Peace Research Institute (SIPRI). Additionally, the study draws on peer-reviewed academic publications, expert legal analyses, and research in international relations, technological ethics, and global security.

During the 2016–2024 period, a growing divide has emerged between major military powers and Global South countries, as well as between state-based and non-governmental organizations. While some nations have promoted self-regulation and responsible technological development, others advocate for the adoption of precautionary bans on lethal autonomous systems. International organizations such as the United Nations and NATO have historically supported dialogue and cooperation but face structural constraints in establishing binding agreements. At the same time, civil society has played a critical role in monitoring and denouncing the ethical and moral risks posed by autonomous weapons and cyberwarfare, advocating for the creation of preventive guidelines and effective, restrictive regulations (Aponte-García et al., 2025).

This text presents the framework through which the diverse and evolving roles of international actors will be examined in a period of profound technological and geopolitical transformation. Through the interpretive analysis of relevant sources (Victoria Ochoa et al., 2023), it seeks to contribute to a critical understanding of the tensions arising between technological advancement, global security, and the norms of international law, within a context of increasing uncertainty and rapid change.

4. **Discussion**

4.1 Regulation of Lethal Autonomous Weapon Systems (LAWS) and Meaningful Human Control

The progressive integration of digital technologies into contemporary warfare marks a structural shift in how military power is conceived and exercised, transforming both strategic planning and operational capabilities in armed conflict. From an analytical perspective, Michael C. Horowitz (2020) argues that the impact of emerging technologies, such as artificial intelligence (AI), unmanned aerial vehicles (drones), and cybersecurity systems, on international politics largely depends on the operational capacity of state and non-state actors to adopt and implement them effectively.

This observation highlights the uneven distribution of technological access, which can generate significant power asymmetries in the international system. However, Horowitz also notes that systematic study of these dynamics is hindered by persistent methodological limitations and a lack of sufficient empirical data, representing a major academic challenge in fully understanding how these tools reshape the contemporary battlefield.

Within this technological transformation, particularly controversial developments have emerged, such as Lethal Autonomous Weapon Systems (LAWS), which operate without direct human intervention and raise complex legal and ethical implications. Porcelli (2021) examines these systems through the lens of International Humanitarian Law (IHL) and concludes that their use raises serious concerns about compatibility with fundamental IHL principles, including distinction, proportionality, and individual responsibility.

His analysis reveals the absence of a clear legal consensus and exposes a troubling regulatory gap in the face of rapid technological advancement. Despite the gravity of these uncertainties, Porcelli dismisses the feasibility of a comprehensive preventive ban. Instead, he advocates for a more pragmatic regulatory approach, focused on strengthening the existing legal regime through the progressive interpretation and adaptation of current norms to meet the challenges posed by the automation of force.

In this regard, Frank Sauer (2020) emphasizes the urgent need to establish a multilateral regulatory regime for LAWS, through the implementation of legal and political standards that ensure the preservation of Meaningful Human Control (MHC) over decisions involving the use of force. From his perspective, MHC is not only essential for compliance with IHL but also for maintaining the moral and political legitimacy of deploying advanced military technologies.

While acknowledging the significant diplomatic, technical, and strategic challenges of reaching effective consensus, especially within the framework of the Convention on Certain Conventional Weapons (CCW), he insists that regulation cannot be indefinitely postponed. According to Sauer, urgency stems from the ethical, legal, and strategic risks associated with unrestricted autonomy in systems capable of making lethal decisions without direct human input. Within this context, MHC becomes a normative anchor for articulating minimum standards of accountability and democratic control over emerging weapon technologies.

However, the issue of human control becomes even more complex when considering agency in the process of selecting military targets. Danielsson and Ljungkvist (2020) propose a critical reinterpretation of human agency, suggesting it should be understood as a situated practice shaped by specific contexts, rather than as a universal or uniform capacity. Challenging traditional assumptions of operational rationality that underlie many military doctrines and technological designs, the authors argue that the human role in warfare cannot be reduced to a mechanical function of oversight or authorization.

Through empirical case analysis, they contend that human agency not only structures but can also disrupt and destabilize military practice, revealing a structural tension between automation processes and contextual human judgment. This tension indicates that, far from being a guaranteed source of legitimacy or effectiveness, human presence in decision-making loops must be critically examined based on operational, institutional, and ethical conditions.

