Drones, Artificial Intelligence, Autonomous Weapons, and Cybersecurity in Armed Conflicts: A Systematic Review of the Legal, Political, and Security Debate

Aponte-Garcia, Maria Stephania[1], Arevalo-Robles, Gabriel Andrés[2], Alexander Romero-Sánchez[3]

[1] PhD Candidate in Law at the Universidad Libre de Colombia, Master's Degree in Constitutional Law, Lawyer. Full-time Lecturer at the Unidad Central del Valle del Cauca (UCEVA), Tuluá, Valle del Cauca, Colombia. ORCID: **https://orcid.org/0000-0003-2642-2896**.
[2] PhD in International Studies, University of the Basque Country / Euskal Herriko Unibertsitatea (UPV/EHU). Official Master's Degree in International Studies (UPV/EHU). Master's Degree in Decentralized International Cooperation (UPV/EHU). Lawyer, Universidad Libre. Sociologist, Universidad Nacional. Currently serves as National Director of Research at Universidad Libre. ORCID: https://orcid.org/0000-0002-4389-5997.
[3] PhD in Business Administration at Universidad San Buenaventura, Cali, Colombia. Master's Degree in Economics, Management, and Business Administration from the Università degli Studi di Salerno. Business Administrator. Vice-Rector for Research and Social Outreach and Full-time Lecturer at the Unidad Central del Valle del Cauca, Tuluá, Valle del Cauca, Colombia. ORCID: https://orcid.org/0000-0003-1928-7315.

Abstract:
The increasing incorporation of drones, artificial intelligence (AI), autonomous weapons, and cyber capabilities into armed conflicts is reshaping practices of organized violence and expanding legal, political, and security controversies surrounding the use of force. This article examines the evolution of this debate and addresses the following question: how has the legal, political, and security discussion surrounding these technologies in armed conflicts changed? A systematic literature review complemented by bibliometric analysis was conducted. The search was carried out in Web of Science (SSCI), and the selection followed the PRISMA guidelines, with explicit inclusion and exclusion criteria. The 2020–2025 period yielded a corpus of 33 articles, which was analyzed through journal mapping, topic–author–country relationships, thematic evolution, and lexical comparison. The methodology combines quantitative and bibliometric analyses supported by tools such as Biblioshiny and Posit PBC™. The results show a shift from questioning the applicability of international law toward the operationalization of International Humanitarian Law (IHL) under conditions of distance, automation, and accelerated decision-making. In the case of drones, the focus moves from "precision" to institutional opacity, accountability, and proliferation. Regarding AI and autonomous weapons, the debate centers on decision-making agency, meaningful human control, and responsibility frameworks. In cybersecurity, disputes predominantly concern the notion of "attack," attribution, and escalation risks, with increasing relevance of the temporal dimension. It is concluded that the prevailing regulatory response tends to re-operationalize IHL through standards, progressive clarification of obligations, and incremental international stabilization mechanisms.

Keywords: armed drones, artificial intelligence, lethal autonomous weapons, cybersecurity, international humanitarian law.

1. INTRODUCTION

The technological transformation of contemporary armed conflicts has intensified the incorporation of unmanned systems, cyber capabilities, and algorithmic tools into critical functions such as surveillance, target identification, and the conduct of hostilities (Winter, 2021). The deployment of armed drones, the integration of artificial intelligence into intelligence and targeting processes (Rogers, 2023), the expansion of operations in cyberspace, and the development of systems with varying degrees of autonomy have reconfigured the way organized violence is exercised and have shifted the debate from a strictly operational plane toward legal, political, and strategic controversies. This technological convergence strains core categories of International Humanitarian Law (IHL) and, at the same time, alters the political incentives associated with decisions to use force and with accountability, with direct implications for international stability and the protection of the civilian population (Borg, 2021).

The legal and security literature has shown that the challenge lies not solely in the emergence of new means, but in the reconfiguration of the methods through which the use of force is planned, executed, and assessed. Operational distance, the automation of functions previously reserved to human judgment, and the acceleration of decision-making cycles alter the manner in which the guiding principles of IHL are implemented (Aravena Flores, 2024). The distinction between military objectives and civilian objects, proportionality between military advantage and incidental harm, and the obligation to take feasible precautions face additional difficulties when effects occur in opaque, distributed, or algorithmically mediated environments. Added to this is the fact that these technologies may broaden the spectrum of legally relevant harm by affecting critical infrastructure and essential services, or by generating losses of functionality without immediate physical destruction (Schmitt, 2022), thereby complicating the legal assessment of certain effects.

The political dimension of this phenomenon is equally central. Remote warfare, automation, and the use of cyber capabilities tend to alter the domestic and diplomatic costs of employing force, at times fostering practices of institutional secrecy, legitimizing narratives based on technological precision, and disputes over transparency and responsibility (Gould & Stel, 2022). The combination of technical capabilities and strategic decisions influences how attacks are justified, how they are publicly communicated, and how the resulting harm is investigated, particularly when operations take place in grey zones between active hostilities, security operations, and contexts of interstate competition (Schmitt, 2022). At this juncture, contemporary debate shifts from the question of the mere applicability of international law toward that of its effective operability and its capacity to structure institutional incentives for compliance.

In the field of international security, the proliferation of capabilities, including their appropriation by non-state actors, expands escalation risks, diversifies threat profiles, and increases systemic vulnerabilities. Drones, for example, have ceased to be exclusively high-cost strategic platforms and have also become mass-deployed tactical tools, susceptible to rapid adaptation and widespread battlefield use. Cyber operations, in turn, introduce uncertainty regarding attribution, intent, and relevant thresholds, thereby increasing the risk of miscalculation and disproportionate responses, especially when integrated with kinetic operations in hybrid campaigns (Mutschler et al., 2024). In parallel, the incorporation of artificial intelligence into intelligence cycles and target selection raises questions about decision traceability and the possibility of "machine-speed" escalation, particularly when automatic or semi-automatic responses are designed (Rogers, 2023).

These dynamics cannot be understood merely as the sum of sectoral debates. Available bibliometric evidence suggests a field of research that has become simultaneously more specialized, through the consolidation of specific technological objects as analytical axes, and more politicized, through the growing number of approaches linking these technologies to surveillance, proliferation, legitimacy, and the governance of the use of force. The sustained centrality of categories such as law, security, and war coexists with the emergence and consolidation of thematic clusters structured around drones, artificial intelligence/autonomous weapons, and cyber operations (Enemark, 2020; Kunertova, 2023). At the same time, academic production displays patterns of authorial and geographical concentration that contribute to fixing dominant regulatory languages, standards, and analytical frameworks, thereby reinforcing the relevance of a systematic synthesis capable of identifying trends, tensions, and gaps.

Despite the sustained growth of publications on drones, artificial intelligence, autonomous weapons, and cybersecurity, the field presents two recurring limitations. On the one hand, thematic fragmentation persists, separating doctrinal debates (focused on IHL, attribution, and responsibility) from security-oriented approaches (centered on proliferation, escalation, and strategy). On the other hand, there is a lack of synthesis that, supported by systematic evidence, allows observation of how the debate has evolved over time, which conceptual cores organize it, and what shifts have occurred between predominantly legal-operational approaches and more political-institutional ones (Aponte et al., 2025; Horowitz, 2020; Ponta, 2021). This lack of integration hampers a robust diagnosis of the state of knowledge and limits the ability to ground regulatory proposals or governance frameworks in a clear empirical panorama of the debate's evolution.

In response to this need, the research is guided by the following question: RQ1: How has the legal, political, and security debate surrounding the use of drones, artificial intelligence, cybersecurity, and autonomous weapons in armed conflicts evolved? The answer is constructed through a systematic literature review complemented by bibliometric analysis, with the aim of critically synthesizing the field, identifying dominant axes, recognizing thematic shifts, and characterizing the intellectual architecture of recent research (Aponte-Garcia et al., 2025). This strategy is particularly pertinent in an emerging and rapidly evolving domain, where the density of publications and the diversity of approaches may obscure patterns of continuity, points of rupture, and areas of normative ambiguity. Methodologically, the study employs a systematic search strategy in Web of Science (SSCI) and a selection process in accordance with PRISMA, with explicit inclusion and exclusion criteria (Romero-Sánchez & Aponte-Garcia, 2024). On this corpus, bibliometric tools are applied to map publication outlets, thematic relationships, and evolutionary patterns of the debate, and this mapping is complemented by a qualitative reading of the selected articles in order to reconstruct arguments, positions, and controversies (Llano Franco et al., 2025). The study focuses on the 2020–2025 period and culminates in a set of 33 articles selected for substantive analysis, allowing the articulation of quantitative evidence on the structure of the field with a qualitative interpretation of its main lines of discussion.

