



War without accountability. AI and the fragmentation of responsibility in contemporary warfare: power infrastructures and technological sovereignty

Guerra sin responsables. IA y la fragmentación de la responsabilidad en la guerra contemporánea: infraestructuras de poder y soberanía tecnológica

Virginia Contreras

Independent researcher.

Attorney, Specialist in Security and Defense. (United States)

vcontreras@oas.org

ORCID: 0009-0008-5141-9190

Resumen

The incorporation of artificial intelligence into security and defense domains has substantially transformed the nature of contemporary warfare, altering not only its operational capabilities but also one of its foundational pillars: the attribution of responsibility. In this new environment, military decisions no longer originate exclusively from clearly identifiable human agents but emerge from complex systems in which algorithms, data, technological infrastructures, state actors, and private companies interact. This article argues that the most profound impact of artificial intelligence in warfare does not lie solely in the automation of processes, but in the progressive fragmentation of responsibility, which complicates the identification of a single accountable subject for decisions and their consequences. In this sense, artificial intelligence does not merely introduce efficiency into military operations but rather produces a structural reconfiguration of responsibility through the fragmentation of the decision-making process, fundamentally altering how decisions and their consequences are attributed in armed conflict. Using an interdisciplinary approach, the article examines transformations in decision-making, the legal and ethical tensions arising from this phenomenon, and the strategic implications of increasing dependence on algorithmic systems. It introduces the notion of the “last human line” as a critical analytical point, representing the increasingly blurred boundary between human decision-making and automation, and highlights the need to rethink normative frameworks for a form of warfare in which responsible actors may be diffuse or virtually absent.

Key words: Iran, United States, Israel, Conflict, Artificial intelligence, Military Decision-Making

How to cite this work: Contreras, Virginia. (2026). War without accountability. AI and the fragmentation of responsibility in contemporary warfare: power infrastructures and technological sovereignty. *Cuadernos de RES PUBLICA en derecho y criminología*, (8), 01–32. <https://doi.org/10.46661/respublica.13315>

Recepción: 16.04.2026

Aceptación: 16.04.2026

Publicación: en prensa



Este trabajo se publica bajo una licencia de Creative Commons Reconocimiento-NoComercial 4.0 Internacional.



Guerra sin responsables. IA y la fragmentación de la responsabilidad en la guerra contemporánea: infraestructuras de poder y soberanía tecnológica

War without accountability. AI and the fragmentation of responsibility in contemporary warfare: power infrastructures and technological sovereignty

Virginia Contreras

Independent researcher.

Attorney, Specialist in Security and Defense. (United States)

vcontreras@oas.org

ORCID: 0009-0008-5141-9190

Abstract

La incorporación de la inteligencia artificial en los ámbitos de la seguridad y la defensa ha transformado sustancialmente la naturaleza de la guerra contemporánea, alterando no solo sus capacidades operativas, sino también uno de sus pilares fundamentales: la atribución de responsabilidad. En este nuevo entorno, las decisiones militares ya no se originan exclusivamente en agentes humanos claramente identificables, sino que surgen de sistemas complejos en los que interactúan algoritmos, datos, infraestructuras tecnológicas, actores estatales y empresas privadas. Este artículo sostiene que el impacto más profundo de la inteligencia artificial en la guerra no reside únicamente en la automatización de los procesos, sino en la fragmentación progresiva de la responsabilidad, lo que complica la identificación de un único sujeto responsable de las decisiones y sus consecuencias. En este sentido, la inteligencia artificial no se limita a introducir eficiencia en las operaciones militares, sino que produce una reconfiguración estructural de la responsabilidad a través de la fragmentación del proceso de toma de decisiones, alterando de manera fundamental cómo se atribuyen las decisiones y sus consecuencias en los conflictos armados. Mediante un enfoque interdisciplinario, el artículo examina las transformaciones en la toma de decisiones, las tensiones jurídicas y éticas que surgen de este fenómeno y las implicaciones estratégicas de la creciente dependencia de los sistemas algorítmicos. Introduce la noción de la «última línea humana», como punto analítico fundamental, que representa la frontera cada vez más difusa entre la toma de decisiones humana y la automatización, y destaca la necesidad de replantearse los marcos normativos para una forma de guerra en la que los actores responsables pueden ser difusos o estar prácticamente ausentes.

Palabras clave: Irán, Estados Unidos, Israel, conflicto, inteligencia artificial, toma de decisiones militares.

Cómo citar este trabajo: Contreras, Virginia. (2026). Guerra sin responsables. IA y la fragmentación de la responsabilidad en la guerra contemporánea: infraestructuras de poder y soberanía tecnológica. *Cuadernos de RES PUBLICA en derecho y criminología*, (8), 01–32. <https://doi.org/10.46661/respublica.13315>.

Recepción: 16.04.2026

Aceptación: 17.04.2026

Publicación: en prensa



Este trabajo se publica bajo una licencia de Creative Commons Reconocimiento-NoComercial 4.0 Internacional.

Part I: Warfare Enters the Algorithmic Era

1. Introduction

21st-Artificial intelligence (AI) is transforming the way contemporary military operations are conceived, planned, and executed, introducing technological dynamics that go beyond mere operational efficiency to profoundly affect the attribution of responsibility in armed conflict. Traditionally, legal and ethical frameworks governing warfare have assumed the existence of clearly identifiable human agency: a subject endowed with judgment, intent, and the capacity to be held accountable for decisions. However, the incorporation of algorithmic and automated systems creates a scenario in which decision-making may be distributed across multiple actors, processes, and structures, making it difficult to identify a single, clear responsible party—a phenomenon this paper conceptualizes as the fragmentation of responsibility in contemporary warfare.

In recent months, two relevant cases have illustrated the complexity and urgency of this issue, motivating the present analysis. The first concerns the public dispute between the artificial intelligence company Anthropic and the United States Department of Defense (DoD) over the military use of AI systems. In January 2026, tensions emerged after Anthropic refused to remove ethical safeguards from its models—including restrictions on autonomous and surveillance-related applications—in response to demands for broader military use (according to multiple Reuters reports and journalistic analyses). This disagreement led the DoD to classify Anthropic as a “supply chain risk” and exclude it from new contracts, triggering a legal dispute that has reached several U.S. federal courts, with conflicting rulings regarding the continuation of this designation and its legal implications (for example, an appellate court’s refusal to block the blacklisting, despite a federal court in San Francisco issuing a

preliminary order favorable to the company) (see Reuters, April 8–9, 2026; Forbes analysis on this turning point for the AI industry).

The second case refers to a tragic event that occurred on February 28, 2026, during the conflict between the United States, Israel, and Iran, when a missile strike hit the Shajareh Tayyebeh primary school in Minab, Hormozgan province, killing numerous students, teachers, and school staff—mostly girls—in what has been described as one of the deadliest civilian casualty incidents in the recent phase of the conflict (Human Rights Watch and international media reports estimate at least 165 deaths, including more than 100 girls, pending independent investigations into potential violations of International Humanitarian Law). Human rights organizations have called for transparent investigations and sanctions for possible breaches of international norms protecting civilians in armed conflict (according to Amnesty International reports and analyses by media and documentation organizations).

These cases are not isolated events, but manifestations of an emerging reality: twenty-first-century warfare unfolds in an environment where the interaction between technology, military decision-making, and legal responsibility is increasingly opaque and distributed. The Anthropic controversy highlights the tension between private technological development and state authority in defining the limits of AI use in defense, while the Minab attack exposes the practical difficulties of clearly attributing responsibility in a conflict environment mediated by information, intelligence, and advanced technological systems.

The research question guiding this article is therefore: how is artificial intelligence transforming the attribution of responsibility in contemporary warfare, and what are the legal, ethical, and strategic implications of this transformation? The central thesis is that AI produces a structural fragmentation of responsibility, resulting from the distribution

of agency among multiple human, technological, and organizational actors, as well as from the inherent opacity of algorithmic systems. This fragmentation does not eliminate responsibility, but rather reconfigures it into a diffuse, shared, and practically difficult-to-enforce form.

To address this question, the article develops an interdisciplinary analysis combining international humanitarian law, theories of technological power, security studies, and military ethics, in order to provide an integrated understanding of how AI-mediated warfare affects responsibility in an increasingly complex global environment.

1.1 Problem Statement

The central problem addressed in this study lies in the growing difficulty of attributing responsibility in an environment where military decisions result from complex, distributed, and technologically mediated processes. In traditional models, responsibility could be linked to clearly identifiable individuals or hierarchical structures. However, the incorporation of artificial intelligence introduces multiple layers of mediation that dilute this relationship.

Decisions are no longer the product of a single subject but of a chain involving software developers, data analysts, military operators, political authorities, and technology companies. In addition, there is the influence of the systems themselves, whose internal logic may not be fully transparent or comprehensible. In this context, responsibility becomes fragmented and dispersed, complicating both attribution and enforceability.

Rather than a simple dispersion, this phenomenon constitutes a form of non-linear distributed responsibility, in which the causality of decisions does not follow a single hierarchical sequence but multiple simultaneous trajectories that interact with one another, producing outcomes that cannot be attributed to a single point of origin.

1.2 The Dispute between the U.S. Department of Defense and Artificial Intelligence Companies

A revealing element of this transformation is the relationship between the state and technology companies in the development of artificial intelligence capabilities. In the case of the United States, this relationship has been marked by significant tensions, particularly regarding ethical boundaries and the use of technologies in military contexts.

A paradigmatic example is the controversy surrounding Project Maven, a Department of Defense initiative launched in 2017 to incorporate artificial intelligence into drone imagery analysis. The goal of the project was to use machine learning algorithms to identify objects and individuals in aerial surveillance footage, improving the speed and accuracy of target identification. Although the system did not directly execute attacks, it played a decisive role in the intelligence processes preceding the use of force.

The participation of technology companies in this project triggered strong internal backlash, particularly within Google, whose employees protested the use of their technology in military applications. This pressure led the company not to renew its contract with the Department of Defense in 2018, marking a significant precedent: for the first time, a major technology corporation actively limited its participation in a military program on ethical grounds.