In parallel, Jonathan Kwik (2022) makes a significant contribution to the MHC debate by proposing a pragmatic and structured approach to facilitate its operational implementation. By identifying five key dimensions, situational awareness, weapons development, contextual control, predictability, and accountability; Kwik offers a conceptual framework that breaks MHC into tangible and measurable components aimed at guiding decision-making in complex military environments.

This framework represents an effort to translate an ethical and normative principle into functional parameters that can be implemented by commanders and weapons system designers. Nonetheless, the author acknowledges that unresolved dilemmas remain, particularly concerning the responsibility gap. This gap emerges when, despite the presence of established procedures and controls, it becomes difficult to precisely determine who is accountable for the actions of an autonomous system operating with a degree of independence from direct human intent.

4.2 Ethical and Legal Tensions on Responsibility, Agency, and Governance

Alessandra Spadaro (2023) offers a critical examination of the traditional doctrine of command responsibility, a central concept in international criminal law used to assign liability for unlawful conduct committed by subordinates. Spadaro argues that this doctrine faces serious limitations when applied to contexts where actions are carried out by Autonomous Weapon Systems (AWS), which lack human agency and do not operate within conventional military hierarchies. As a result, the absence of a clear subordination link, along with the opacity of certain automated decision-making processes, undermines the effectiveness of this legal framework in establishing clear and enforceable accountability. Nevertheless, Spadaro does not reject the doctrine's usefulness; rather, she suggests that it can offer a valuable reference point for rethinking and redefining the boundaries of required human control, especially concerning predictability, oversight, and the governance of complex systems. Her analysis calls for an adaptive reinterpretation of international law, capable of addressing the normative challenges posed by increasing technological autonomy in the military domain.

A more radical theoretical approach is proposed by Mia Swart (2023), who argues for the development of a new concept of electronic responsibility in response to the challenges posed by the growing autonomy of weapon systems. Drawing an analogy with legal persons, entities that are granted legal capacity despite lacking human agency; Swart contends that it might be possible, at least on an exploratory basis, to consider the direct attribution of responsibility to autonomous agents.

This thesis, still in its early stages, openly challenges traditional normative frameworks of international criminal law, which are based on individual culpability and human intent. In doing so, Swart highlights the conceptual limitations of current law in dealing with phenomena where causality and intent are diffused across complex algorithmic systems. Her proposal not only represents an epistemological break from conventional legal categories but also calls for a fundamental reconfiguration of legal accountability in contexts where technology operates with increasing autonomy and unpredictability.

In parallel, the operational dimension of these systems has been explored empirically in asymmetric conflict scenarios. In this regard, Borg (2020), in his study of the warfare practices of the Israel Defense Forces (IDF), provides evidence of how unmanned aerial vehicles (UAVs) have transformed the contemporary paradigm of warfare. His research demonstrates that the combined use of UAVs for intelligence, surveillance, and reconnaissance (ISR) has significantly expanded tactical control capabilities, nearly eliminating military casualties on the deploying side.

However, while civilian casualties have decreased numerically, their impacts are temporally extended, resulting in prolonged suffering among affected populations. From a theoretical perspective grounded in actor-network theory, Borg conceptualizes drones as sociotechnical actors that interact with social structures and military tactics, illustrating how these technologies reshape not only combat capabilities but also the collective experience of conflict's consequences.

4.3 Cybersecurity, Cyberwarfare, and International Law

A particularly diffuse and complex domain in the configuration of contemporary military power is cyberspace. Roguski (2021) highlights the enormous challenges the international community faces in establishing an effective inspection and control regime over cyberweapons. Among the main obstacles, he points to the intangibility of these assets, their dual-use nature, both civilian and military, and the reluctance of states to subject their cyber capabilities to multilateral verification and regulatory mechanisms.

This combination not only prevents the level of transparency necessary for building trust among state actors but also complicates accountability in the event of attacks, given the ambiguous threshold between espionage, sabotage, and acts of war. Despite the existence of soft law frameworks, such as the United Nations' codes of conduct, these have proven insufficient to prevent the escalation of tensions in cyberspace. As a result, cyberspace continues to consolidate itself as a strategic theater characterized by opacity, legal fragmentation, and the absence of binding consensus.