The main contribution of this study lies in offering an integrated characterization of the debate across three levels of analysis: the conceptual evolution of legal dilemmas associated with the conduct of hostilities, attribution, and responsibility; the political dimension related to legitimacy, transparency, and institutional incentives surrounding the use of force; and the security dimension linked to proliferation, escalation, and governance (C. Aponte Garcia et al., 2025; M. S. Aponte Garcia et al., 2025). This approach seeks to demonstrate not only what is discussed regarding each technology, but also how the problems, languages, and priorities of the field have been reordered in recent years.

Structurally, the article is organized as follows: first, the methodological strategy and corpus selection procedure are presented; second, the results are set out, combining a bibliometric characterization of the field with a substantive synthesis organized by technological categories; finally, a discussion interprets the identified shifts and their implications for regulation and international stability, followed by conclusions that synthesize the findings and suggest avenues for future research.

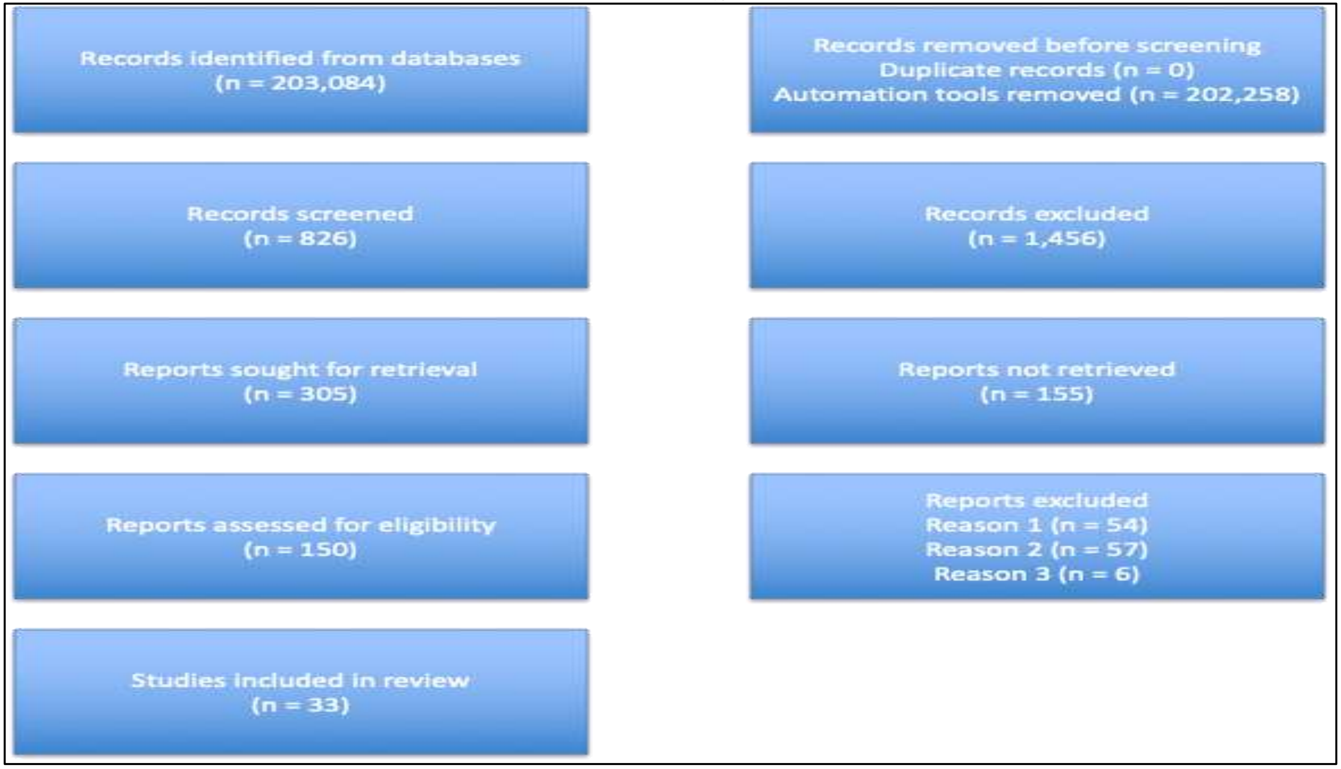
2. METHODOLOGICAL PERSPECTIVE

A systematic review of the legal and normative impact of new technologies on contemporary armed conflicts makes it possible to critically and comprehensively synthesize the current state of scientific knowledge in this field. This rigorous approach enables the structured evaluation of the literature, minimizing bias and ensuring reliable findings (Romero et al., 2024). The review is particularly relevant in emerging areas characterized by rapid technological change and growing academic production, such as the use of artificial intelligence, autonomous weapon systems, cyber warfare, and other digital technologies applied to the military domain, where significant theoretical, normative, and regulatory gaps persist.

The Web of Science database was used rather than combining multiple sources, as managing different interfaces and syntaxes can hinder efficient searching. There are disadvantages to using multiple databases, since searchers face complications when translating strategies across interfaces with different field codes and proximity operators (Glanville et al., 2019).

The search was conducted using a Boolean equation designed to capture the largest possible number of relevant studies in Clarivate Analytics' Web of Science Core Collection™ Citation Index: SSCI (Social Sciences Citation Index). In addition, the PRISMA methodology (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) was applied (see Figure 1).

Figure 1. PRISMA flow diagram and the steps involved in the identification of bibliographic data and the refinement of searches. Source: Adapted from Haddaway et al. (2020).


Records identified from databases
(n = 203,084)
Records removed before screening
Duplicate records (n = 0)
Automation tools removed (n = 202,258)
Records screened
(n = 826)
Records excluded
(n = 1,456)
Reports sought for retrieval
(n = 305)
Reports not retrieved
(n = 155)
Reports assessed for eligibility
(n = 150)
Reports excluded
Reason 1 (n = 54)
Reason 2 (n = 57)
Reason 3 (n = 6)
Studies included in review
(n = 33)

Source: Authors' own elaboration based on Romero et al. (2025).

The identification process constitutes the first critical step of the PRISMA methodology, aimed at ensuring a comprehensive and systematic search for all potentially relevant studies (Page et al., 2021). A systematic search was conducted in scientific databases using the Boolean equation: "drones" OR "artificial intelligence" OR "cybersecurity" OR "autonomous weapon" OR "digital warfare" OR "military technology" AND "armed conflict" OR "warfare" OR "military conflict" OR "violent conflict". An initial total of 203,084 results was obtained.

Using automation tools, open-access articles were excluded, reducing the results to 106,343 by eliminating 96,741 records. Subsequently, the results were limited to publications from the last five years (2020–2025), excluding 13,842 articles. Academic journal articles only were then retained, eliminating an additional 20,363 documents, which resulted in a total of 72,138 records. Finally, the Web of Science thematic category "Law" was applied, yielding 826 articles, with a total of 202,258 references excluded at the identification stage.

During the screening stage, the 826 selected articles were examined. A further screening by specific subject areas, including privacy, human–robot interaction, international criminal law, and Supreme Court, resulted in 305 articles selected and 521 records excluded. In addition, only documents published in English and Spanish were considered, eliminating 96 articles and leaving a total of 209 records. Lastly, the Web of Science meso-level subject areas were applied, excluding an additional 59 articles and resulting in a final set of 150 references selected for eligibility assessment.

Of the 150 publications assessed for eligibility, documents were excluded for three main reasons. First, 54 articles were excluded because they did not have a direct relationship with new technologies. Second, 57 articles were excluded because, although they addressed new technologies, they did not explicitly refer to their application in armed conflicts. Third, 6 articles were excluded because they discussed the regulation of new technologies without specifying their impact on armed conflicts. As a result, 33 articles were selected for the systematic literature review.

Our systematic review carefully adheres to the rigorous research protocol introduced by Donthu et al. (2021), emphasizing the importance of establishing clear inclusion and exclusion criteria.

Table 1. Criteria for the retrieval of documents included in our dataset.

Items	**Criterion**
Time horizon	2020-2025
DataBase	Clarivate Analytics' Web of Science Core Collection™
Citation index	SSCI (Social Sciences Citation Index)
Combination of keywords and Boolean operators / Search equation† :	"drones" (All Fields) OR "artificial intelligence" (All Fields) OR "cybersecurity" (All Fields) OR "autonomous weapon" (All Fields) OR "digital warfare" OR "military technology"(All Fields) AND "armed conflict"(All Fields) OR "warfare"(All Fields) OR "military conflict"(All Fields) OR "violent conflict" (All Fields) OR "Research funding" (All Fields)
Categorized by Web of Science categories	Law, privacy, human-robot interaction, international criminal law, y Supreme Court

Quick filters by Web of Science	Acceso abierto
Categorized by document type:	Solo artículos de investigación originales.
Software††:	VosViewer®; Gephi 0.10.1®; Posit PBC™, formerly known as RStudio. It is a rebranding that reflects the expansion toward Python and VS Code, as well as its web-based interface, Biblioshiny, the bibliometrics application.

Source: Modified from Borges et al. (2022).