This episode demonstrated that technology companies are not neutral providers but actors with real capacity to influence strategic national security decisions. Their role extends beyond technical development and includes defining operational, ethical, and functional boundaries of the systems they produce.

The resistance of certain sectors of the technology industry to participation in military projects highlights the complexity of the relationship between innovation, ethics, and national security. At the same time, the growing dependence of states on these

companies reinforces their position within the power ecosystem.

This interaction directly contributes to the fragmentation of responsibility, insofar as decisions and consequences are distributed among actors with different interests, values, and normative frameworks. Thus, responsibility for the use of force no longer rests exclusively within the military chain of command but extends—diffusely—to those who design, develop, and shape the technologies used on the battlefield.

1.3 Opacity in Contemporary Military Decision-Making

Opacity is one of the most problematic features of the incorporation of artificial intelligence into military decision-making. Many systems in use today, particularly those based on machine learning, operate as “black boxes”: they process large volumes of data and generate recommendations or classifications without even their users—and sometimes not even their developers—being able to precisely explain how a given result was produced.

In practice, this opacity manifests in concrete situations. For example, an intelligence system may process satellite imagery, behavioral patterns, and communications data to classify a target as a “high-value threat.” The operator receives this conclusion with a statistical confidence level, but not necessarily with a comprehensible explanation of which variables were decisive or how they were weighted. As a result, the final decision—although formally human—relies on a process that is not fully transparent or verifiable in real time.

This limitation not only complicates oversight but also the subsequent reconstruction of events. In the event of an error—for instance, a strike against the wrong target—it becomes difficult to determine whether the failure originated in the data, the algorithm’s design, its training process, or the human interpretation of its output.

In an environment where accountability depends on the ability to explain and justify decisions, this lack of traceability represents a significant challenge. The inability to fully understand how a result was produced limits the attribution of responsibility and weakens control mechanisms.

Thus, opacity is not merely a technical problem, but a structural factor that directly contributes to the fragmentation of responsibility in contemporary warfare, by introducing critical decisions whose origin cannot be clearly identified or fully explained.

1.4 Research Question and Thesis of the Article

Based on the above elements, this article is guided by the following research question: how does artificial intelligence transform the attribution of responsibility in contemporary warfare, and what are the implications of this transformation for the law and ethics of war?

The thesis advanced is that artificial intelligence generates a structural fragmentation of responsibility, resulting from the distribution of agency among multiple human and non-human actors, as well as from the inherent opacity of algorithmic systems. This fragmentation does not imply the disappearance of responsibility, but rather its transformation into a diffuse, shared, and difficult-to-enforce form, leading to a model of warfare that can be characterized as a war without accountable actors in practical terms.

2. The Power Behind Military Artificial Intelligence

The development and deployment of artificial intelligence in the military domain cannot be understood solely as a technological advancement; it is, above all, a political and strategic phenomenon. Rather than a mere tool, artificial intelligence is emerging as an infrastructure of power that redefines the relationships between the state, technology companies, and actors involved in military decision-making.

Its impact lies not only in improved operational capabilities, but in its ability to reshape who controls information, how decisions are structured, and under what conditions authority is exercised. In this sense, artificial intelligence introduces a profound transformation: power is no longer concentrated exclusively in the state chain of command but is distributed across technological and organizational networks that include developers, contractors, and system providers.

This transformation can be understood as a form of structural power, insofar as it shapes the systems and dependencies through which military actors operate (Nye, 2011; Farrell & Newman, 2019). Unlike traditional military power based on visible material capabilities, this new form of power is exercised indirectly through control over data, algorithms, and platforms that mediate decision-making.

The implications are significant. Authority over military action becomes more diffuse, while technological dependence increases. States require capabilities they do not fully control, and the companies that provide them acquire a role that extends beyond the technical sphere into the strategic domain.

In this context, artificial intelligence not only transforms the exercise of power in war, but also the conditions under which responsibility can be attributed. The fragmentation of responsibility—the central axis of this work—does not appear as an accidental effect, but as a direct consequence of this new architecture of power.

2.1 The AI Defense Ecosystem: Companies, the State, and Contractors

Contemporary military power no longer resides exclusively in the capacity of armed forces to deploy force, but in the ability to control and configure the systems upon which others depend (Nye, 2011). In the case of artificial intelligence, this control is exercised within a complex ecosystem that connects private technology companies, state institutions, and specialized contractors.

Within this environment, certain technology companies have acquired a central role due to their capacity to develop advanced models, data infrastructures, and analytical platforms that are critical for defense. Companies such as Anthropic, Palantir, or OpenAI participate in this ecosystem not only as tool providers but as actors contributing to the definition of the conditions under which decision-making systems operate.

The key issue is not the individual behavior of these companies, but the structure of the market and knowledge ecosystem in which they operate. The development of advanced artificial intelligence requires massive datasets, high-cost computational infrastructure, and highly specialized talent, all of which create significant barriers to entry. As a result, only a limited number of actors can compete at this level, consolidating a privileged position within the ecosystem.

This concentration does not necessarily imply wrongdoing, but it does produce a structural effect: a power gap between companies that possess these capabilities and those that could potentially compete under more open access to resources, data, and infrastructure. Consequently, the market does not evolve purely under competitive logic but under dynamics of technological concentration.

From the perspective of states, this situation creates increasing dependence on specific providers whose technology becomes critical infrastructure. This dependence introduces strategic vulnerabilities, as interruption, restriction, or conditional access to these systems may directly affect military decision-making and operational capacity (Farrell & Newman, 2019).

In this context, the AI defense ecosystem not only reshapes public-private relations, but also reconfigures power and dependency structures. This reconfiguration directly affects how responsibility is distributed—and diluted—in contemporary warfare.

2.2 Procurement and Technological Development Processes in the Military Domain

Defense procurement and technological development processes have evolved into complex models of public-private collaboration that, although formally regulated, are in practice highly technical, prolonged, and difficult to fully trace across all stages. Contracts are no longer limited to the provision of hardware or software, but include training, system integration, data access, and continuous maintenance, creating long-term strategic relationships between states and providers.

These processes typically unfold in several stages: from the definition of strategic needs and technical requirements, to bidding, awarding, and contract execution. Throughout this cycle, multiple actors are involved—public institutions, technology companies, specialized contractors, and in some contexts representatives of interests or lobbying groups—whose participation is regulated but who play a relevant role in information flows, standard-setting, and solution framing.

In countries such as the United States, lobbying activity is part of a legal framework requiring transparency and registration. However, its existence reflects a structural reality: access to procurement processes and strategic information is not uniform. Companies with greater technical capacity, financial resources, and institutional presence tend to engage from the earliest stages of the process, allowing them to shape requirements and position themselves advantageously in later stages.

The result is not necessarily an illegal distortion of the system, but the consolidation of an environment in which access, information, and influence are unevenly distributed. Thus, procurement processes do not only select suppliers; they also reproduce and reinforce a power structure in which certain actors occupy a privileged position within the defense technology ecosystem.

As Arquilla and Ronfeldt (1997) argue, in the information age, power is no longer measured solely by the strength of weapons, but by the ability to configure and control information and decision networks. Military artificial intelligence represents an extension of this phenomenon: controlling algorithms and technological infrastructure not only enhances operational capacity but also shapes available options, both against adversaries and within the internal chain of command.

In this context, procurement processes cease to be merely administrative procedures and become spaces where strategic power is constructed. This configuration directly influences technological dependence dynamics and the increasing difficulty of clearly attributing responsibility in military decision-making.

2.3 Structural Influence and Strategic Power of Technology Companies

As discussed in the previous sections, the AI defense ecosystem and the procurement processes through which these technologies are developed and acquired do not merely organize the provision of capabilities; they also configure a power structure in which certain actors occupy a central position. In this context, the influence of technology companies is not exercised only through direct intervention in specific decisions, but more deeply and persistently: by shaping the operational reality in which those decisions take place.

This power is manifested in fundamental yet often invisible aspects: which data is collected and prioritized, which variables are considered relevant, which scenarios are modeled, and which options are presented as viable or recommendable. In other words, it is not only about influencing decisions, but about structuring the framework within which decisions become possible.

Several authors have warned that this technological dependence may evolve into a form of indirect coercion, particularly in geopolitical competition contexts, where

control over technologies, data, or critical infrastructures allows certain actors to shape the behavior of others (Farrell & Newman, 2019). This type of power does not require direct imposition; it operates through dependency, asymmetry of capabilities, and limitation of real alternatives.

Consequently, military sovereignty can no longer be understood solely in terms of traditional military capabilities, but also as the ability to maintain effective control over critical technological infrastructure, including the algorithms and data that power artificial intelligence systems.

Thus, the structural influence of technology companies is not an ancillary phenomenon but a central element in the reconfiguration of power in contemporary warfare. This reconfiguration, as will be developed in the following chapters, has direct implications for the autonomy of military decision-making and for the increasing difficulty of clearly attributing responsibility.

2.4 Artificial Intelligence as Critical Power Infrastructure

In light of the above, artificial intelligence in the military domain can be understood not only as an advanced tool, but as a critical infrastructure of power. Its centrality lies not only in technical capabilities, but in its ability to organize information, structure decisions, and generate long-term strategic dependencies.

This condition implies a qualitative shift: AI systems come to occupy a position similar to other critical infrastructures such as communication networks or energy systems, upon which essential state functions depend. However, unlike those systems, AI incorporates levels of opacity and complexity that hinder traceability and responsibility attribution.

In this context, as Farrell and Newman (2019) note, the concentration of technological capabilities in a limited number of actors and dependence on complex systems can weaken traditional accountability mechanisms. The

result is a growing disjunction between capacity for action and attribution of responsibility.

Therefore, understanding artificial intelligence as critical infrastructure is not merely an analytical exercise, but a strategic necessity. It is essential for designing procurement, regulation, and oversight policies that preserve not only operational effectiveness but also the integrity of the principle of responsibility in warfare.