On another front, Amoroso and Tamburrini (2021) critically examine the ethical dilemmas posed by Lethal Autonomous Weapon Systems (LAWS), emphasizing the tension between tactical efficiency and humanitarian principles. Their main objection is that these systems, by operating without direct human intervention in target selection, promote a dehumanization of warfare by removing moral judgment from life-and-death decisions.

This functional autonomy not only undermines individual responsibility but also raises essential questions regarding the moral legitimacy of using automated force. Nonetheless, the authors acknowledge that, from a strictly operational standpoint, LAWS may offer benefits such as reduced own-force casualties and greater tactical precision, part of what explains their appeal to certain armed forces. This duality, effective tactical tool vs. source of ethical concern (Aponte & Llano, 2022), reveals the profound ambivalence inherent in the integration of AI into military applications and calls for a critical, balanced assessment of the values guiding their design and use.

From a legal standpoint, Aravena Flores (2024) explores the compatibility of LAWS with the fundamental principles of International Humanitarian Law (IHL), particularly distinction, proportionality, and precaution. He argues that, in their current stage of development, these systems face serious limitations in meeting such normative standards, as algorithm-based decision-making does not sufficiently guarantee the

ability to distinguish between combatants and civilians or to proportionately assess collateral damage. Furthermore, the lack of transparency in system programming and training processes hinders external verification and accountability.

Given this context, Aravena Flores concludes that the only viable path for aligning technological advancement with international legal obligations is to ensure the effective and verifiable incorporation of meaningful human control at every stage of the use-of-force process. This condition would not only help safeguard IHL principles but also enhance the legal and moral legitimacy of employing emerging military technologies.

Lastly, Cotino Hueso and Gómez de Ágreda (2024) offer a comprehensive analysis of the ethical and legal criteria that should guide the design, development, and deployment of AI-based military systems. Their approach begins with the recognition that the defense sector's specificity, marked by high-stakes scenarios, dynamic operational contexts, and potentially irreversible consequences, demands a distinct and stricter regulatory framework than what is applied in civilian environments. Accordingly, the authors argue that any integration of AI into weapon systems must be grounded in solid principles that ensure technical reliability, algorithmic decision traceability, minimization of discriminatory bias, and effective human responsibility throughout the entire system life cycle, from design and testing to deployment and eventual deactivation.

They further warn that simply transposing civilian regulatory models to the military domain is unfeasible due to the unique characteristics of warfare-related technologies. These include the dual-use potential of many applications, their operational scalability, and the inherent risk of uncontrolled escalation in conflict scenarios. Therefore, they advocate for a specific ethical regulatory framework for the defense sector that integrates legal principles with technical and operational requirements tailored to military realities.

This perspective emphasizes the urgency of a preventive, cross-cutting approach that incorporates ethics from the earliest stages of technological innovation, rather than relegating it to a corrective role after deployment. In doing so, the authors help outline a governance model that recognizes the complexity of the relationship between AI and international security, one that aims to uphold human control not merely as a formal safeguard but as a substantive condition for the legitimate use of force.

5. Results

The evidence presented in this study confirms that International Humanitarian Law (IHL) faces unprecedented challenges due to the rapid integration of autonomous technologies, artificial intelligence, and cyber capabilities into modern conflict scenarios. Traditional regulation, based on principles such as distinction, proportionality, and responsibility, proves inadequate in the face of systems that operate with increasing levels of autonomy, thereby blurring the concept of individual human agency. In this regard, the article aligns with scholars such as Scharre and Lamberth (2022) and Taylor (2022) in identifying a "regulatory gap" between the pace of technological development and the ability of international law to anticipate and mitigate its associated risks.

A key contribution of this research is the critical integration of the concept of "Meaningful Human Control" (MHC) as a central axis of regulatory efforts. Unlike more formal approaches that reduce MHC to technical supervision, this study adopts a substantive perspective, inspired by Kwik (2022) and Santoni de Sio & Van den Hoven (2022), which includes dimensions such as contextual judgment, traceability, and accountability. This represents a normative advancement by redefining human control not merely as an operational validation mechanism but as an ontological condition for the legal and ethical legitimacy of force.

The article also contributes to the debate by questioning the applicability of classical doctrines such as "command responsibility," following Spadaro (2023), and proposes expanding the spectrum toward more flexible notions such as "distributed responsibility" or "electronic responsibility," which are still under development. This approach complements the pioneering work of Amoroso and Tamburrini (2021) and Swart (2023), who have also called for rethinking accountability frameworks in light of algorithmic opacity

and the functional autonomy of weapon systems.