Recognizing the importance of integrating technologies into research, we adopted an innovative methodology using Bibliometrix®, an open-source R package developed by Aria and Cuccurullo (2017). Its compatibility with key databases such as Web of Science, Scopus, and PubMed, as well as its ability to export data in multiple formats, position it as a valuable resource for researchers (Romero et al., 2024). Following the recommendations of Haddaway et al. (2020), the data were exported in BibTeX format through the Biblioshiny interface, ensuring content integrity for rigorous analysis and accurate academic evaluation (Aponte & Sánchez, 2024).

3. RESULTS

3.1. Historical Background: Remote Hostilities and the Legal Construction of the Military Objective

Historical analysis shows that contemporary debates on drones, autonomy, and cyber operations are embedded within a broader legal problem related to the conduct of hostilities at a distance. From the earliest attempts to regulate aerial warfare in the early twentieth century, International Humanitarian Law was compelled to adapt its categories to forms of violence that expanded the battlespace and reduced proximity between attacker and target (Borg, 2021; Germain, 2015). The 1923 Hague Rules, although lacking binding force, consolidated the shift toward the concept of the "military objective" as the central axis of legal analysis, which entailed a redefinition of the status of civilians and protected objects (Gould & Stel, 2022).

Nevertheless, critical scholarship demonstrates that this early adaptation of the law produced not only restrictive effects but also legitimizing ones. By operating with a narrow and functional notion of the civilian and by privileging the attacker's intent over the concrete effects of the attack, these legal categories facilitated the normalization of collateral damage and offered wide interpretive margins to justify aerial attacks (Salaymeh, 2021; Smith, 2022). This ambivalence between the limitation and the facilitation of violence constitutes a structural feature that reappears in contemporary debates on emerging military technologies (García, 2020).

3.2. Drones and Remote Warfare: Precision, Expansion of the Use of Force, and Accountability

In the contemporary context, the use of armed drones has reconfigured the legal and political debate by deepening the logic of remote warfare. From the perspective of IHL and international human rights law, drones have intensified discussions on the legality of targeted killings, the principle of necessity in the use of lethal force, and the obligation to allow surrender when there is no manifest military necessity (Enemark, 2020). The physical distance between the operator and the target raises additional questions regarding the proper application of the principles of distinction, proportionality, and precaution, as well as the traceability of the decisions that lead to the use of force (Leghari et al., 2020; Rogers, 2023).

At the political level, the use of drones has been defended as a tool capable of increasing the precision of attacks and reducing risks to one's own forces (Brenneke, 2020). However, this narrative coexists with critiques that warn of the banalization of recourse to force, the reduction of the political costs of violence, and the weakening of accountability mechanisms. From a security perspective, the proliferation of drones and precision-strike technologies has expanded the number of actors capable of exercising violence at a distance, including non-state armed groups, thereby transforming strategic dynamics and increasing risks to civilian populations (Kunertova, 2023).

3.3. Artificial Intelligence and Autonomous Weapons: Lethal Decision-Making, Agency, and Human Control

The development of systems based on artificial intelligence and, in particular, autonomous weapons introduces a qualitative shift in the legal debate by moving the focus from the time and place of the attack to the issue of decision-making agency (Kwik, 2022). Unlike drones, which remain under direct human control, autonomous systems raise questions about who makes the lethal decision and whether such a decision can comply with the normative standards of IHL (Klamberg, 2023). The literature converges on the absence of an international consensus regarding the definition and regulation of these systems, which has led to assessments of their lawfulness primarily through the principles of distinction, proportionality, and precaution (Aravena Flores, 2024).

The prevailing diagnosis holds that, at the current state of technology, autonomous systems lack the contextual judgment required to apply these principles adequately, due to the limitations of artificial intelligence in understanding complex environments, human intentions, and indeterminate legal values (Winter, 2021). However, alongside this critical position, an emerging line of argument maintains that such incompatibility is not necessarily permanent, and that future technological advances could enable more consistent evaluations less influenced by human factors such as fear or fatigue. At the political level, this divergence translates into a debate between the preventive prohibition of autonomous weapons and a gradual regulatory approach based on standards such as "meaningful human control" (Cotino Hueso & Gómez De Ágreda, 2024).

3.4. Cybersecurity and Armed Conflicts: Normative Interpretation, Attribution, and Instability

In the field of cybersecurity, the debate has followed a distinct yet convergent evolution. After an initial phase focused on affirming the applicability of international law to cyberspace, the discussion has shifted toward the concrete interpretation of existing norms (Ponta, 2021; Schmitt, 2022). Within the framework of IHL, the main points of friction concern the definition of an "attack," the identification of military and civilian objects in the digital environment, and the legal treatment of operations that do not produce immediate physical damage but generate significant effects on the functionality of essential infrastructure.

The difficulty of attributing cyber operations to specific actors also introduces an element of legal and strategic instability. The opacity inherent in cyberspace complicates the determination of responsibility and increases the risk of inadvertent escalation, particularly when cyber operations are integrated into hybrid military campaigns alongside kinetic means (Haataja, 2024). In this context, the literature highlights the need to clarify applicable legal thresholds and to avoid overly restrictive interpretations that could leave civilians and essential assets unprotected in highly digitalized societies (Eldem, 2021).

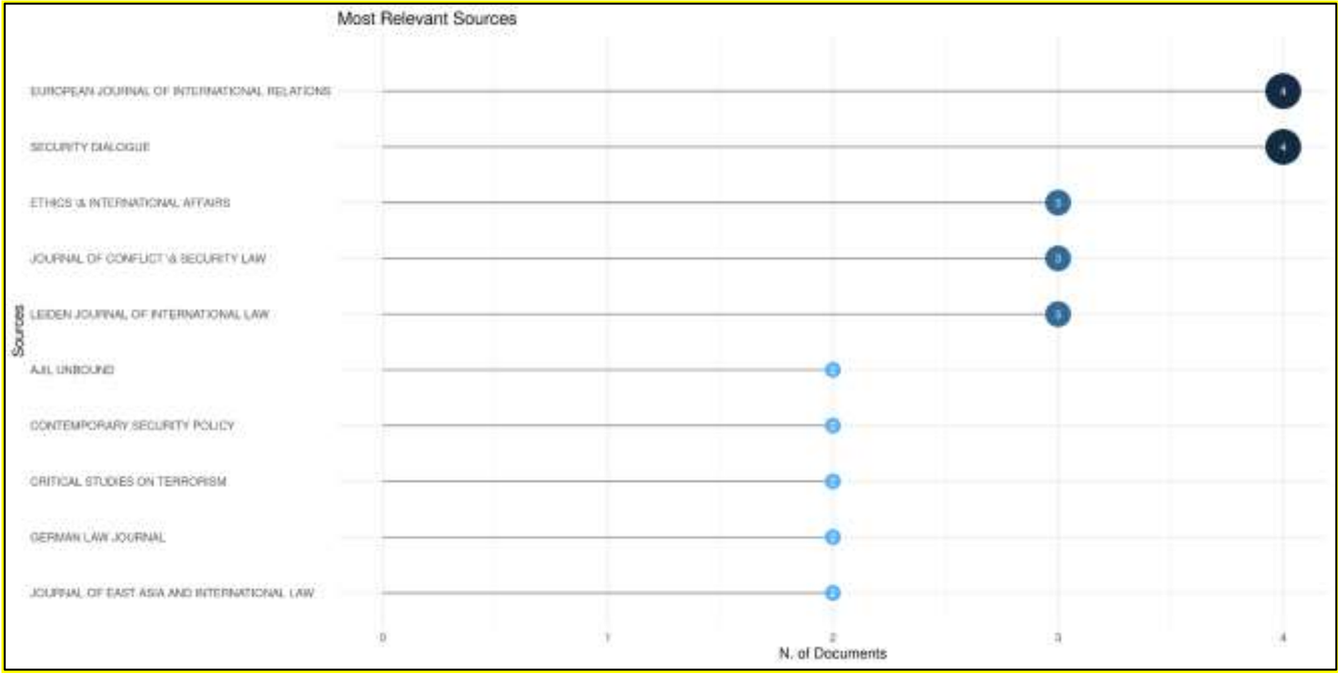
3.5. International Governance: Soft Law, Confidence-Building Measures, and Due Diligence

In light of the difficulty of reaching legally binding agreements in areas such as autonomous weapons and cybersecurity, the prevailing response of the international community has been the development of gradual governance mechanisms. These include non-binding norms, standards of responsible behavior, and transparency and confidence-building measures aimed at reducing the risk of misunderstandings and escalation. Regional initiatives, such as those promoted by the OSCE in the field of cybersecurity, illustrate this incremental approach, which prioritizes practical cooperation over the immediate codification of new norms (Copeland et al., 2023).

Within this framework, the principle of due diligence emerges as a key tool for structuring expectations of state conduct, even though its legally binding character remains the subject of debate. The literature suggests that the progressive consolidation of these practices contributes to generating stability and predictability in an environment characterized by rapid technological change and normative uncertainty (Aravena Flores, 2024; Ponta, 2021; Schmitt, 2022). Taken together, these findings show an evolution of the debate from attempts at substantive regulation toward forms of flexible governance aimed at managing the risks associated with the use of emerging military technologies.