3. The Fundamental Principle: Responsibility in War

Contemporary warfare cannot be analyzed solely from the perspective of strategy or technology; at its core lies a fundamental principle: responsibility for decisions and their consequences. The emergence of artificial intelligence in the military domain, with its capacity to process information, assist, or even automate lethal decisions, presents an unprecedented challenge to this principle. Responsibility, both in U.S. law and in international humanitarian law, constitutes the condition of possibility of the law of armed conflict and a pillar of ethical and legal legitimacy.

3.1 Responsibility in United States Law

Within the U.S. legal framework, responsibility in the conduct of war is structured through a constitutional architecture designed to balance power between branches of government, preventing the unilateral concentration of authority over the use of force. The Constitution establishes a clear division of competencies: Congress holds the power to declare war under Article I, Section 8, while the President serves as Commander-in-Chief of the Armed Forces under Article II, Section 2. This design reflects a structural principle of democratic control over the use of force, where the legitimacy of military action rests on the interaction between legislative authorization and executive command.

The War Powers Resolution of 1973 reinforces this institutional framework by requiring

notification to Congress within 48 hours of the deployment of forces into hostilities, as well as imposing temporal limits on the use of military force without legislative authorization. Although its application has historically been subject to flexible interpretations, the norm reaffirms a core principle of the U.S. system: war must ultimately be a politically attributable decision within a constitutional framework of responsibility.

From this perspective, neither the Constitution nor the War Powers Resolution depends on the type of technology used in military operations. The legal framework does not regulate whether decisions are supported by artificial intelligence, automated systems, or algorithmic analysis. Instead, it is based on a fundamental criterion: the existence of a human and institutional authority to which the decision to use force can be attributed.

However, it is precisely at this point that the incorporation of artificial intelligence introduces a tension not at the normative level, but at the operational level of decision-making. The use of algorithmic systems in intelligence, planning, and military execution does not modify the formal structure of constitutional responsibility, but it does transform the way in which the decision that is later attributed to a human actor is constructed.

In contemporary practice, military decisions are not isolated acts of individual will, but the result of a complex chain of technical mediations. The information underlying an operation may have been previously collected, filtered, prioritized, or classified by automated data systems developed by private actors under state contracts and subsequently integrated into military command structures. This algorithmic mediation does not formally replace human decision-making, but it does condition its content, speed, and deliberative margin.

In this context, legal responsibility continues to rest on identifiable human authorities; however, the process leading to the decision

becomes increasingly distributed. This creates a tension between the logic of law—which requires clear attribution to a responsible subject—and the operational reality of contemporary warfare—in which decisions are constructed through hybrid systems of information, recommendation, and automation.

Authors such as P. W. Singer (2009) have described this phenomenon as a form of “diffuse responsibility,” where the decision chain is fragmented among multiple actors: technology designers, system providers, intelligence analysts, military operators, and political authorities. This fragmentation does not eliminate legal responsibility, but it complicates its traceability, evidentiary clarity, and causal attribution in concrete cases.

Consequently, the challenge introduced by artificial intelligence in this context is not the replacement of the constitutional framework of responsibility, but its practical tension: a system designed to assign decisions to human subjects now operates in an environment where those decisions are the product of technologically mediated processes whose complexity makes linear reconstruction of responsibility increasingly difficult without artificially simplifying operational reality.

3.2 Responsibility in International Humanitarian Law

International Humanitarian Law (IHL), also known as the Law of Armed Conflict (LOAC), constitutes the legal framework governing the conduct of hostilities and the protection of persons who are not directly participating in armed conflicts. Its primary legal foundation lies in the 1949 Geneva Conventions and their 1977 Additional Protocols, as well as customary international law, as systematized by the International Committee of the Red Cross (ICRC). This framework is complemented by the regime of individual criminal responsibility established under the 1998 Rome Statute of the International Criminal Court, which defines war crimes and reinforces the obligation of accountability for

serious violations of international humanitarian law.

This normative system is structured around essential principles that not only regulate conduct in combat but also define the legal limits of the use of force: the principle of distinction, requiring parties to distinguish at all times between combatants and civilians (Additional Protocol I, Article 48); the principle of proportionality, prohibiting attacks in which incidental civilian harm would be excessive in relation to the anticipated concrete and direct military advantage (Additional Protocol I, Article 51(5)(b)); and the principle of precautions in attack, which requires all feasible measures to be taken to avoid or minimize harm to civilians (Additional Protocol I, Article 57).

Alongside these substantive principles, IHL relies on a dual structure of responsibility: state responsibility for internationally wrongful acts committed by its armed forces, and individual criminal responsibility applicable to commanders and subordinates who order, execute, or fail to prevent serious violations of the law of armed conflict. In this sense, Article 28 of the Rome Statute establishes the doctrine of command responsibility, according to which military superiors may be held criminally liable if they knew, or should have known, that their subordinates were committing crimes and failed to take reasonable measures to prevent or repress them.

Within this legal framework, the incorporation of artificial intelligence into military systems introduces a tension that does not affect the validity of the law itself, but rather its practical application. When a semi-autonomous system participates in target identification, threat classification, or the recommendation of courses of action, and an attack subsequently results in civilian harm, a central question arises: how responsibility is allocated within a technologically mediated decision-making chain.

From a legal standpoint, IHL does not allow responsibility to be transferred to

technological systems. Neither algorithms nor artificial intelligence platforms constitute subjects of international law. Consequently, responsibility continues to rest necessarily with human and institutional actors: the state as the primary subject of international law, the commanders responsible for planning and executing operations, and the chain of command authorizing the use of force.

However, this normative clarity contrasts with the growing complexity of the contemporary operational environment. Military decisions are no longer isolated acts of will but the result of a chain of processes involving automated systems for data collection, filtering, and prioritization. This algorithmic mediation does not replace legal responsibility, but it can make factual traceability more difficult, particularly in high-speed operational environments or situations of incomplete information.

Authors such as Michael Schmitt (2013) have argued that the law of armed conflict does not prohibit the use of autonomous or semi-autonomous systems, but it does require that decisions with lethal consequences remain under a degree of meaningful human control. This standard does not eliminate the technical complexity of modern warfare, but it reaffirms a structural principle of IHL: the necessity of a responsible human judgment within the decision-making chain.

In this sense, the contemporary challenge does not lie in the absence of legal norms, but in the tension between a normative system that demands clear attribution of responsibility and an operational environment in which decisions are constructed through multiple technological, organizational, and algorithmic mediations. The central issue, therefore, is not whether IHL recognizes responsibility—it clearly does—but how to ensure its effective identification in contexts where decision-making processes are increasingly complex and distributed.

3.3 Principles of Distinction, Proportionality, and Command

The principles of distinction, proportionality, and command constitute the operational core of International Humanitarian Law, insofar as they translate its general norms into concrete criteria of conduct in the battlefield. Their function is not merely declarative but practical: they allow for real-time assessment of the legality of military operations and, subsequently, the determination of responsibility for potential violations of the law of armed conflict. However, the incorporation of artificial intelligence systems into intelligence, planning, and execution processes introduces significant changes in the material conditions under which these principles are applied.

The principle of distinction requires parties to a conflict to distinguish at all times between combatants and civilians, as well as between military objectives and civilian objects, in accordance with Article 48 of Additional Protocol I (1977). Operationally, this distinction depends on the ability to correctly identify the nature of a target in a highly complex and dynamic environment. The use of algorithmic systems for pattern recognition, image analysis, or data processing may enhance the speed and scope of identification, but it also introduces a critical dependence on statistical models that do not “understand” the legal or human context of classification. As a result, distinction ceases to be exclusively a situated human judgment and becomes partially dependent on automated inference based on correlations, which may generate classification errors that are difficult to detect in real time, especially under conditions of uncertainty or incomplete information.

The principle of proportionality prohibits attacks in which incidental civilian harm would be excessive in relation to the concrete and direct military advantage anticipated, as established in Article 51(5)(b) of Additional Protocol I. This principle requires a complex qualitative assessment that cannot be reduced to purely quantitative calculations, as it involves legal, strategic, ethical, and

humanitarian considerations. The introduction of artificial intelligence into this process may contribute to scenario modeling, collateral damage estimation, or operational simulation; however, these systems tend to translate qualitative judgments into optimizable numerical parameters, which can create a false sense of precision or control. The central risk is not only computational error, but the gradual substitution of human normative judgment with a technical optimization logic in which what is “acceptable” may be defined by statistical thresholds rather than substantive legal criteria.

The principle of command, finally, constitutes one of the structural pillars of IHL regarding responsibility. This principle implies not only the existence of a hierarchical chain of authority, but also the obligation that decisions involving the use of force are made by individuals capable of understanding their consequences and assuming responsibility for them, in line with the doctrine of command responsibility established in Article 28 of the Rome Statute. The introduction of artificial intelligence into military decision-making processes does not formally eliminate this chain of command, but it does introduce intermediate levels of technical mediation that may affect the clarity of the link between decision, execution, and responsibility. In practice, commanders may receive recommendations generated by opaque data analysis systems whose internal variables are not fully accessible or interpretable, transforming decision-making into a partially assisted process governed by algorithmic structures whose logic is not always fully traceable.

Authors such as Crootof (2016) have warned that autonomous or semi-autonomous systems may “recommend, prioritize, or even execute attacks without any human fully understanding the totality of processed information.” This does not imply the disappearance of human control, but rather its qualitative transformation: control shifts

from full comprehension of the decision-making process to operational trust in complex systems. In this context, the risk is not only technical error, but the gradual erosion of the conditions that allow for fully informed human judgment.

In sum, the incorporation of artificial intelligence does not suspend the validity of the principles of distinction, proportionality, and command, but it does modify the material conditions under which these principles are applied. The most significant consequence is not strictly legal, but operational-normative: the increasing difficulty of ensuring that military decisions remain fully attributable to conscious, informed, and legally responsible human judgment.

3.4 Responsibility as a Condition of Possibility of the Law of War

The Law of War is not merely a set of norms designed to limit violence in armed conflict, but a legal system that makes the existence of regulated violence possible. Its function is not to eliminate war, but to transform it into an activity governed by rules, limits, and accountability mechanisms. In this sense, responsibility is not an accessory element of the system, but its structural condition of functioning.