In the field of cyberwarfare, the research confirms that the lack of verifiable attribution mechanisms and the absence of binding regulations create a highly precarious legal environment. Unlike technocratic positions that merely suggest adapting IHL principles to cyberspace (Lin, 2012), this study emphasizes that the ontological ambiguity of the digital environment demands new legal frameworks, developed through an adaptive governance logic rather than through normative transposition.

An additional contribution concerns the role of civil society and epistemic actors. While much of the literature highlights their role as whistleblowers or campaigners, this study argues that these actors must also be recognized as normative co-designers, capable of contributing conceptual frameworks, ethical criteria, and viable technical proposals.

Finally, the article makes a methodological contribution by adopting an interpretive approach that not only describes the positions of international actors but also interprets their ideological foundations and their impact on the construction of the global legal order (Aponte & Sánchez, 2024). This approach supports a deeper understanding of the discursive logics shaping international normativity in the context of the Fourth Industrial Revolution.

6. Conclusions

Emerging military technologies are radically transforming contemporary forms of warfare by blurring the boundaries between human and automated actions. The progressive integration of autonomous systems, artificial intelligence, and cyber capabilities into the military domain poses significant challenges that cannot be addressed from a single disciplinary perspective. On the contrary, a holistic approach is required, one that integrates political theory, international law, applied ethics, security studies, and technological analysis.

The need to establish robust and legitimate regulatory frameworks is inescapable. However, such frameworks cannot be built on inherited legal categories that prove insufficient in confronting the complexity of technological autonomy. Rethinking the concept of meaningful human control, reconsidering the nature of agency in automated environments, and redefining notions of responsibility and accountability are urgent tasks if we are to prevent the automation of military violence from eroding ethical and legal judgment in armed conflict. In this context, the international governance of military AI should not be viewed solely as a technical or strategic imperative, but as a matter of preserving the fundamental principles of international humanitarian law and human dignity in extreme situations.

Emerging military technologies are deeply altering warfare practices, gradually displacing human protagonism in decision-making processes related to the use of force. The deployment of lethal autonomous systems, AI in defense applications, and offensive cyber capabilities has produced structural transformations in how war is conceived, with far-reaching ethical, legal, and geopolitical implications. However, technological advancement has not been matched by equivalent normative evolution, resulting in a critical mismatch between innovation and legal governance.

One of the main obstacles to establishing a global normative framework for military AI use lies in the profound asymmetry of power between technologically advanced states and traditional norm-setting actors. While powers such as the United States, China, and Russia invest heavily in developing disruptive military technologies, international regulatory frameworks are constrained by a lack of political will and these states' resistance to accept limits that might compromise their strategic advantage. This structural inequality has generated a dynamic in which the most technologically dominant actors are also the least inclined to accept binding regulation, stalling the formation of solid legal consensus at the multilateral level.

In this context, the limitations of current multilateralism become apparent. Institutions like the United Nations and forums such as the Convention on Certain Conventional Weapons (CCW) have provided platforms to discuss guiding principles for the use of autonomous systems and other emerging technologies. However, the scope of their initiatives remains limited due to the voluntary nature of many

of their instruments and the absence of enforcement mechanisms. Furthermore, the CCW's consensus-based decision-making has allowed a minority of states to block substantive progress, perpetuating a normative stagnation that is increasingly dysfunctional in light of accelerating technological change.

Faced with this institutional gridlock, civil society has emerged as a key actor articulating ethical and humanitarian demands. Global campaigns such as "Stop Killer Robots" have raised public awareness about the dangers of unrestricted autonomy in the use of force and the urgent need for clear legal limits. Likewise, NGOs, academic experts, and interdisciplinary networks have enriched the debate with legal, technical, and philosophical arguments. Nevertheless, these efforts are often constrained by a lack of institutional support and by the difficulty of translating ethical activism into binding political commitments. The effective integration of civil society into multilateral processes still faces structural barriers that limit its influence.

Together, these factors have deepened a concerning gap between technological innovation and normative development. The period between 2016 and 2024 has witnessed an exponential acceleration in the research and deployment of emerging military technologies. However, this evolution has not been accompanied by the creation of an adequate legal regime to channel their use within the framework of international humanitarian law. As a result, a legal and ethical vacuum has emerged, exposing both state and non-state actors to a normative gray zone, with unpredictable implications for global stability and the protection of human rights in armed conflict.