3.1. Most Relevant Journals

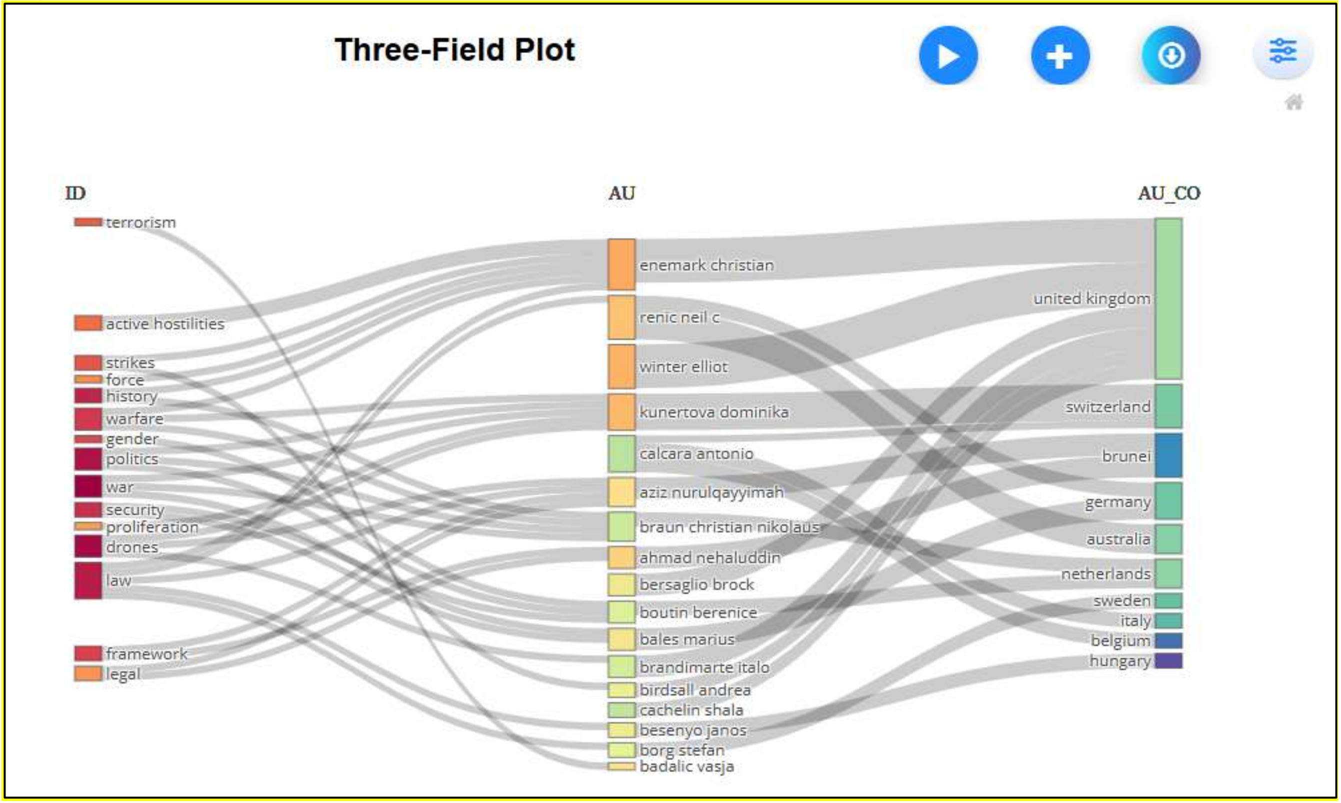
Figure 2. Most Relevant Journals



Authors' own elaboration based on bibliometric tools.

Based on the analysis of the most relevant journals in which academic production on drones, artificial intelligence, autonomous weapons, and cybersecurity is concentrated, it is evident that the debate is articulated in a clearly interdisciplinary manner, with a strong anchoring in both international law and critical security studies and international relations. The higher recurrence of publications in journals such as European Journal of International Relations and Security Dialogue (see Figure 2) indicates that these technologies are not approached solely as technical or normative issues, but as phenomena that transform the logics of war, sovereignty, and the international order, privileging theoretical and critical perspectives on power, violence, and technological change. At the same time, the prominent presence of specialized legal journals such as Leiden Journal of International Law and Journal of Conflict & Security Law (see Figure 2) reveals that the core of the debate remains normative, centered on the interpretation and adaptation of International Humanitarian Law and general international law to new modalities of the use of force. The inclusion of journals such as Ethics & International Affairs highlights the ethical dimension of the debate, particularly with respect to the delegation of lethal decisions to algorithmic systems and moral responsibility in contexts of remote and autonomous warfare. Likewise, the appearance of publications in venues such as AJIL Unbound, German Law Journal, and Contemporary Security Policy (see Figure 2) reflects a trend toward more flexible formats and open doctrinal debates, in which recent developments, state positions, and governance proposals are discussed, particularly in the areas of cybersecurity and soft law. Taken together, this distribution shows that the academic debate has evolved from predominantly doctrinal approaches toward a broader dialogue between law, politics, and security, in which emerging military technologies are analyzed as structural factors that reconfigure legal norms, strategic practices, and the legitimacy frameworks governing the use of force in contemporary armed conflicts.

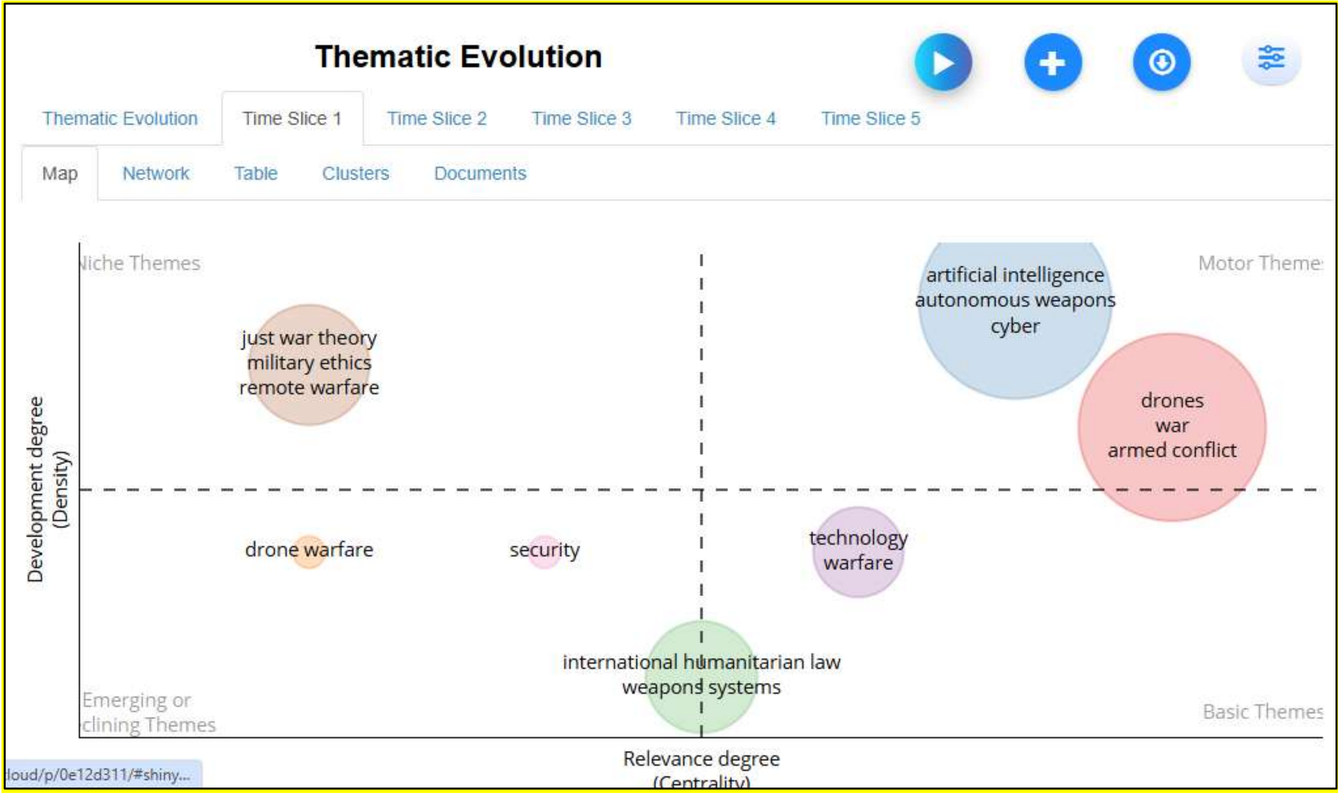
Figure 3. Three-Field Plot



Authors' own elaboration based on bibliometric tools.