The logic of International Humanitarian Law and the law of armed conflict is based on a fundamental premise: every legally relevant military action must be attributable to an identifiable subject, whether a state, a commander, or a chain of command. This attribution is not only a matter of legal technique but the mechanism that gives the norms their effectiveness. Without responsibility, the law loses its capacity to regulate conduct, sanction violations, and prevent recurrence.

In practical terms, responsibility fulfills three essential functions within the law of war. First, an attribution function, which links a specific action to a determined legal subject. Second, a control function, which enables institutional and judicial oversight of military decisions.

Third, a deterrence function, insofar as the possibility of sanctions influences the behavior of actors involved in the use of force.

However, the incorporation of artificial intelligence into military decision-making processes introduces a transformation in the material conditions under which this structure operates. Military decisions are no longer constructed solely through direct human judgment, but through hybrid systems involving data processing algorithms, predictive analytics platforms, and automated recommendation mechanisms. This does not eliminate legal responsibility in formal terms, but it does alter its practical configuration by introducing multiple levels of mediation between decision and execution.

In this context, the central problem is not the absence of responsibility at the normative level, but the increasing difficulty of locating it at the factual level. The question is no longer whether a responsible actor exists in abstract terms, but how to identify that actor with precision within increasingly complex, distributed, and technologically mediated chains of decision-making.

Therefore, responsibility begins to acquire a dual character. On the one hand, it remains a legally attributable principle associated with states, commanders, and political authorities. On the other hand, it emerges as a systemic phenomenon, insofar as decisions depend on technological infrastructures, algorithmic models, private providers, and organizational structures that directly influence the final outcome.

However, this systemic dimension should not be interpreted as a dissolution of responsibility, but as a warning regarding its possible functional fragmentation. As will be developed in the following chapters, the contemporary risk is not the absence of responsibility, but its dispersion to such an extent that it becomes difficult to effectively attribute, thereby weakening one of the fundamental pillars of the law of armed conflict.

4. The emergence of artificial intelligence in the military domain

Artificial intelligence has moved from being a support tool to becoming a strategic component of contemporary warfare. Its application not only transforms how information is collected and processed, but also alters decision-making dynamics, operational risks, and the very nature of responsibility. This chapter explores how AI is embedded in the military domain, its advantages, its risks, and how major international actors integrate it into their strategies.

Artificial intelligence does not merely introduce efficiency into warfare; it introduces a structural reconfiguration of responsibility through the fragmentation of the decision-making process.

4.1 What artificial intelligence is and how it operates in military contexts

Artificial intelligence can be understood as a set of computational techniques designed to enable digital systems to perform tasks that normally require human cognitive abilities, such as pattern recognition, information classification, behavior prediction, and the generation of recommendations based on the analysis of large datasets (Russell & Norvig, 2021).

Operationally, AI is not a form of autonomous “intelligence” in the human sense, but rather an advanced statistical system that identifies correlations within datasets and produces probabilistic outputs. Its functioning depends on three core elements: the data that feeds the system, the algorithms that process it, and the computational power that enables large-scale processing.

In the military domain, these systems are integrated into intelligence, surveillance, reconnaissance, and decision-support processes. Common applications include satellite and drone imagery analysis for target detection, prediction of adversary movements, simulation of conflict scenarios, and automated prioritization of operationally

relevant information. In this sense, AI does not formally replace military decision-making, but it directly shapes how decisions are constructed by selecting, organizing, and presenting information to human actors.

This algorithmic mediation has significant implications for military operations. First, it creates a structural dependence on data: decision quality depends directly on the quality, integrity, and representativeness of the information used to train and feed the systems. Second, it introduces the risk of algorithmic bias, whether due to limitations in training data, design choices, or changing operational environments not anticipated by the model. Third, it may generate a false perception of technical objectivity that does not necessarily reflect the normative and contextual complexity of military decisions, particularly those governed by International Humanitarian Law.

For these reasons, artificial intelligence in the military domain should be understood not as an autonomous decision-making actor, but as an infrastructure for information processing and mediation that influences human decision-making. Its relevance lies not only in analytical capacity, but in how it reshapes access to, interpretation of, and prioritization of information underlying operational judgment in armed conflict.

4.2 Semi-autonomous systems and assisted decision-making

Most current military applications of artificial intelligence can be described as semi-autonomous systems, meaning systems that do not fully replace human decision-making but assist it at different stages of the operational process. In this model, AI may identify patterns, suggest targets, classify threats, or prioritize relevant information, while the final decision—at least formally—remains in the hands of a human operator or command chain.

This approach is based on the idea of “meaningful human control,” namely the requirement that real human intervention

exists in decisions with potentially lethal consequences. However, in operational practice, this control may be weakened by algorithmic speed, data complexity, and operational pressure in conflict environments, reducing the effective capacity for oversight. Yet this principle contains an operational paradox: the faster the system becomes, the weaker real human intervention tends to be.

In contrast, autonomous systems are those in which AI not only assists but selects, prioritizes, and executes actions without direct human intervention at the moment of decision. In such cases, the system operates with a higher degree of functional independence, determining when and how to act within programmed parameters. Although their deployment in lethal combat contexts remains limited and internationally debated, they represent a relevant technological horizon in the evolution of contemporary warfare.

In both cases—semi-autonomous and autonomous—a common problem arises: the increasing difficulty of attributing responsibility in a clear and linear way. As several authors have noted, this technological evolution may produce forms of distributed responsibility, where the final decision results from the interaction between human operators, algorithmic systems, and complex organizational structures, making it difficult to identify a single responsible subject (Crootof, 2016).

4.3 Operational advantages of AI: precision, speed, and information processing

The use of artificial intelligence in military contexts improves strike precision, accelerates decision-making, and processes vast amounts of information in real time—critical capabilities in modern warfare. These functions reduce commanders' cognitive burden, enable better integration of multi-source intelligence (satellite imagery, signals intelligence, surveillance, reconnaissance), and support faster and more coordinated operations.

In this sense, AI not only increases operational efficiency but also transforms how the battlefield is perceived, providing predictive analysis and probable scenarios that directly influence strategic planning.

However, as Singer (2009) warns, technological efficiency does not replace ethical responsibility or the obligation of human oversight. On the contrary, these systems may amplify existing errors if input data is incomplete, biased, or misinterpreted, generating significant operational consequences.

4.4 Structural risks of AI: error, opacity, and acceleration of conflict

The risks associated with artificial intelligence in military contexts are not merely incidental or technical, but structural, as they derive from the very way these systems process information and contribute to decision-making under uncertainty.

First, algorithmic opacity makes it difficult to understand how a system reaches a specific recommendation or decision. In many cases, even developers cannot fully reconstruct the internal sequence of processing, which complicates effective human oversight and weakens traditional accountability mechanisms.

Second, AI introduces a critical acceleration factor in the military decision cycle. By drastically reducing the time between threat detection, assessment, and response, these systems can generate escalation dynamics faster than human political or strategic deliberation can manage. This is particularly relevant in high-tech power confrontation scenarios, where speed becomes a decisive advantage but also a source of irreversible errors.

Third, AI systems operate within interconnected and interoperable ecosystems where multiple actors—states, companies, and contractors—depend on shared infrastructures. As Brundage et al. (2018) note, this technological interdependence can lead to situations in which the effects of

military action are difficult to attribute to a single responsible actor, especially when automated systems intervene at multiple stages of the decision process.

Together, these factors create a scenario in which risk no longer arises only from isolated human or technical error, but from the interaction between speed, opacity, and distributed technological power, fundamentally transforming the traditional logic of military control.

4.5 Use of AI in conflicts and international actors

The development and integration of artificial intelligence in the military domain is not uniform; it reflects differentiated strategies shaped by geopolitical interests, technological capacity, and national objectives.

In the United States, AI investment has focused primarily on advanced surveillance systems, cyber defense, and decision-support capabilities, including semi-autonomous applications. This strategy is conceived as a competitive advantage in a rapidly intensifying global technological rivalry (DoD, 2022).

China has adopted a strategy of convergence between artificial intelligence and military modernization, aiming to achieve technological superiority in critical domains. Its approach seeks to close the gap with the United States through systematic integration of AI into offensive, defensive, and command-and-control capabilities (Li & Cheng, 2021).

Russia has focused its AI development on electronic warfare applications, experimental autonomous systems, and reducing human intervention in high-risk environments, reflecting a strategy oriented toward operational efficiency in direct confrontation scenarios (Kremlin, 2022).

Iran, although with more limited capabilities, has shown increasing interest in surveillance systems, drones, and automation tools applied to regional conflicts, reflecting a broader trend toward the democratization of

access to military AI technologies (Meir, 2022).

Ukraine, by contrast, has integrated artificial intelligence into its defense against the Russian invasion, particularly in intelligence analysis, real-time information processing, and the use of open-source and OSINT platforms for tactical decision-making (Jane's, 2023).

Finally, NATO has incorporated AI into its interoperability and collective defense architecture, particularly in scenario simulation, multinational coordination, and procedural standardization. Its role is not only as a user of these technologies but also as a normative actor contributing to the definition of standards and frameworks governing AI deployment in joint operations (NATO, 2023).

4.6 Risks for responsibility and human control

The integration of artificial intelligence into military systems raises fundamental challenges for ethics, responsibility, and decision-making in warfare. Although algorithms can process large volumes of information and perform high-speed functions, they lack moral judgment, contextual understanding, and the ability to properly weigh legal, strategic, and humanitarian consequences.

In this sense, contemporary doctrine emphasizes the need to maintain a degree of human oversight in weapons systems and decision-support tools, particularly in functions involving the use of lethal force. This approach is known as human-in-the-loop, requiring a human operator to remain embedded in the decision cycle, authorizing or validating critical system actions.

However, in operational practice, formal human supervision does not necessarily guarantee effective control. Algorithmic speed, model complexity, and operational pressure may turn human intervention into a formal rather than substantive act, weakening real deliberative capacity.