In sum, the current landscape reveals a growing tension between the pace of technological development and the capacity of international law to regulate its impacts. Overcoming this tension requires a fundamental rethinking of traditional conceptual frameworks and the construction of a more inclusive, effective, and adaptive international governance model. Only then can emerging technologies be developed and used responsibly, in accordance with the core principles of humanity and international law.

7. Recommendations

An integrated strategy to address the challenges posed by emerging military technologies requires a set of recommendations aimed at both strengthening global governance and promoting the ethical and responsible development of these capabilities.

First, it is essential to reinforce multilateral spaces for dialogue and negotiation, particularly within the framework of the Convention on Certain Conventional Weapons (CCW) and the United Nations system. This involves not only revitalizing existing institutional mechanisms but also ensuring the effective inclusion of Global South actors, civil society organizations, and epistemic communities with interdisciplinary approaches. The diversity of perspectives is key to building a legitimate global consensus that overcomes current regulatory fragmentation.

In light of the absence of clear legal criteria regarding the use of Lethal Autonomous Weapon Systems (LAWS), a global moratorium on their development, production, and operational deployment is proposed as a precautionary measure. Such a moratorium would allow time to develop regulatory frameworks that clearly define thresholds for legality, responsibility, and compliance with international humanitarian law. The precautionary principle should guide this process, thereby preventing the unrestricted use of autonomous technologies from resulting in systemic violations of fundamental rights and the principles of the law of armed conflict.

Complementarily, the construction of a specific and binding international regulatory framework is urgently needed to govern the military use of artificial intelligence. This regime should incorporate principles such as accountability, meaningful human oversight, algorithmic traceability, and transparency in both the design and operation of autonomous systems. These principles are fundamental to ensuring that decisions regarding the use of force remain under deliberate human control, upholding the minimum standards of international law. Clear regulation would also help reduce legal ambiguity, which currently benefits states with greater technological capabilities.

In this process, it is imperative to foster partnerships between states, academic institutions, non-governmental organizations, and international bodies to create shared technical and ethical standards. These multi-stakeholder alliances can facilitate the formation of operational consensus on the responsible development and deployment of military technologies, moving beyond the prevailing unilateral or exclusively military logic. Moreover, collaboration across sectors would enable better articulation between technical expertise, legal analysis, and social demands for a more humanized and controlled approach to defense.

Lastly, there is a pressing need to promote interdisciplinary research in key areas such as cyberwarfare, autonomous weapons systems, and the ethics of artificial intelligence. An anticipatory and preventive approach is essential to identify emerging risks and build strong regulatory capacities before these technologies become entrenched in real-world conflict scenarios. Rigorous academic production, grounded in critical theory, empirical analysis, and normative debate, can significantly contribute to the formulation of evidence-based public policies aimed at protecting human life and upholding the international legal order.

8. Future Research Directions and Limitations

This study provides a foundational understanding of the complex regulatory, ethical, and legal challenges posed by emerging military technologies, particularly lethal autonomous weapon systems (LAWS), artificial intelligence, and cyber capabilities. However, it also presents certain limitations that open the door for future lines of research. One of the primary limitations lies in the scope of the empirical data: while this article offers a comprehensive review of official documents, academic literature, and policy statements, it does not incorporate direct interviews or fieldwork with military personnel, policymakers, or AI system designers. Future studies could address this by adopting qualitative methodologies that gather firsthand insights into the practical implementation of emerging technologies in military contexts.

Another limitation is the focus on normative analysis, which, while crucial, may benefit from being complemented by more quantitative or data-driven approaches. For instance, future research could use network analysis or discourse analytics to map the positions of states and civil society actors in multilateral forums like the CCW. This would allow scholars to identify patterns of resistance or cooperation and better understand how influence and normative change are distributed across the global system.

A particularly fertile line of inquiry involves the development of legal frameworks capable of integrating technical principles such as algorithmic transparency, accountability, and meaningful human control. Interdisciplinary collaboration between legal scholars, AI engineers, and ethicists will be essential to operationalize these concepts into enforceable norms. Similarly, more research is needed on the operational dynamics of human–machine interaction in warfare, particularly concerning cognitive load, trust calibration, and decision-making under uncertainty in high-stakes environments.