The analysis of the three-field plot (see Figure 3), which links thematic areas, authorship, and national affiliation, makes it possible to identify structural patterns in academic production on drones, artificial intelligence, autonomous weapons, and cybersecurity in armed conflicts. The thematic distribution shows a concentration around notions such as law, security, war, drones, proliferation, and terrorism (see Figure 3), indicating that the debate is articulated at the intersection between normative issues related to the use of force and strategic concerns linked to international security. These areas are consistently connected to a relatively limited set of recurring authors, suggesting the existence of specialized epistemic communities that have contributed in a sustained manner to the consolidation of the field, rather than a broad dispersion of approaches or isolated lines of research. Likewise, the geographic dimension of authorship reveals a marked concentration in European and Anglophone countries, with notable centrality of the United Kingdom and significant links to Germany, Switzerland, the Netherlands, and Australia, highlighting a structural asymmetry in the production of knowledge on these technologies. This configuration suggests that academic debates on the legal regulation and security implications of contemporary technological warfare are strongly anchored in national contexts where technological capabilities, active participation in international normative processes, and well-established academic traditions in international law and security studies converge. Taken together, the plot not only visualizes relationships among themes, authors, and countries, but also reveals a research field structured around dominant nodes that contribute to shaping the languages, priorities, and analytical frameworks through which the use of emerging military technologies in contemporary armed conflicts is problematized.

Figure 4. Thematic Evolution

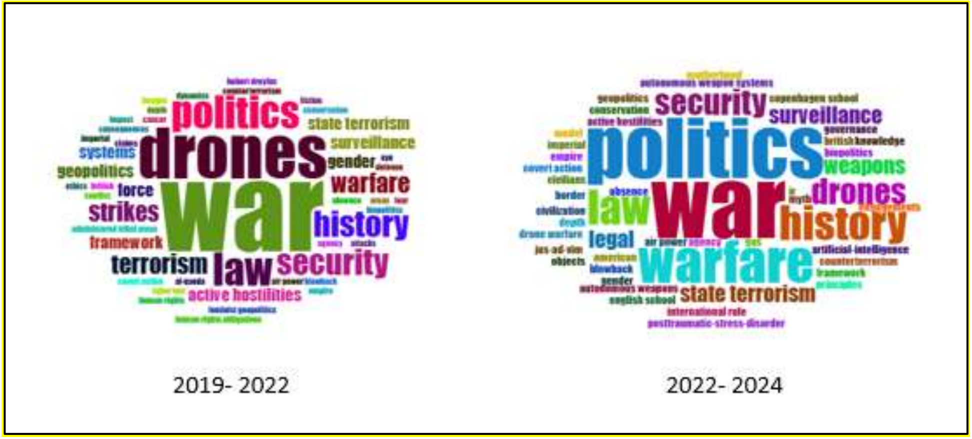


Authors' own elaboration based on bibliometric tools.

The analysis of thematic evolution makes it possible to observe a progressive transformation of the academic debate on the use of emerging military technologies in armed conflicts, both in terms of centrality and conceptual density. In the thematic map, highly developed and central motor themes can be identified, among which drones, war, and armed conflict stand out (see Figure 4), indicating that the use of drones has consolidated as a key organizing axis of the debate, closely linked to classical discussions on the conduct of hostilities and the use of force. In parallel, the clustering of artificial intelligence, autonomous weapons, and cyber (see Figure 4) emerges as another thematic core of high relevance and density, reflecting the growing academic attention to forms of warfare mediated by algorithms and digital systems, as well as the convergence between lethal autonomy and cyber operations. In contrast, areas such as international humanitarian law and weapons systems (see Figure 4) are positioned as basic themes, with high centrality but lower density, suggesting that, although they constitute the normative foundation of the field, their conceptual development depends on interaction with more specific debates on particular technologies. Likewise, the presence of technology and warfare in an intermediate position indicates a process of transition, in which the focus shifts from a general reflection on the technologization of war toward more specialized analyses.

Finally, niche themes such as just war theory, military ethics, and remote warfare (see Figure 4) display a high degree of internal development but lower centrality, highlighting their theoretical importance without structuring the overall debate. Taken together, this thematic evolution reveals a gradual shift from general normative and ethical approaches toward a debate more concentrated on specific technologies, drones, artificial intelligence, autonomous weapons, and cyber operations, which now function as central axes for problematizing the legality, legitimacy, and governance of contemporary armed violence.

Figure 5. Most relevant keywords in the study



Authors' own elaboration based on bibliometric tools.

The comparative analysis of the word clouds corresponding to the periods 2019–2022 and 2022–2024 makes it possible to identify significant shifts in the emphasis and orientation of the academic debate on emerging military technologies in armed conflicts. In the first period, the prominence of terms such as *war*, *drones*, *law*, *security*, *terrorism*, and *history* (see Figure 5) suggests an approach focused on situating drones within already consolidated legal and security-analytical frameworks, with particular attention to the legality of the use of force, counterterrorism operations, and the historical continuity of aerial warfare. This pattern indicates that the debate remained strongly anchored in discussions of existing practices and in the adaptation of International Humanitarian Law to relatively familiar—albeit technologically sophisticated—means of warfare.

By contrast, the second period reveals a reconfiguration of the semantic field, marked by a notable increase in the centrality of terms such as *politics*, *surveillance*, *weapons*, *armed conflict*, and *law* (see Figure 5). This shift reflects an expansion of the debate toward more explicitly political and structural dimensions of the use of these technologies. The greater visibility of *surveillance* and *weapons* points to growing concern about the systemic effects of technological surveillance, the proliferation of advanced military capabilities, and their implications for the governance of the use of force.

At the same time, the persistence of *war* and *law* as core conceptual anchors in both periods indicates normative continuity within the debate, even as the analytical focus gradually moves from the legality of specific tools toward broader questions of power, security, and the regulation of armed violence in contemporary conflict settings. Taken together, this lexical evolution suggests a transition from a predominantly legal-operational debate to a more politicized and interdisciplinary analysis, in which emerging military technologies are understood not merely as means of warfare, but as factors that reshape the dynamics of armed conflict and the frameworks of legitimacy governing the use of force.

The characterization of the field reveals an intellectual architecture shaped by the convergence between international law and security studies, with scholarly output concentrated in journals that function as spaces of dialogue between normative approaches and political–strategic frameworks. The relational structure linking themes, authors, and countries suggests a field organized around relatively stable nodes of specialization and a geography of knowledge production that is predominantly European and Anglophone, thereby contributing to the consolidation of dominant discourses on legality, the use of force, and technological governance.

The internal dynamics of the debate point to a transition from general frameworks—such as ethical approaches and broad discussions of remote warfare—toward the centrality of specific technologies.

In particular, drones and armed conflict emerge as a consolidated motor axis, while artificial intelligence, autonomous weapons, and cyber operations cluster as a second nucleus of high conceptual density, signalling the expansion of the debate toward forms of violence mediated by algorithms and digital infrastructures.

This reorientation is also reflected in the lexical shift observed across periods, which suggests a movement from a predominantly legal–operational discussion toward a more political and institutional problematization of the phenomenon, with greater emphasis on categories associated with surveillance, proliferation, and weapons systems. Analytically, these patterns describe a field that is becoming simultaneously more specialized and more politicized: specialized through the consolidation of concrete technological objects as central research foci, and politicized through the growing attention to the structural effects of these technologies on the legitimacy of the use of force, the protection of civilians, and international regulatory mechanisms.

4. DISCUSSIONS

From an evolutionary perspective, the results suggest that the legal, political, and security debate surrounding the use of drones, artificial intelligence, autonomous weapons, and cybersecurity in armed conflicts has experienced a progressive shift in its central axes. While early discussions focused primarily on the applicability and adequacy of International Humanitarian Law to new technological capabilities, contemporary debate increasingly revolves around structural issues related to the control of the use of force, the attribution of responsibility, and international stability in contexts characterized by distance, automation, and speed (Gaeta, 2024; Spadaro, 2024).

In the case of drones, this evolution is particularly evident. The initial debate, centered on precision and the supposed reduction of collateral damage, has given way to a broader problematization of remote warfare as a persistent form of violence at a distance (Pacholska, 2023). From a legal perspective, attention has shifted to the limits on the use of lethal force outside active hostilities, the interaction between IHL and international human rights law, and the practical challenges of ensuring accountability for civilian casualties (Kwik, 2022). Politically, the use of drones has been associated with practices of institutional secrecy and strategies to minimize political costs, contributing to an erosion of traditional mechanisms for democratic oversight of the use of force. From a security standpoint, the proliferation of drones (Kwik, 2022) and their adoption by non-state actors has transformed the dynamics of armed conflict, shifting the focus from high-end strategic platforms to ecosystems of widespread tactical use, with direct impacts on civilian protection.