In this context, the risks associated with AI use go beyond technical errors or isolated failures and relate instead to deeper transformations in the structure of responsibility:

- The dilution of responsibility, where final decisions emerge from interactions between multiple human and technological actors.
- The displacement of effective human judgment, when supervision becomes reactive rather than deliberative.
- Excessive trust in automated systems, leading to implicit delegation of critical decisions.
- Interoperability challenges in multinational environments, increasing error attribution complexity.

Together, these elements show that the central problem is not merely the presence or absence of human supervision, but the progressive fragmentation of the decision-making process, which complicates the identification of a clearly responsible subject within the military chain of action.

4.7 Synthesis and transition

The integration of artificial intelligence into the military domain progressively redefines the balance between operational efficiency and decision-making responsibility. While algorithmic systems offer significant advantages in speed, precision, and large-scale information processing, these same characteristics introduce dynamics that alter the traditional structure of human control.

In particular, accelerated decision cycles, algorithmic opacity, and growing dependence on distributed technological infrastructures contribute to a profound transformation in the exercise of military authority. In this context, human oversight tends to shift toward more formal rather than substantive levels, weakening traceability and complicating accountability.

This tension between technological efficiency and normative control is not merely operational but structural. It marks the inflection point at which the classical architecture of responsibility in war begins to fragment.

The next chapter examines precisely this process of transformation: how the interaction between algorithms, institutional actors, and technological structures contributes to the progressive dilution of responsibility, and why traditional accountability mechanisms are increasingly insufficient to capture the complexity of contemporary warfare.

5. The rupture: the algorithmic dilution of responsibility

In contemporary warfare, the incorporation of artificial intelligence systems does not merely represent an improvement in speed or information-processing capacity, but a structural transformation in how military decision-making is organized. Planning processes, target identification, and operational execution are no longer exclusively the result of linear human judgment, but rather the product of a complex interaction between algorithms, operators, military command structures, and interconnected technological systems.

This reconfiguration alters one of the fundamental principles of the law and ethics of war: the existence of a clearly identifiable subject to whom responsibility for decisions can be attributed. As decisional functions are distributed across multiple actors and levels—from system design to operational deployment—the chain of responsibility becomes progressively fragmented.

In this context, the difficulty lies not only in determining who executes an action, but in reconstructing the full process that leads to it. Military decision-making ceases to be an attributable individual act and becomes the result of a distributed system of action, in which human and algorithmic contributions

are intertwined in ways that are difficult to separate.

This transformation does not eliminate responsibility in formal terms, but it changes its practical nature, generating what can be described as an algorithmic dilution of responsibility, in which legal and ethical attribution becomes diffuse, fragmented, and often retrospectively constructed.

5.1 Fragmentation of the decision chain

The incorporation of artificial intelligence systems into the military domain substantially modifies the traditional structure of the decision chain. In classical models, responsibility was organized in a relatively linear manner, from strategic planning to operational execution, allowing a clearer identification of authority levels and decision attribution.

However, the integration of semi-autonomous systems and advanced data-analysis platforms introduces a far more distributed decision architecture. In this new environment, decision-making is no longer concentrated at a single command level, but is instead broken down into multiple interdependent stages involving system designers, software engineers, intelligence analysts, military operators, and algorithms that process and prioritize information in real time.

This configuration generates a decision chain in which each actor participates only in a fraction of the process, without necessarily having a full understanding of the whole. As Singer (2009) notes, this form of technological organization contributes to the emergence of fragmented responsibility, where individual attribution is weakened because decisions emerge from a collective system rather than a clearly identifiable single will.

The result is a profound transformation of the traditional concept of command, as military decision-making ceases to be a singular and recognizable act and becomes the product of a distributed sequence of human and algorithmic interventions, making *ex post*

reconstruction of responsibility in conflict contexts increasingly difficult.

5.2 Technological opacity and traceability challenges

Artificial intelligence systems used in the military domain, particularly those based on machine learning, exhibit the phenomenon mentioned previously, known as the “black box,” in which the internal processes leading to a decision are not fully interpretable even by their own developers. This introduces a significant level of technological opacity that complicates oversight, control, and especially the attribution of responsibility in cases of error.

It is important to distinguish this phenomenon—referred to here as the “black box”, mentioned previously—from the systems used in aviation. In aircraft systems, although large volumes of data are recorded, flight recorders allow for relatively precise reconstruction of the final minutes of operation, enabling the identification of human, technical, or procedural failures. There is, therefore, a sequential traceability that allows reconstruction of the chain of events.

In contrast, in many military AI systems, traceability is not equivalent to the mere recording of input and output data. Even when system decisions are logged, it can be extremely difficult to reconstruct why a model assigned a particular priority, identified a target, or recommended a specific action, due to model complexity, variable interaction, and lack of internal interpretability.

This problem becomes more severe in operational contexts where algorithmic decision-making is integrated in real time into human command chains. In a hypothetical scenario, for example, a decision-support system could mistakenly classify a civilian installation as a military target due to flawed statistical correlations in training data or misinterpreted visual patterns. In such a case, post-event reconstruction faces a core difficulty: it is not only necessary to determine

who authorized the action, but also how the system generated that specific recommendation within millions of interdependent parameters.

Consequently, opacity in AI systems is not limited to lack of access to the decision process; it implies a rupture in causal reconstruction capacity, significantly weakening traditional mechanisms of investigation, auditing, and accountability in armed conflict contexts.

5.3 Displacement of human judgment

As artificial intelligence increasingly performs functions traditionally associated with analysis and decision support in military contexts, a progressive displacement of human judgment emerges in complex operational environments. While these systems may optimize speed, precision, and information-processing capacity, they lack ethical understanding, moral deliberation, and the ability to interpret the political and human dimensions of war.

This displacement is not merely a technical improvement in task execution, but a deeper transformation in the nature of military decision-making. Human judgment—historically linked to responsibility, prudence, and contextual evaluation—becomes increasingly shaped by algorithmic recommendations that prioritize operational efficiency over normative reflection.

The central concern is not only functional substitution, but the potential reconfiguration of decision criteria in conflict scenarios. Algorithmic logic introduces metrics based on probability, optimization, and performance, while traditional military decision-making also relies on values, legal norms, and ethical principles embedded in military training and doctrine.

This process may generate internal tension within command structures, as operational decisions increasingly rely on systems that do not share—or cannot comprehend—the normative framework guiding human military action. The risk is not only technical but

normative: the gradual erosion of ethical criteria that have historically guided the lawful use of force.

Overall, the displacement of human judgment does not eliminate formal responsibility, but it reshapes the conditions under which that responsibility is exercised, weakening the direct link between decision, intent, and consequence.

5.4 Illustrative cases and attribution problems

The algorithmic dilution of responsibility can be observed in various situations where the interaction between automated systems, human decision-making, and institutional structures complicates the identification of a clear responsible actor.

In military operational contexts, incidents have been documented in which decision-support systems or automated targeting platforms contributed to errors with significant civilian consequences. In these cases, the difficulty lies not only in determining whether a technical or human failure occurred, but in reconstructing the degree of influence exerted by algorithmic systems on the final decision, especially when processed information comes from multiple partially supervised automated sources.

In parallel, at the institutional and technological level, controversies have emerged between AI developers and government agencies, such as public debates surrounding the involvement of companies like Anthropic in projects linked to the U.S. Department of Defense. These discussions are not limited to technological development, but extend to the distribution of ethical and political responsibility in the potential use of AI systems in military contexts.

Both types of situations illustrate the same structural phenomenon: the growing difficulty of establishing a clear line of attribution when decisions result from interactions between algorithmic systems, human operators, and institutional entities with different interests and levels of control. Responsibility thus

ceases to be a clearly identifiable individual attribute and becomes a distributed problem within complex decision systems.

5.5 The production of infinite wars: consequences of responsibility dilution

The increasing incorporation of artificial intelligence into military decision-making introduces the possibility of a profound transformation in the temporal dynamics of armed conflict. In this context, an emerging form of algorithmic perpetuation of conflict can be identified, in which system logic tends to sustain continuous cycles of threat identification, assessment, and response.

This phenomenon is linked, first, to the absence of autonomous ethical criteria in AI systems. Unlike human judgment, these systems lack moral reflection or long-term contextual balancing capacity, operating instead through predefined recognition patterns and objectives. Consequently, their functioning is oriented toward task efficiency, which may sustain operational dynamics even when the broader strategic or political context has changed.

Second, the dilution of responsibility in complex decision chains reduces the capacity to introduce clear institutional brakes on the use of force. When decision attribution is distributed across multiple human and technological actors, identifying a single responsible authority becomes increasingly difficult, weakening traditional political and legal mechanisms of conflict containment.

Additionally, the speed of algorithmic processing and response introduces a continuous interaction cycle between detection, evaluation, and action, potentially intensifying escalation dynamics. Under such conditions, war becomes less a sequence of deliberate decisions and more an automated process of stimulus-response, reducing the pauses necessary for negotiation or de-escalation.

Finally, in scenarios where multiple state and technological actors integrate AI systems into their military capabilities, the interaction

between heterogeneous algorithms can increase operational complexity. This does not imply the total replacement of human decision-making, but rather an increasing technological mediation of threat identification and response processes, which reshapes political agency in conflict and reinforces the tendency toward more continuous and automated warfare dynamics.

6. The Responsibility of Input: The Invisible Link

In the era of artificial intelligence applied to the military domain, responsibility is no longer limited exclusively to the final decision. It extends into earlier stages of the decision-making process that have traditionally remained outside legal and political analysis. In particular, the role of the data that feeds algorithmic systems becomes crucial, as it largely determines the outputs produced by artificial intelligence.

The so-called responsibility of input refers to the obligation to ensure not only the technical quality of data, but also its integrity, provenance, and the conditions under which it is collected, selected, and introduced into systems. This is not merely about ensuring that information is accurate or statistically representative, but about recognizing that data is never neutral: it reflects structural biases, institutional interests, and even deliberate strategic decisions.