Another critical area involves the role of the Global South in shaping international AI governance. While much of the literature centers on technologically advanced states, there is limited analysis of how less-developed countries engage with, resist, or propose alternatives to dominant regulatory models. South–South cooperation, regional initiatives, and counter-hegemonic discourses are emerging as important forces that merit systematic study.

Cyberwarfare and its regulation remain another key field with unresolved questions. The dual-use nature of cyber capabilities, their attribution challenges, and the blurred lines between espionage, sabotage, and acts of war call for tailored ethical and legal frameworks. Future work should explore how current norms can be adapted, or entirely reimagined, to address the unique features of cyber conflict.

Finally, further studies should investigate the proactive role of civil society in co-designing governance frameworks for military AI. Moving beyond advocacy, non-governmental organizations and epistemic communities increasingly contribute to the articulation of ethical standards, technical safeguards, and participatory models of decision-making. Understanding these contributions could illuminate more inclusive pathways to global norm development.

While this study lays the groundwork for a critical interpretation of emerging military technologies and their implications for international humanitarian law, much remains to be explored. Addressing these gaps will be essential for constructing a more equitable, accountable, and human-centered governance of warfare in the age of autonomy.

References

[1] Amoroso D, Tamburrini G. Hacia un modelo normativo de control humano significativo sobre sistemas de armas. Ética y Asuntos Internacionales. 2021;35(2):245-272. doi:10.1017/S0892679421000241

[2] Aponte García, C. A., Lozano Hurtado, A. M., Arcila Montoya, L. J., Muñoz González, L. C., & García Valdés, M. del P. (2024). Medical responsibility in the Colombian context: A review of negligence from the legal framework and ethical perspective. Evolutionary Studies in Imaginative Culture, 1884–1897. https://doi.org/10.70082/esiculture.vi.1603

[3] Aponte García, M. S., Llano Franco, J. V. (2022). Preceptos de la Justicia Transicional reconocidos por la jurisprudencia constitucional colombiana. Cuestiones Constitucionales, (47), 3-35. https://doi.org/10.22201/iij.24484881e.2022.47.17521

[4] Aponte García, M. S., Romero-Sánchez, A., Aponte García, C. A., García Valdés, M. del P., & Urriago Fontal, J. C. (2025). The impact of Revolution 4.0 on international law and arms regulation (2016–2024). Review of Contemporary Philosophy, 24(1), 280–288. https://doi.org/10.52783/rcp.1150

[5] Aponte, M. S., Llano, J. V., Sánchez, G. (2021). Perspectiva neoconstitucional y de sociología jurídica en el régimen disciplinario en Colombia. Verba Iuris (46),231–252. https://doi.org/10.18041/0121-3474/verbaiuris.2.8503

[6] Aponte, M., & Sanchez, S. (2024). Globalization, human rights and Colombian armed conflict. Migration Letters, 21(S5), 1237–1251.https://doi.org/10.59670/ml.v21iS6.8109

[7] Aponte-García, M. S., & Sánchez-Arteaga, S. (2024). Transitional Justice in Colombia: A Systematic Literature Review. Evolutionary Studies In Imaginative Culture, 8.2(S3), 500–531. https://doi.org/10.70082/esiculture.vi.1867

[8] Aravena Flores, M. A. (2024). Dilemas derivados del uso de sistemas autónomos de armas letales en el derecho internacional humanitario. Justicia, 29(45). https://doi.org/10.17081/just.29.45.7143

[9] Ardiansyah, M. (2025). Legal Framework on Autonomous Weapon Systems. Journal of Legal and Policy Horizons, 5(4), 122–134. https://doi.org/10.38035/jlph.v5i4.1575

[10] Autonomous Weapons: The Role of the Joint Criminal Enterprise Doctrine. University of Pittsburgh Law Review, 83(1). https://doi.org/10.5195/lawreview.2021.822

[11] Ávila García, I. L. (2024). Ciberseguridad y derecho internacional: El conflicto en el ciberespacio. Revista Derechos Humanos, Conflicto y Justicia, 3(6), 115–127. https://esdegrevistas.edu.co/index.php/rdcj/article/view/4946

[12] Borg, S. (2020). Armando la guerra israelí con drones: Vigilancia merodeadora y sostenibilidad operativa. Security Dialogue, 52 (5), 401-417. https://doi.org/10.1177/0967010620956796 (Trabajo original publicado en 2021)

[13] Cotino Hueso, L., y Gómez de Ágreda, Ángel. (2024). Criterios éticos y de derecho internacional humanitario en el uso de sistemas militares dotados de inteligencia artificial. Novum Jus, 18(1), 249–283. https://doi.org/10.14718/NovumJus.2024.18.1.9.