The discussion on artificial intelligence and autonomous weapons represents a second key phase in this evolution of the debate. Here, the focus is no longer primarily on the physical distance between operator and target, but on the delegation of critical decision-making functions to algorithmic systems (King, 2024; Rogers, 2023). Legally, the debate has been redirected toward the compatibility of these systems with the principles of distinction, proportionality, and precaution, as well as the distribution of responsibility across complex chains that include design, training, deployment, and supervision. Politically, this discussion translates into a regulatory dilemma between proposals for preventive bans and gradual regulation approaches based on standards such as meaningful human control (McFarland, 2022). From a security perspective, the potential incorporation of autonomous systems in high-intensity contexts raises additional risks of escalation, particularly when decision-making speed exceeds human capacities for supervision and correction (Boutin, 2023).

A central element of the most recent debate is that the issue of artificial intelligence is not limited to lethal autonomy but extends to the use of algorithmic systems in intelligence processes, data analysis, and target selection (King, 2024; Klamberg, 2023). This broadening of the analytical focus represents a shift from individual weapons toward warfare methods based on data infrastructures and integrated command-and-control systems, further complicating the application of normative frameworks originally designed for discrete, human-centered, and temporally bounded decision-making (Renic, 2019).

In the realm of cybersecurity, the evolution of the debate shows significant parallels with the discussion on autonomy, particularly regarding speed and attribution. Following an initial phase focused on affirming the applicability of international law to cyberspace, attention has shifted to the concrete interpretation of concepts such as *attack*, *military object*, and *damage* (Brandimarte, 2023), as well as the challenges posed by attributing actions in a technically opaque environment (Eichensehr, 2022; Haataja, 2024; Martins, 2018). From an international security perspective, the potential for automated responses and cyber operations integrated into hybrid military campaigns introduces risks of inadvertent escalation and miscalculation, compressing decision times and reducing opportunities for human corrective intervention. In this sense, part of the contemporary debate is not only legal but also temporal, as existing norms presuppose decision windows that current technologies tend to shrink or eliminate.

In response to these transformations, the evolution of the debate reveals a gradual shift from seeking substantive normative solutions toward incremental governance approaches. In both autonomous weapons and cybersecurity, the difficulty of reaching legally binding consensus has fostered the development of nonbinding norms, responsible-conduct standards, and transparency and confidence-building mechanisms (Eslami, 2022; Khalymon et al., 2021; Mutschler et al., 2024). The principle of due diligence and regional initiatives aimed at preventing the misuse of state infrastructures exemplify this tendency to manage risk rather than eliminate it, through successive layers of regulation, cooperation, and shared expectations.

The evolution of the legal, political, and security debate on drones, artificial intelligence, autonomous weapons, and cybersecurity reveals a transition from discussions focused on the applicability of law toward deeper questions regarding how to maintain control, accountability, and legitimacy in the use of force within an environment characterized by distance (Besenyő & Málnássy, 2024; Horowitz, 2020; Pinheiro et al., 2020), automation, and accelerated decision-making processes. Far from replacing the framework of International Humanitarian Law, this evolution points to its re-operationalization through interpretive standards, the redistribution of responsibilities, and flexible governance mechanisms aimed at addressing the challenges posed by emerging military technologies in contemporary armed conflicts (see Table 2).

Table 2. Description of the Reviewed Articles

Title	Authors and Year	Main Findings
A Practicable Operationalisation of Meaningful Human Control	Jonathan Kwik (2022)	Proposes a Meaningful Human Control (MHC) framework with five key elements: situational awareness, weapon selection (weaponeering), context control, prediction, and accountability, aimed at closing the “responsibility gap” in the use of autonomous weapons.

Assembling Israeli drone warfare: Loitering surveillance and operational sustainability	Stefan Borg (2021)	Argues that the tactical use of drones for persistent surveillance (loitering) enables armed forces to control the tempo of the battle and achieve “operational sustainability” by spreading civilian casualties over time.
Criterios éticos y de DIH en el uso de sistemas militares dotados de IA	Lorenzo Cotino Hueso y Ángel Gómez de Ágreda (2024)	Emphasizes the need for human control throughout the entire lifecycle of military AI and highlights the difficulty of applying the "doctrine of double effect" to autonomous systems due to their intrinsic unpredictability.
Drones have boots: Learning from Russia’s war in Ukraine	Dominika Kunertova (2023)	Concludes that the war in Ukraine has shown that small, commercial drones have a greater tactical impact than larger ones, functioning as "expendable munitions" directly supporting infantry ("boots on the ground").
A Weapon is No Subordinate: AWS and the Scope of Superior Responsibility	Alessandra Spadaro (2023)	Argues that the doctrine of superior responsibility does not apply to machines, since autonomous weapons are objects, not subordinates, and lack the mental capacity (mens rea) to commit crimes.
Who Acts When Autonomous Weapons Strike?	Paola Gaeta (2023)	States that any “action” by a smart weapon is legally considered an act of the user (the commander or the state), making state responsibility indisputable, since the weapon functions solely as a tool..
Cyber operations and automatic hack backs under international law on necessity	Samuli Haataja (2024)	Analyzes the risks associated with “automatic hack backs,” warning that they may escalate conflicts at “machine speed” and generate unintended effects due to the complexity of interconnected systems.
Digital Targeting: Artificial Intelligence, Data, and Military Intelligence	Anthony King (2024)	Argues that the true revolution of artificial intelligence does not lie in lethal autonomous weapons, but rather in the use of Big Data processing to radically accelerate and enhance military target selection.
Dilemas derivados del uso de SAAL en el DIH	Marcos Antonio Aravena Flores (2024)	Argues that autonomous systems are incapable of complying with IHL principles of distinction, precaution, and proportionality, and therefore their use

		must be strictly constrained by human control.
Can IHL Regulate Recent Drone Strikes?: A Case Study	Nehaluddin Ahmad, Faizah Rahim y Nurulqayyimah Aziz (2024)	Examines recent attacks (Soleimani, Gaza, Ukraine) and highlights that the remote nature of drones complicates the distinction between combatants and civilians, demanding a more robust regulatory framework.
The enduring problem of 'grey' drone violence	Christian Enemark (2022)	Proposes that the persistent use of drone violence outside active battlefields constitutes a form of "quasi-imperialism," in which territory is controlled through the constant risk of violence without assuming responsibility for the welfare of the affected population.
Strategic ignorance and the legitimation of remote warfare: The Hawija bombardments	Lauren Gould y Nora Stel (2022)	Analyzes how states employ "strategic ignorance" and secrecy to evade accountability for civilian casualties in remote strikes, thereby sustaining the narrative that such warfare is "precise and risk-free."
Regulatory Choices at the Advent of Gig Warfare	Mark Klamberg (2023)	Explores the integration of artificial intelligence into platform-based command-and-control systems of the "Uber-type" (as observed in Ukraine) and argues that regulation should focus not only on the "means" of warfare (weapons), but also on the "methods" of warfare, including tactics and rules of engagement.
Requirement of Mens Rea for War Crimes in the Light of AWS	Xavier J. Ramírez García de León (2021)	States that the current framework of the International Criminal Court is ill-suited to prosecute crimes committed by autonomous weapon systems (AWS), as attributing intent requires excessive assumptions under existing law.
International Cybersecurity Norms and Responsible Cyber Sovereignty	Tuba Eldem (2021)	Describes the evolution of "responsible cyber sovereignty" at the UN, defining it as the obligation of states to ensure that their infrastructure is not used for international illicit acts through cyber proxies.

Battlefield Mercy: Supererogation in War	Neil C. Renic (2020)	Examines how the "remote intimacy" of drone operators affects their mental health, generating moral harm by preventing them from exercising acts of "mercy" that would go beyond their legal duty.
Breathless war: martial bodies, aerial experiences and the atmospheres of empire	Italo Brandimarte (2023)	Analyzes how aerial warfare and the use of technologies such as drones create "more-than-human" experiences that reinforce a racialized global order and imperial ambitions, where the air functions as both a technical and affective medium.
Do Emerging Military Technologies Matter for International Politics?	Michael C. Horowitz (2020)	Argues that drones can lower the threshold for conflict and the risk of political escalation, as leaders tend to respond less aggressively to the downing of a drone than to that of a manned aircraft.
Drones as Techno-legal Assemblages	Adam Smith (2022)	Proposes that drones function as "assemblages" combining technology and law to legitimize killing; digital surveillance transforms people into actionable data, enabling a "perpetual war" of constant suppression.
Drones, imagem-tempo e o fim do poder soberano	Ulysses Pinheiro (2020)	Argues that drone imagery represents an "eternal present" of waiting and threat; its "tactile" dimension (the operator touches what they see through the controls) reflects the totalizing immanence of power in late capitalism.
Geopolitical Dimension of Libyan Drone Warfare	János Besenyő y András Málnássy (2024)	Analyzes how the massive use of Turkish drones (Bayraktar TB2) in Libya allowed Turkey to project "hard power," neutralize traditional air superiority, and alter the regional balance of power.
International Humanitarian Law and the Conduct of Cyber Hostilities	Michael N. Schmitt (2022)	Discusses whether digital data should be considered "objects" protected under DIH and warns that the speed of cyber attacks may force automatic responses that increase the risk of human attribution errors.
Iran's Drone Supply to Russia and Changing Dynamics of the Ukraine War	Mohammad Eslami (2022)	Explain how the sale of Iranian loitering munitions (Shahed-136) has enabled Russia to mitigate its shortcomings in unmanned technology and attack