From this perspective, the chain of responsibility expands to actors that were traditionally not considered part of military decision-making processes, including system developers, data analysts, information providers, and institutions that collect, filter, or classify the inputs feeding artificial intelligence models.

Therefore, the central question is not only what artificial intelligence does with data, but who defines the data, how it is selected, what is deliberately excluded, and under which power logics the informational universe that feeds algorithmic decision-making is constructed. This shift toward the input stage

introduces a critical dimension in understanding contemporary responsibility, as decisions are shown not to emerge solely from the algorithm, but from a prior process of constructing operational reality.

This approach will be further developed in the following sections, which analyze the legal and strategic implications of manipulation, bias, and data structuring in armed conflict contexts.

6.1 The Role of Data in Algorithmic Decision-Making

Artificial intelligence systems depend structurally on the data they receive in order to generate recommendations, classifications, or automated decisions. As Russell and Norvig (2021) note, the performance of an AI system is strongly conditioned by the quality, structure, and representativeness of the information used to train and feed it.

In the military domain, such data includes heterogeneous sources such as satellite imagery, signals intelligence, operational reports, historical databases, and real-time information flows. However, these inputs are not merely neutral technical support; they are part of a broader process of constructing the operational reality upon which strategic decisions are made.

Thus, the key issue is not only technical accuracy, but also selection, classification, and prioritization of data, since these processes determine what information is considered relevant, what is excluded, and what patterns are deemed significant. In this way, data does not only feed the system—it structures the interpretive framework through which AI understands the environment.

When data is incomplete, outdated, or biased, systems may produce outputs that affect core principles of international humanitarian law, such as distinction, proportionality, and military necessity. However, the problem is not limited to errors in system outputs; it extends to the very origin of the information used to train or activate the system.

In operational scenarios, for instance, incorrect classification of activity patterns or satellite imagery may lead to the misidentification of targets. Yet the central difficulty lies not only in the final result, but in determining whether the error originated in the algorithm, the quality of the data, or human decisions that determined what information was included and under which criteria.

6.2 Manipulation, Bias, and the Construction of Operational Reality

Scholarly literature on AI ethics and governance has emphasized that data bias is not merely a technical flaw, but a structural factor shaping how systems interpret reality and generate decisions (Crawford, 2021). In the military context, this phenomenon acquires particular sensitivity, as algorithmic systems do not only process information—they help define what is considered relevant, visible, or constitutive of a threat.

However, the issue is not limited to unintended bias. In certain contexts, deliberate manipulation of input data may become a tool of strategic influence. This manipulation may occur at different levels: selection of information sources, classification of targets, exclusion of datasets, or construction of training databases designed to steer system behavior toward specific outcomes.

Thus, the central issue is not only data quality, but the fact that data can be politically structured to produce specific algorithmic decisions. This implies that AI does not operate on an objective pre-existing reality, but on a reality that has already been filtered, organized, and hierarchically structured by human and institutional actors.

A particularly relevant aspect is that these processes may generate cumulative effects that are difficult to reverse. Once a system has been trained on biased or incomplete datasets, these patterns tend to be reproduced and amplified over time, consolidating an “operational reality” that

does not necessarily reflect real-world conditions.

This phenomenon not only increases the risk of tactical or strategic errors, but also raises a profound question of responsibility: whether an erroneous decision stems from the algorithm, system design, or the informational architecture underlying it. Therefore, input manipulation is not peripheral—it is central to understanding responsibility in algorithmic warfare.

6.3 “Input Responsibility” as an Analytical Category

The notion of input responsibility expands traditional analyses of accountability in automated military contexts by shifting focus from the final decision to the earlier stages of information construction, selection, and structuring that feed AI systems. The input—the data entering the model—thus becomes central to shaping automated outcomes.

Responsibility can no longer be understood solely as attributing consequences to an operator or linear chain of command. Instead, it becomes a distributed phenomenon involving all actors participating in constructing the informational environment in which automated decisions are made.

This includes software developers, intelligence analysts, data providers, state institutions, and oversight bodies, insofar as their decisions directly or indirectly shape system behavior. As Brundage et al. (2018) argue, this invisible layer of decision-making is critical in AI governance, particularly in contexts where decisions may have lethal consequences.

Beyond identifying actors, the analytical value of this concept lies in redefining the nature of responsibility itself in modern warfare. The key question is not only who operates or authorizes the system, but who determines what information is considered valid, what is excluded, and what structures of meaning are embedded in the model.

From this perspective, data selection and curation are not neutral technical acts, but acts of power with strategic and normative implications. Input responsibility is therefore not a marginal extension of traditional accountability, but a substantive transformation of it. The input ceases to be a technical element and becomes a space of power.

6.4 Legal Implications: Can There Be Liability for Deliberate Data Input Manipulation?

The expansion of AI in military contexts raises complex legal questions extending beyond international humanitarian law into domestic administrative, criminal, and constitutional frameworks. The notion of input responsibility opens debate on whether legal liability can extend to actors involved in pre-decisional stages of automated systems.

Under international humanitarian law, the issue relates to accountability where incorrect, incomplete, or manipulated data contributes to violations of distinction, proportionality, or precaution. The challenge lies not only in attributing responsibility to operators or commanders, but in determining whether external actors—developers, contractors, or data providers—can incur liability for intentional or negligent actions affecting system performance.

At the domestic level, complexity increases further, as responsibility chains may include private entities operating under state contracts or technological partnerships. This raises questions about criminal or administrative liability when data manipulation or deficiencies indirectly contribute to harm in military operations.

This legal framework is complemented by an ethical dimension. Responsibility in algorithmic warfare cannot be reduced to formal legality; it must also be examined through moral principles governing the use of force. The central question is not only whether legal responsibility exists, but whether ethical responsibility arises from the deliberate or negligent construction of

systems influencing potentially lethal decisions.

7. Strategic, Institutional, and Human Implications

The growing integration of artificial intelligence into military systems does not merely transform technical decision-making processes; it reshapes the strategic, institutional, and human architecture of contemporary warfare. War increasingly becomes a hybrid system in which algorithmic mediation plays a decisive role.

Previous chapters have analyzed algorithmic responsibility dilution and input manipulation as factors undermining traceability and accountability. However, these dynamics extend beyond the technical or legal domain, directly affecting how states structure military capabilities, interact with private technology actors, and define authority in conflict.

Strategically, reliance on algorithmic infrastructure introduces new forms of interdependence between state and non-state actors, reshaping geopolitical competition. Institutionally, it challenges traditional command chains operating in environments increasingly mediated by automated systems. Humanly, it transforms combat experience, leadership, and perceptions of responsibility under high-risk conditions.

7.1 Geopolitical Competition and the AI Arms Race

Artificial intelligence has become a central component of contemporary geopolitical competition, redefining how states project military power, manage strategic information, and ensure responsiveness in conflict. The United States, China, Russia, Iran, and other actors are competing not only for technological development, but for control over algorithmic infrastructures that determine decision speed and operational reach.

This is not simply a technological race; it represents a structural transformation of

power, where strategic advantage depends increasingly on processing capacity, predictive modeling, and partial automation of decision-making.

However, this acceleration introduces tension between strategic efficiency and normative control. Pressure to maintain competitive advantage may prioritize speed over legal and ethical constraints, increasing the risk of irreversible automated decisions.

7.2 Privatization of Power and State–Corporate Tensions

AI militarization has intensified structural transformation in state–private relations, where technology companies are no longer mere contractors but co-producers of strategic capability. Military AI ecosystems increasingly depend on deep interdependence between states and corporations developing complex algorithmic systems.

This creates functional dependency: access to data, models, and updates may determine operational continuity. Power is no longer defined only by force, but by control over digital infrastructures enabling force projection.

Private companies may influence system usage conditions, updates, or restrictions, raising sovereignty concerns. Critical capabilities may depend on decisions outside state institutions, blurring public-private boundaries in warfare governance.

7.3 Internal Military Debates and Concerns

The introduction of AI systems has generated significant internal military debates, particularly around human control, accountability, and compliance with international humanitarian law. These debates reflect deeper tensions regarding the transformation of military judgment in automated environments.

A central dilemma emerges: faster and more precise operations may conflict with the need for understanding and responsibility. Algorithmically filtered information

challenges traditional command structures based on direct human authority.

This raises institutional concerns about traceability of decisions in complex operational environments where multiple systems contribute simultaneously to targeting and threat assessment.

7.4 Transformation of the Human Experience of War

AI integration profoundly changes how soldiers perceive and assume responsibility in high-pressure environments. Although AI assists in target identification and operational recommendations, final decisions remain human—creating tension between human judgment and machine-mediated information.

This introduces cognitive and moral uncertainty, as operators may act on systems whose internal logic is not fully transparent, potentially creating disconnection between action and consequence.

Yet ultimately, war still depends on human intervention. No AI system operates without authorization. This creates a critical ethical

tension at the moment where irreversible decisions are made under algorithmic pressure.

7.5 Impact on Military Morale and Leadership

AI integration affects military morale and leadership structures. Responsibility dilution generates uncertainty regarding accountability, affecting trust in command structures and institutional protection.

Military personnel face both physical risk and cognitive vulnerability due to reliance on opaque systems. This creates tension between obedience, technological trust, and independent judgment.

Leadership evolves from tactical command into managing algorithmic uncertainty and distributed responsibility.

With the aim of facilitating the understanding of the key concepts used throughout this analysis, the following glossary presents definitions of the main terms related to the use of artificial intelligence in the military domain¹

¹ This section seeks to provide conceptual clarity and terminological coherence, particularly in a context where technical and legal notions tend to overlap.

- **Artificial Intelligence (AI):**A field of computer science and engineering that develops systems capable of performing tasks that normally require human cognitive abilities, such as pattern recognition, data analysis, prediction, and recommendation of actions. In the military context, AI is understood as the overarching framework within which different algorithm-based technological systems operate.
- **Algorithmic systems:**A set of computational models and mathematical procedures designed to process large volumes of data and generate outputs, classifications, or predictions. In the military domain, these systems constitute the technical infrastructure that enables the functioning of artificial intelligence applications, including image analysis, pattern identification, and the prioritization of operational information.
- **Decision-support systems:**Specific applications of artificial intelligence used in military contexts to assist human operators in decision-making processes. These systems do not formally replace human decision-

making but complement it through recommendations, risk assessments, target identification, and operational scenario simulations.