[14] Danielsson A, Ljungkvist K. (2023) A choking(?) engine of war: Human agency in military targeting reconsidered. Review of International Studies; 49(1):83-103. doi:10.1017/S0260210522000353

[15] De Berríos, O. G., & Briceño de Gómez, M. Y. (2009). Enfoques epistemológicos que orientan la investigación

de 4to. nivel. Visión Gerencial, (Edición Especial), 47–54. Universidad de los Andes. Recuperado de http://www.redalyc.org/articulo.oa?id=465545882009

[16] Dörmann, K., Gisel, L., & Rodenhaüser, T. (2021). Twenty years of IHL and the effects of cyber operations during armed conflicts. International Review of the Red Cross, 102(913), 287–314. doi:10.1017/S1816383120000387, https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/twenty-years-ihl-effects-of-cyber-operations-during-armed-conflicts-913.pdf

[17] García Vázquez, B. (2021). El derecho internacional frente a los nuevos medios y espacios en que desarrollar la guerra: La ciberguerra. Revista Chilena De Derecho Y Tecnología, 10(2), pp. 43–68. https://doi.org/10.5354/0719-2584.2021.57077

[18] Horowitz, M. C. (2020). Do Emerging Military Technologies Matter for International Politics. Annual Review of Political Science. Vol. 23:385-400. https://doi.org/10.1146/annurev-polisci-050718-032725

[19] Human Rights Watch. (2015). Mind the gap: The lack of accountability for killer robots. Human Rights Watch & Harvard Law School International Human Rights Clinic. https://www.hrw.org/report/2015/04/09/mind-gap/lack-accountability-killer-robots.

[20] Kwik, J. (2022). A Practicable Operationalisation of Meaningful Human Control. Laws, 11(3), 43. https://doi.org/10.3390/laws11030043

[21] Kwik, Jonathan. 2022. A Practicable Operationalisation of Meaningful Human Control. Laws 11:43. https://doi.org/10.3390/laws11030043.

[22] Lin H. (2012) Cyber conflict and international humanitarian law. International Review of the Red Cross.;94(886):515-531. doi:10.1017/S1816383112000811

[23] Llano Franco, J. V., & Aponte, M. S. (2024). Estado del Arte: Estudios de antropología y sociología jurídica en el Norte del Cauca. Revista Estudios Socio-Jurídicos, 26(2), 4.

[24] Madubuike-Ekwe, J. (2021). Cyberattack and the use of force in international law. Beijing Law Review, 12, 631–649. https://doi.org/10.4236/blr.2021.122034

[25] Martínez Barrios, H. E., Salcedo Mosquera, J. D., & Romero Sánchez, A. (2022). Observation as a research technique. (Reflections, types, recommendations and examples). Russian Law Journal, 10(4), 792–798. https://doi.org/10.52783/rlj.v10i4.4348

[26] Martínez, H. E., Pumarejo H. M., Montero M, J., & Monter, E. (2024). State of the art design: Reflections, meaning, objective, structure and example. Russian Law Journal, Vol. 12(1). https://doi.org/10.52783/rlj.v12i1.3931

[27] Podar, Heramb & Colijn, Alycia. (2025). Technical Risks of (Lethal) Autonomous Weapons Systems. https://doi.org/10.48550/arXiv.2502.10174

[28] Porcelli, A. M. (2021). La inteligencia artificial aplicada a la robótica en los conflictos armados. Debates sobre los sistemas de armas letales autónomas y la (in) suficiencia de los estándares del derecho internacional humanitario. Estudios Socio-Jurídicos, 23(1). https://doi.org/10.12804/revistas.urosario.edu.co/sociojuridicos/a.9269

[29] Roguski, P. (2021). An Inspection Regime for Cyber Weapons: A Challenge Too Far? AJIL Unbound, 115, 111–115. doi:10.1017/aju.2021.6