		strategic Ukrainian targets at a very low cost.
La inteligencia artificial aplicada a la robótica en los conflictos armados	Adriana Margarita Porcelli (2021)	It concludes that there is no international consensus to preventively ban SAAL; it advocates for a human-centered ethical framework that ensures the verifiability of decisions made by algorithms.
Legal instability in cyberspace and OSCE's mitigation role	Adina Ponta (2021)	Highlights the role of the OSCE in creating confidence-building measures for cyberspace and advocates the principle of "due diligence" to ensure that states prevent their infrastructure from being used in cross-border attacks.
Legal regulation of UAV application in the surveillance of the state border of Ukraine	Serhii Khalymon et al. (2021)	Evaluates the use of drones for border surveillance in Ukraine, proposing legal reforms to allow automatic recordings to be admitted as official evidence in criminal proceedings without infringing on the right to privacy.
Lethal Autonomous Weapon Systems and Their Compatibility with IHL	Matthias Brenneke (2020)	States that LAWS are currently incompatible with IHL because AI cannot make subjective proportionality judgments nor comprehend indeterminate legal concepts such as "excessive."
Minimum Levels of Human Intervention in Autonomous Attacks	Tim McFarland (2022)	Argues that IHL requires humans to retain sufficient information and capacity to correct system failures, given the inherent "fragility" of AI software in unexpected situations.
On the responsible use of armed drones: prospective moral responsibilities	Christian Enemark (2020)	Defines the responsible use of drones through five responsibilities: toward other states (sovereignty), their citizens (consent), intended victims, accidental victims, and own personnel (moral harm).
The impact of precision strike technology on the warfare of non-state armed groups	Mutschler, Bales y Meininghaus (2024)	It reveals how groups such as the Houthis and Daesh use precision drones to conduct a "liquid war," targeting distant strategic infrastructure and compensating for their lack of traditional territorial control.

5. CONCLUSIONS

The analysis conducted examined the evolution of the legal, political, and security debate regarding the use of drones, artificial intelligence, autonomous weapons, and cybersecurity in armed conflicts, combining a substantive review of the corpus with bibliometric evidence. The findings indicate that the debate has shifted from a focus on the applicability of international law and the adequacy of International Humanitarian Law (IHL) in the face of new capabilities toward a more structural concern with the effective conditions for controlling the use of force in environments characterized by operational distance, automation, and accelerated decision-making cycles.

Regarding drones, the findings show that the controversy is no longer organized solely around "precision" as a technological promise, but rather around the normative and political effects of remote warfare: the persistence of violence at a distance, institutional opacity, and challenges in ensuring accountability for civilian harm. The technological proliferation and expanded use of drones by diverse actors intensify these dilemmas, shifting the focus from exceptional platforms to widespread, tactical, and adaptive practices, with direct impacts on civilian protection and the governance of the use of force.

In relation to artificial intelligence and autonomous weapons, the analysis indicates a qualitative shift in the debate toward decision-making agency. The central question moves from merely assessing ex post compliance with IHL principles to ensuring ex ante that algorithmic systems performing critical functions—selection, prioritization, and potential engagement—operate under standards of distinction, proportionality, and precaution, while maintaining a legally attributable accountability architecture. Within this framework, the notion of meaningful human control has consolidated as a regulatory requirement aimed at translating legal obligations into verifiable and auditable procedures.

In cybersecurity, the results reflect a shift from broad consensus on the applicability of international law toward interpretive and operational controversies: defining an "attack," determining protected objects and relevant thresholds, attribution, and escalation risks. The temporal dimension acquires special significance: "machine speed" associated with automated responses and integrated operations reduces windows for human intervention, challenges traditional IHL assumptions, and increases the risk of unanticipated effects and miscalculations between states.

Bibliometric evidence supports that the field has become simultaneously more specialized and more politicized. The sustained centrality of categories such as law, security, and war combines with the consolidation of specific technologies as driving axes (drones; AI/autonomous weapons; cyber), while the recent lexical shift toward notions associated with surveillance, proliferation, and weapon systems reflects an expansion of the debate from the legality of specific means toward their structural effects on legitimacy, power, and governance. The concentration of authorship and geography further suggests that dominant frameworks emerge in specific institutional contexts, highlighting the need to understand these agendas as situated productions that also shape standard-setting processes.

The analysis also concludes that the predominant regulatory response does not seek to replace IHL but to re-operationalize it through incremental mechanisms: interpretive standards (such as meaningful human control), progressive clarification of obligations (including due diligence in cyberspace), and stabilization tools (transparency measures and confidence-building). In general terms, the central challenge lies not in the absence of norms but in the capacity to translate legal principles into institutional designs, technical procedures, and verifiable practices that preserve traceability, accountability, and civilian protection in scenarios where distance, automation, and speed tend to erode them.

Acknowledgment

This article is developed within the framework of the doctoral research project entitled: The Impact of the Fourth Industrial Revolution on International Law and Weapons Regulation: Technological Advances, Autonomous Weapons, Artificial Intelligence, and Cyber Warfare (2016–2024), as part of the academic requirements of the PhD in Law at the Universidad Libre de Colombia

6. REFERENCES

1. Aponte Garcia, C., Martinez, H., Aponte-Garcia, M., Romero-Sánchez, A., & Garcia Valdes, M. del P. (2025). Governance and Regulation of Autonomous Weapons and Cybersecurity (2016–2024): The Influence of States, International Organizations, and Civil Society on International Humanitarian Law. Contemporary Readings in Law and Social Justice. https://doi.org/10.52783/crlsj.537

2. Aponte Garcia, M. S., Romero, A., Aponte Garcia, >Carlos, Urriago, J. C., & Garcia Valdes. (2025). The Impact of Revolution 4.0 on International Law and Arms Regulation (2016-2024). Review of Contemporary Philosophy. https://doi.org/10.52783/rcp.1150

3. Aponte, M. S., Aponte, C. A., & Romero, A. (2020). Derecho internacional público, justicia global y modelos transicionales. En M. Aponte (Comp.), Derechos humanos, conflicto armado y construcción de paz (pp. 12-50). Uceva. https://repositorio.uceva.edu.co/bitstream/handle/20.500.12993/1942/Derechos-humanos-conflicto-construccion-paz. pdf?sequence=1 &isAllowed=y

4. Aponte, M. S., Aponte, C. A., & Romero, A. (2020). La reparación de las víctimas en el modelo de justicia transicional colombiano. En M. Aponte (Comp.), Derechos humanos, conflicto armado y construcción de paz (pp. 51-72). Uceva. https://repositorio.uceva.edu.co/bitstream/handle/20.500.12993/1942/Derechos-humanos-conflicto-construccion-paz. pdf?sequence=1&isAllowed=y

5. Aponte, M. S., Arevalo, G., & Romero, A. (2025). Evolution of the Industrial Revolutions and International Law: From mechanization to the regulatory challenges of the 4.0 Revolution. Contemporary Readings in Law and Social Justice. https://doi.org/10.52783/crlsj.612

6. Aponte-García, M. S., & Sánchez-Arteaga, S. (2024). Transitional justice in Colombia: A systematic literature review. Evolutionary Studies in Imaginative Culture, 500–531. https://doi.org/10.70082/esiculture.vi.1867

7. Aponte-Garcia, M. S., Arevalo_robles, G., & Romero-Sánchez, A. (2025). Advanced Technologies and Battlefield Transformation: A Legal and Ethical Reading of the Russia-Ukraine Conflict. Review of Contemporary Philosophy. https://doi.org/10.52783/rcp.1321

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. Aria M, Cuccurullo C. bibliometrix : An R-tool for comprehensive science mapping analysis. J Informetr 2017;11:959–75. https://doi.org/10.1016/j.joi.2017.08.007.