- **Semi-autonomous systems:**Technological systems that can perform complex functions of analysis, classification, or recommendation with a limited degree of human intervention. Although they do not possess full autonomy, they can significantly influence operational decision-making by reducing the time required for human deliberation.
- **Autonomous systems:**Systems capable of selecting, prioritizing, and executing actions without direct human intervention at the moment of decision. In the military domain, their use remains the subject of ethical and legal debate, particularly regarding the use of lethal force.
- **Military decision-making chain:**A structured sequence of processes through which information is analyzed, alternatives are evaluated, and operational decisions are made in military contexts. Traditionally linear, this chain has become more complex and distributed with the incorporation of algorithmic systems.
- **Distributed responsibility:**A form of attribution of responsibility in which decision-making cannot be

Part II: Power Infrastructures and Technological Sovereignty: How GPS, BeiDou, Starlink, and SWIFT Redefine the Geopolitics of the Iran–United States–Israel Conflict

8. Strategic Autonomy

In contemporary warfare, power is no longer measured solely by conventional military capacity. Strategic competition has shifted toward controlling invisible infrastructures that sustain the operation of the modern state: satellite positioning systems, global communication networks, and international financial platforms.

The conflict between the Islamic Republic of Iran and the United States–Israel axis represents a paradigmatic case of how these infrastructures determine the autonomy, vulnerability, and resilience capacity of state actors.

This article analyzes three fundamental pillars of this power architecture: the GPS satellite navigation system—and its Chinese counterpart BeiDou—the Starlink satellite communication network, and the international financial system SWIFT. Based on these axes, it examines how the United States projects power beyond traditional military domains and how Iran responds

through adaptation strategies aimed at reducing structural dependency.

The study argues that modern war is not fought solely on physical terrain but also in the ability to control, disrupt, or replace the networks that allow a state to operate. The Iranian experience reveals a transition toward a model of strategic resilience, where technological, financial, and informational autonomy becomes a determining factor in the balance of power.

The conflict between Iran, the United States, and Israel has evolved into a confrontation that transcends the conventional battlefield. Current disputes unfold in domains where sovereignty does not depend exclusively on territorial control but on access to systems that allow positioning, communication, and global commerce.

For decades, the United States has consolidated its influence through the control of these infrastructures. Economic sanctions, technological restrictions, and indirect pressure mechanisms have led states such as Iran to rethink their dependency models. Rather than accepting a subordinate position, Iran has developed strategies to reduce structural vulnerabilities, diversify alliances, and create functional alternatives.

assigned to a single individual but instead results from the interaction between multiple human, technological, and institutional actors. This concept reflects the complexity of contemporary military systems based on artificial intelligence.

- **Input responsibility:**A concept referring to responsibility associated with the selection, construction, and structuring of data that feed artificial intelligence systems. It recognizes that data are not neutral and that their quality, bias, or manipulation can directly influence the decisions produced by algorithmic systems.
- **Algorithmic opacity:**A characteristic of some artificial intelligence systems that prevents a full understanding of the internal processes through which outputs or decisions are generated. This lack of transparency hinders supervision, auditing, and the attribution of responsibility.

- **Meaningful human control:**A normative principle according to which decisions with potentially lethal consequences must maintain real, substantive, and verifiable human intervention within the decision-making process. It is a central standard in debates on the use of artificial intelligence in weapons systems.
- **Algorithmic dilution of responsibility:**A process by which responsibility for military decisions becomes fragmented and blurred due to the interaction between automated systems, human operators, and complex institutional structures, making it difficult to clearly attribute responsibility.
- **Human judgment in military contexts:**The ability of military actors to assess information, interpret contexts, and make decisions based not only on data, but also on ethical, legal, and strategic principles. This judgment may be influenced or displaced by algorithmic recommendations

This process does not imply the total elimination of dependency—which would be unrealistic in the current international system—but rather its progressive reconfiguration, aiming to limit external actors' coercive capacity. Analyzing systems like GPS, SWIFT, and Starlink allows understanding not only technological tools but also the mechanisms through which power is exercised in the digital era (Farrell & Newman, 2019).

Iran cannot be understood solely as a contemporary geopolitical actor; its strategic behavior is deeply influenced by a historical legacy tracing back to Persian civilization, which has fostered a culture of resistance, adaptation, and autonomous development in the face of external pressures.

In contrast, the United States has built its power on a global architecture combining military superiority with the control of critical systems, extending influence without the need for direct intervention (Drezner, 2021). Israel acts as a technological multiplier within this system, contributing advanced intelligence, defense, and electronic warfare capabilities, increasing pressure on Iran across multiple dimensions.

9. GPS, BeiDou, and Iranian Strategic Autonomy

The case of U.S. GPS illustrates how a technological infrastructure used in everyday life becomes a strategic power vector. Many readers know GPS for its function in mobile phones or car navigation systems: it indicates routes, calculates distances and arrival times, and allows precise trip planning. However, behind this civilian utility lies a system originally designed for military purposes by the U.S. Department of Defense. Its primary objective is to provide high-precision positioning, navigation, and timing (PNT) for missiles, drones, and logistics operations worldwide (Department of Defense, 2025).

Technically, GPS operates via a constellation of satellites emitting temporal signals. A ground receiver calculates its three-

dimensional position and exact time through trilateration, comparing the difference in signal arrival times from multiple satellites. Accuracy varies by signal type: the public signal used by civilians has lower precision, while the encrypted military signal controlled by the United States allows weapon guidance and synchronization of communication networks with millimeter-level precision (Department of Defense, 2025).

This means that dependence on GPS places Iran in a strategically vulnerable position, as the United States can degrade, interfere with, or limit its signal during conflict scenarios.

During the so-called Twelve-Day War in 2025, Iran detected deviations in GPS-guided missiles and drones, demonstrating that reliance on a system controlled by an adversary can be exploited as a tactical vector (Al Jazeera). Furthermore, journalistic and technical reports recorded intense GPS interference in the Persian Gulf and the Strait of Hormuz, affecting not only military but also civilian and maritime positioning systems, forcing commercial vessels to operate with erroneous or inconsistent location data (The Beirut, 2023).

These experiences showed that GPS, despite being perceived as a civilian tool, is in fact a key strategic infrastructure in any modern conflict, due to its role in guided weapons, military logistics, and communication synchronization.

9.1. Iran's Transition to BeiDou

Faced with this vulnerability, Iran turned to China's BeiDou satellite navigation system, designed from the outset with dual-use capability: civilian and military. Unlike GPS, whose military signal can be interfered with or degraded by an adversary, BeiDou provides redundancy and resilience against electronic warfare, allowing Iran to operate autonomously in strategic operations and project an image of technological resilience in the face of Western blockades (Defence Security Asia, 2023).

Iran's transition from GPS to BeiDou is not a mere technological adjustment but a structural transformation in its conception of modern warfare. For years, the United States assumed that control over critical infrastructures—like GPS—granted a decisive advantage in any confrontation scenario. This premise was based on clear logic: whoever controls the global positioning system controls the adversary's precision.

However, this hypothesis began to erode when Iran demonstrated it could drastically reduce its dependence on GPS, incorporating alternative systems capable of operating even in intensive electronic warfare environments (Al Jazeera).

9.2. Strategic Features of BeiDou

The BeiDou system introduces qualitative advantages that shift the strategic balance:

- **Anti-jamming capability:** Unlike GPS, whose signal can be degraded or manipulated, BeiDou incorporates advanced mechanisms such as frequency hopping and navigation message authentication, making electronic spoofing difficult (Military Aerospace, 2023).
- **Simultaneous use of multiple constellations:** Allows integration of signals from different systems, increasing resilience against blocking or interference attempts (Military Aerospace, 2023).
- **Bidirectional communication:** Unlike GPS, BeiDou allows sending instructions to devices in flight, enabling real-time reprogramming of missiles or drones (Military Aerospace, 2023).

These features do not completely eliminate vulnerability but distribute it strategically, making it difficult for an adversary to fully neutralize Iran's positioning and navigation capabilities.

9.3. Strategic Relevance for Iran

The transition to BeiDou represents an operational vulnerability reduction vis-à-vis an adversary with electronic interference capacity. Adoption of BeiDou allowed Iran to:

- Maintain operational precision in critical weapon systems even under electronic warfare.
- Reduce dependence on technologies controlled by coercive states.
- Increase operational autonomy in space and communication domains.

This process was not merely a technological project but a strategic decision accelerated after the practical vulnerability experience in 2025. Beyond system substitution, simultaneous use of multiple constellations introduces a new operational paradigm: states combine signals and systems to mitigate interference and degradation, reducing vulnerability and complicating complete neutralization by adversaries.

10. Starlink and the War for Satellite Information Control

While GPS and navigation systems like BeiDou condition weapons precision and operational synchronization, satellite communication networks—especially Starlink, developed by SpaceX, owned by Elon Musk—have emerged as critical information infrastructures in conflict scenarios. These domains transmit not only civilian data but also coordinate intelligence, operations, public perception, and information resilience.

10.1. What Starlink Is and How It Works

Starlink is a constellation of thousands of low-orbit satellites designed to provide high-speed, low-latency global internet. Unlike terrestrial networks—dependent on cables, towers, or easily disrupted infrastructure in conflicts—Starlink offers connectivity even when conventional networks have been degraded or blocked, making it a strategic asset for any actor seeking communication, coordination, and real-time information access.

10.2. Starlink in Iran: Resistance, Blockages, and Clandestine Use

In the Iran–United States–Israel conflict, Starlink has played a complex and contentious role. During periods of intense internet restrictions in Iran—including national blackouts during protests—the satellite service was seen as an alternative communication channel. However, Iranian authorities responded with forceful measures:

- Service blocking and degradation: Iran interfered with and “blinded” Starlink terminals, causing significant satellite service interruptions using jammers and sophisticated signal blockades.
- Equipment confiscation: Authorities announced the seizure of hundreds of clandestinely distributed Starlink terminals, labeling them as “enemy devices” subject to severe penalties.
- Information control and censorship: During crises, the government cut national internet access, even affecting satellite connections like Starlink.