[30] Romero-Sánchez, A., & Aponte-García, M. S. (2024). The academic spin-off ecosystem: A comparative analysis between Colombia and global trends. Evolutionary Studies in Imaginative Culture, 1538–1563. https://doi.org/10.70082/esiculture.vi.2000

[31] Romero-Sánchez, A., Perdomo-Charry, G. & Burbano-Vallejo, E. (2024). From Academic Entrepreneurship to the Performance of Academic Spin-Offs: A systematic Review of the International Gap and the Colombian Context. Review of Contemporary 147 Philosophy. ISSN: 1841-5261, e-ISSN: 2471-089X

https://doi.org/10.52783/rcp.107

[32] Romero-Sánchez, A., Perdomo-Charry, G., & Burbano-Vallejo, E. L. (2025). Factores determinantes en la creación de Spin-Off Académicas: Una perspectiva multiteórica. Revista De Ciencias Sociales, 31(1), 162–181. https://doi.org/10.31876/rcs.v31i1.43496

[33] Romero-Sánchez, A., Perdomo-Charry, G., & Burbano-Vallejo, E. L. (2024). Academic spin-offs through the lens of pragmatism and mixed methods. Evolutionary Studies in Imaginative Culture, 8.1(S-2), 30-67. https://doi.org/10.70082/esiculture.vi.951

[34] Romero-Sánchez, A., Perdomo-Charry, G., & Burbano-Vallejo, E. L. (2024). Políticas, transferencia y financiamiento: factores clave para Spin offs académicas: Revisión Sistemática de Literatura. Revista Venezolana De Gerencia, 29(12), 1330-1346. https://doi.org/10.52080/rvgluz.29.e12.27

[35] Salcedo, J., Martínez, H., Urriago, J. y Romero, A. (2022). The theoretical framework in research: meaning, functions, structure and example for its design. Russian Law Journal, 10, 877-884. https://doi.org/10.52783/rlj.v10i4.4450

[36] Santini, A., et al. (2021). Toward a Normative Model of Meaningful Human Control over Weapons Systems. Ethics & International Affairs, 35(2), 245–272. https://doi.org/10.1017/S0892679421000241

[37] Santoni de Sio, F., & Van den Hoven, J. (2022). Meaningful Human Control and the Principle of Accountability. Science and Engineering Ethics, 28(1), 6. https://doi.org/10.3389/frobt.2018.00015

[38] Sauer, F. (2020). Stepping back from the brink: Why multilateral regulation of autonomy in weapons systems is difficult, yet imperative and feasible. International Review of the Red Cross, 102(913), 235–259. doi:10.1017/S1816383120000466

[39] Scharre, P., & Lamberth, M. (2022). Artificial Intelligence and Arms Control. Center for a New American Security. https://doi.org/10.48550/arXiv.2211.00065

[40] Shakarian, P., Simari, G. I., Moores, G., Parsons, S., & Falappa, M. A. (2014). An argumentation-based framework to address the attribution problem in cyber-warfare. arXiv. https://doi.org/10.48550/arXiv.1404.6699

[41] Spadaro, A. (2023). A Weapon is No Subordinate: Autonomous Weapon Systems and the Scope of Superior Responsibility. Journal of International Criminal Justice, Volume 21, Issue 5, November 2023, Pages 1119–1136. https://doi.org/10.1093/jicj/mqad025

[42] Swart, M. (2023). Constructing "Electronic Liability" for International Crimes: Transcending the Individual in International Criminal Law. German Law Journal, 24(3), 589–602. doi:10.1017/glj.2023.28

[43] Taylor Smith, P. (2022). Resolving responsibility gaps for lethal autonomous weapon systems. Frontiers in Big Data. https://doi.org/10.3389/fdata.2022.1038507

[44] Victoria Ochoa, D., Aponte García, C., García Valdés, M., Aponte García, M., Romero Sánchez, A. (2023). Normative Statements and Correction Claim in the Logical Comprehension Domain. Migration Letters. 20, S9 (Nov. 2023), 653–666. DOI: https://doi.org/10.59670/ml.v20iS9.4835

[45] Winter, E. (2021). The Accountability of Software Developers for War Crimes Involving

[46] Zurek, K., Kwik, J., & van Engers, T. (2023). Legal Norms and Autonomous Systems in Warfare. Ethics and Information Technology, 25(3), 441–457. https://doi.org/10.1007/s10676-023-09682-1