10. Besenyő, J., & Málnássy, A. (2024). Geopolitical Dimension of Libyan Drone Warfare: The Use of Turkish Drones on the North African Battlefields. Obrana a Strategie (Defence and Strategy), 24(1), 003–017. https://doi.org/10.3849/1802-7199.24.2024.01.003-017

11. Borg, S. (2021). Assembling Israeli drone warfare: Loitering surveillance and operational sustainability. Security Dialogue, 52(5), 401–417. https://doi.org/10.1177/0967010620956796

12. Boutin, B. (2023). State responsibility in relation to military applications of artificial intelligence. Leiden Journal of International Law, 36(1), 133–150. https://doi.org/10.1017/S0922156522000607

13. Brandimarte, I. (2023). Breathless war: Martial bodies, aerial experiences and the atmospheres of empire. European Journal of International Relations, 29(3), 525–552. https://doi.org/10.1177/13540661231153259

14. Brenneke, M. (2020). Lethal Autonomous Weapon Systems and Their Compatibility with International Humanitarian Law: A Primer on the Debate. In T. D. Gill, R. Geiß, H. Krieger, & C. Paulussen (Eds.), Yearbook of International Humanitarian Law, Volume 21 (2018) (Vol. 21, pp. 59–98). T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-343-6_3

15. Copeland, D., Liivoja, R., & Sanders, L. (2023). The Utility of Weapons Reviews in Addressing Concerns Raised by Autonomous Weapon Systems. Journal of Conflict and Security Law, 28(2), 285–316. https://doi.org/10.1093/jcsl/krac035

16. Cotino Hueso, L., & Gómez De Ágreda, Á. (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

17. Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. Journal of Business Research, 133, 285-296. https://doi.org/10.1016/j.jbusres.2021.04.070

18. Eichensehr, K. E. (2022). Ukraine, Cyberattacks, and the Lessons for International Law. AJIL Unbound, 116, 145–149. https://doi.org/10.1017/aju.2022.20

19. Eldem, T. (2021). Uluslararası Siber Güvenlik Normları ve Sorumlu Siber Egemenlik. İstanbul Hukuk Mecmuası, 79(1), 347. https://doi.org/10.26650/mecmua.2021.79.1.0010

20. Enemark, C. (2020). On the responsible use of armed drones: The prospective moral responsibilities of states. The International Journal of Human Rights, 24(6), 868–888. https://doi.org/10.1080/13642987.2019.1690464

21. Eslami, M. (2022). Iran's Drone Supply to Russia and Changing Dynamics of the Ukraine War. Journal for Peace and Nuclear Disarmament, 5(2), 507–518. https://doi.org/10.1080/25751654.2022.2149077

22. Gaeta, P. (2024). Who Acts When Autonomous Weapons Strike? Journal of International Criminal Justice, 21(5), 1033–1055. https://doi.org/10.1093/jicj/mqae001

23. Garcia, D. (2020). Disarmament in International Law. In D. Garcia, International Law. Oxford University Press. https://doi.org/10.1093/obo/9780199796953-0204

24. Germain, É. (2015). Out of sight, out of reach: Moral issues in the globalization of the battlefield. International Review of the Red Cross, 97(900), 1065–1097. https://doi.org/10.1017/S1816383116000461

25. Glanville, J., Foxlee, R., Wisniewski, S., Noel-Storr, A., Edwards, M. y Dooley, G. (2019). Traducción del filtro Cochrane EMBASE RCT desde la interfaz de Ovid a Embase.com: un estudio de caso. Revista de información y bibliotecas de salud . https://doi.org/10.1111/hir.12269 .

26. Gould, L., & Stel, N. (2022). Strategic ignorance and the legitimation of remote warfare: The Hawija bombardments. Security Dialogue, 53(1), 57–74. https://doi.org/10.1177/09670106211038801

27. Haataja, S. (2024). Cyber operations and automatic hack backs under international law on necessity. Computer Law & Security Review, 53, 105992. https://doi.org/10.1016/j.clsr.2024.105992

28. Haddaway NR, Page MJ, Pritchard CC, McGuinness LA. PRISMA2020 : An R package and Shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimised digital transparency and Open Synthesis. Campbell Systematic Reviews 2022;18. https://doi.org/10.1002/cl2.1230.

29. Horowitz, M. C. (2020). Do Emerging Military Technologies Matter for International Politics? Annual Review of Political Science, 23(1), 385–400. https://doi.org/10.1146/annurev-polisci-050718-032725

30. Khalymon, S., Hrynko, S., Zolka, V., Hrynko, R., & Volynets, N. (2021). Legal regulation of unmanned aerial vehicles application in the surveillance of the state border of Ukraine. Revista Amazonia Investiga, 10(40), 190–200. https://doi.org/10.34069/AI/2021.40.04.19

31. King, A. (2024). Digital Targeting: Artificial Intelligence, Data, and Military Intelligence. Journal of Global Security Studies, 9(2), ogae009. https://doi.org/10.1093/jogss/ogae009

32. Klamberg, M. (2023). Regulatory Choices at the Advent of Gig Warfare. Journal of International Humanitarian Legal Studies, 1–27. https://doi.org/10.1163/18781527-bja10088

33. Kunertova, D. (2023). Drones have boots: Learning from Russia's war in Ukraine. Contemporary Security Policy, 44(4), 576–591. https://doi.org/10.1080/13523260.2023.2262792

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

35. Leghari, F. A., Abbas, H., & Banbhan, A. A. (2020). Role of Diplomacy and Deterrence in Managing Pakistan-India Crisis: A Case Study of Post-Bombay Attacks Crisis. Global Regional Review, V(III), 230–237. https://doi.org/10.31703/grr.2020(V-III).23

36. Llano Franco, Aponte, M. S., & Romero-Sánchez, A. (2025). CONSTITUTIONS AND CITIZENS: EXCLUSION AND INCORPORATION IN 19TH-CENTURY LATIN AMERICA. International Journal of Applied Mathematics, 38(6s), 1350–1366. https://doi.org/10.12732/ijam.v38i6s.661

37. Martins, R. P. (2018). Punching Above Their Digital Weight: Why Iran is Developing Cyberwarfare Capabilities Far Beyond Expectations. International Journal of Cyber Warfare and Terrorism, 8(2), 32–46. https://doi.org/10.4018/IJCWT.2018040103

38. McFarland, T. (2022). Minimum Levels of Human Intervention in Autonomous Attacks. Journal of Conflict and Security Law, 27(3), 387–409. https://doi.org/10.1093/jcsl/krac021

39. Mutschler, M., Bales, M., & Meininghaus, E. (2024). The impact of precision strike technology on the warfare of non-state armed groups: Case studies on Daesh and the Houthis. Small Wars & Insurgencies, 35(7), 1123–1150. https://doi.org/10.1080/09592318.2024.2319216

40. Pacholska, M. (2023). Military Artificial Intelligence and the Principle of Distinction: A State Responsibility Perspective. Israel Law Review, 56(1), 3–23. https://doi.org/10.1017/S0021223722000188

41. Page, M., McKenzie, J., Bossuyt, P., Boutron, I., Hoffmann, T., Mulrow, C., Shamseer, L., Tetzlaff, J., Akl, E., Brennan, S., Chou, R., Glanville, J., Grimshaw, J., Hrõbjartsson, A., Lalu, M., Li, T., Loder, E., Mayo-Wilson, E., McDonald, S., McGuinness, L., Stewart, L., Thomas, J., Tricco, A., Welch, V., Whiting, P., & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews.. Journal of clinical epidemiology. https://doi.org/10.1016/j.jclinepi.2021.03.001.

42. Pinheiro, U., Almeida, L. M. C. D., & Lima, D. R. (2020). Drones, imagem-tempo e o fim do poder soberano. Trans/Form/Ação, 43(1), 213–244. https://doi.org/10.1590/0101-3173.2020.v43n1.12.p213

43. Ponta, A. (2021). Legal instability in cyberspace and OSCE's mitigation role. Juridical Tribune, 11(3). https://doi.org/10.24818/TBJ/2021/11/3.01

44. Renic, N. C. (2019). Battlefield Mercy: Unpacking the Nature and Significance of Supererogation in War. Ethics & International Affairs, 33(3), 343–362. https://doi.org/10.1017/S0892679419000364

45. Rogers, J. (2023). Rethinking remote warfare. International Politics, 60(4), 781–789. https://doi.org/10.1057/s41311-023-00449-5

46. Romero, A., Perdomo-Charry, G. and Burbano-Vallejo, E.L. (2024) 'Exploring the entrepreneurial landscape of university-industry collaboration on public university spin-off creation: A systematic literature review', Heliyon. https://doi.org/10.1016/j.heliyon.2024.e27258

47. Romero-Sánchez & Aponte-García. (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

48. Romero-Sánchez, A., Perdomo-Charry, G., & Burbano-Vallejo, E. L. (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 Philosophy, 23(1), 667-700. https://doi.org/10.52783/rcp.107

49. Salaymeh, L. (2021). Comparing Islamic and International Laws of War: Orthodoxy, "Heresy," and Secularization in the Category of Civilians. The American Journal of Comparative Law, 69(1), 136–167. https://doi.org/10.1093/ajcl/avab001

50. Schmitt, M. N. (2022). International Humanitarian Law and the Conduct of Cyber Hostilities: Quo Vadis? Journal of International Humanitarian Legal Studies, 13(2), 189–221. https://doi.org/10.1163/18781527-bja10059

51. Smith, A. (2022). Drones as Techno-legal Assemblages. Law, Technology and Humans, 4(1). https://doi.org/10.5204/lthj.2333

52. Spadaro, A. (2024). A Weapon is No Subordinate. Journal of International Criminal Justice, 21(5), 1119–1136. https://doi.org/10.1093/jicj/mqad025

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