Clandestine use and citizen support: Despite restrictions, activists and citizens attempted to connect Starlink devices obtained through international networks.

Cyberactivity and resilience: Iranian hacker groups used Starlink to sustain online operations and cyber resilience, even where terrestrial connections were heavily degraded.

These events demonstrate that, although Starlink is a critical connectivity tool, it is not immune to countermeasures by states controlling the electromagnetic spectrum or restricting its use for security reasons.

10.3. Starlink in Ukraine: Connectivity and Controversies in a Prolonged Conflict

Since Russia’s invasion in 2022, Ukraine has used Starlink terminals to restore civilian internet and maintain emergency and

government communications after attacks on terrestrial infrastructure. Starlink also facilitated military operations, including unit communications, logistical support, and real-time tactical data transmission.

However, Starlink’s use in conflict has sparked controversies: Russian forces reportedly used Starlink equipment to support drones or communication in occupied zones, prompting Ukraine to work with SpaceX to restrict unauthorized terminal usage.

This pattern—use for both civilian connectivity and tactical military support—underscores that satellite networks like Starlink transcend their original civil purpose and become key components in the informational and operational strategies of states and non-state actors.

11. Strategic Implications and Digital Sovereignty

Experiences in Iran and Ukraine reveal several key lessons:

1. Satellite connectivity is not neutral: designed as a civilian service, it becomes strategic infrastructure with direct impact on military operations and conflict perception.
2. Control versus autonomy: states may attempt to restrict, degrade, or capture satellite infrastructure to preserve informational sovereignty.
3. Resilience and innovation: entities dependent on external networks seek to diversify and adapt technologies to avoid vulnerabilities.
4. Ethical and operational dilemmas: Starlink’s dual-use nature raises questions about regulation, neutrality, and control in conflict zones. This pattern—the dual use for civilian connectivity and tactical military support—underscores that satellite networks transcend their original purpose.

Starlink introduces a disruptive variable: critical infrastructure in private hands with autonomous decision-making capacity, redefining traditional sovereignty parameters.

12. SWIFT: From Financial Domination to the Search for Alternatives

The SWIFT system (Society for Worldwide Interbank Financial Telecommunication) is the main international financial messaging network enabling thousands of banks to exchange payment instructions securely and standardized. It is important to emphasize that SWIFT is not a U.S. institution but a cooperative headquartered in Belgium. Nevertheless, its operation is deeply conditioned by the Western financial system, particularly the dollar's weight and the U.S.'s ability to exert political and regulatory pressure on participating actors.

Exclusion from SWIFT has become one of the most potent economic coercion tools. Iran was partially disconnected in 2012 and restricted again in 2018 as part of U.S.-led sanctions. Similar cases, with nuances, have occurred in Russia (after the 2022 Ukraine invasion), North Korea, and to a lesser extent Venezuela. While formal decisions to disconnect banks lie with SWIFT, in practice they respond to political pressures and the need to comply with Washington-led sanctions.

Operationally, SWIFT exclusion complicates, slows, and increases the cost of money transfers:

- International transfers must use intermediaries or indirect channels.
- Transaction times lengthen considerably.
- Costs increase due to multiple intermediaries.
- Many foreign banks avoid operating with the sanctioned country to prevent secondary sanctions.

The result is functional financial isolation, directly affecting foreign trade, especially in strategic sectors such as energy. For Iran, this significantly impacted its ability to sell oil and receive payments efficiently.

Iran has developed alternative mechanisms, including bilateral agreements in local currencies, use of China's CIPS or Russia's SPFS, and informal or crypto mechanisms. These remain limited compared to SWIFT's scale and efficiency.

This acquires strategic significance when linked to the Strait of Hormuz, a major global energy corridor. In tense geopolitical contexts, Iran has suggested—directly or indirectly—that countries transiting this route or trading its oil should transact in non-dollar currencies. This is not merely tactical but part of a broader strategy to reduce dependence on Western-dominated financial systems.

While the petrodollar system underpins U.S. financial power, a shift toward alternative currencies—yuan, ruble, or regional currencies—signals a long-term trend toward de-dollarization and potential fragmentation of international finance.

12.1. BRICS and the Construction of an Alternative Financial Ecosystem

This process of seeking alternatives to the Western-dominated financial system does not occur in isolation. Rather, it is embedded within a broader dynamic driven by the BRICS group, a bloc of emerging economies originally composed of Brazil, Russia, India, China, and South Africa, and later expanded to include new actors such as Iran, Saudi Arabia, the United Arab Emirates, Egypt, and Ethiopia.

Although BRICS does not constitute a formal alliance with a unified agenda or a rigid institutional structure, it does reflect a convergence of interests around a shared objective: reducing dependence on the international financial system centered on the U.S. dollar and on infrastructures such as SWIFT.

Within this framework, Iran's participation acquires particular strategic relevance. It should not be understood merely as a sanctioned state seeking to bypass restrictions, but rather as an actor integrating into a multilateral platform that promotes alternative mechanisms, such as:

- the use of local currencies in bilateral trade;
- the strengthening of alternative payment systems (such as China's CIPS or Russia's SPFS);
- the promotion of new financial institutions, such as the BRICS New Development Bank; and, more incipiently, discussions surrounding clearing mechanisms or reference currencies other than the U.S. dollar.

The coexistence within this framework of actors such as Iran and Saudi Arabia—historically adversaries, yet both highly relevant in the global energy market—introduces an additional layer of complexity. It suggests that, beyond regional rivalries, there exists a shared interest in diversifying financial channels and reducing exposure to external pressure mechanisms.

Recent and forthcoming BRICS meetings, including those held in India, reinforce this trend. While they do not entail immediate decisions capable of transforming the global financial system, they do consolidate a space for coordination in which these ideas evolve and gain political traction.

In this sense, rather than a cohesive bloc, BRICS can be understood as a space of convergence where mechanisms of controlled fragmentation of the international financial system are being tested. It does not replace the existing order, but contributes to eroding its centrality, generating a more multipolar and less predictable environment.

Consequently, although Iran's demands regarding the use of alternative currencies in energy trade do not imply an immediate rupture of the petrodollar system or the role of SWIFT, they do form part of a broader process that could, over time, reduce the effectiveness of these instruments of Western economic control. This diversification strategy seeks to limit Iran's vulnerability to sanctions and financial blockades by creating alternative channels which, although still limited,

represent a step toward partial financial autonomy.

For example, the adoption of bilateral agreements in yuan, rubles, or even regional currencies, together with alternative transfer systems such as INSTEX or SPFS, allows Iran to maintain critical operations without relying entirely on the global financial system dominated by the United States and the European Union.

From a strategic perspective, this process carries significant implications:

Pressure on the petrodollar: Although the dollar remains the dominant currency in energy trade, Iran's insistence on receiving payments in alternative currencies introduces a precedent that could be replicated by other sanctioned states or by countries with similar tensions with Washington, gradually eroding the universality of the dollar in international transactions.

Resilience to sanctions: The ability to operate outside SWIFT, even partially, enables Iran to sustain essential trade relations with strategic actors, including China, Russia, and certain Gulf countries. This financial resilience translates into reduced dependency and, therefore, lower vulnerability to unilateral economic blockades.

Demonstration effect: Iran's policy serves as a signal to other regional and global actors. It demonstrates that dependence on centralized financial systems can be mitigated through diversification, strategic alliances, and the development of alternative financial infrastructures.

13. Conclusions

Power in the contemporary international system is no longer defined exclusively by military capability, but increasingly by the control and resilience of critical infrastructures that enable states to operate within complex and interdependent environments.

Modern warfare is configured as a multidimensional phenomenon, in which

geospatial, informational, and financial domains are intertwined, redefining the traditional boundaries between conflict and strategic competition. In this context, systems such as GPS, BeiDou, and Starlink do not merely constitute technological tools, but rather instruments of structural power, capable of conditioning the operational autonomy of states. The progressive instrumentalization of civilian infrastructures for strategic purposes reveals a profound transformation: the distinction between civilian and military spheres is becoming increasingly blurred, generating new risks and dilemmas in terms of global governance.

The case of Iran demonstrates that vulnerability is not a permanent condition, but rather one that can be mitigated through strategies of technological, financial, and geopolitical diversification. The emergence of initiatives such as BRICS and alternative systems to SWIFT reflects a broader trend toward the fragmentation of the international order, in which interdependence ceases to function solely as a mechanism of integration and increasingly becomes a tool of pressure and resistance. Consequently, contemporary conflicts must be interpreted as competitions for strategic autonomy, where the ability to operate outside infrastructures dominated by external actors becomes a determining factor in the balance of power.

Finally, the absence of clear regulatory frameworks regarding the use and control of critical infrastructures—particularly those operated by private actors—reveals a gap in global governance that increases the risk of escalation and demands a coordinated international response.

The analysis shows a structural transformation of warfare driven by AI, where speed, precision, and automation coexist with a central problem: progressive fragmentation of responsibility. This phenomenon is not merely technical but political, legal, and human.

AI integration reshapes command chains, introduces technological dependency, and

partially displaces human judgment into opaque systems. Responsibility becomes distributed across multiple actors, weakening traceability and accountability mechanisms.

Beyond strategic implications, this affects the human experience of war, influencing morale, cohesion, and leadership under conditions of uncertainty.

At the same time, there is growing concentration of critical capabilities in a small number of private technology actors. This may generate structural power asymmetries where companies become central nodes in defense ecosystems, blurring public-private boundaries and complicating identification of real decision centers.

Existing legal and political frameworks are insufficient to address this complexity. A comprehensive rethinking of responsibility is required, extending beyond final decisions to include system design, data input, and operational architecture.

Final Reflection

In the 21st century, sovereignty is defended not only at borders but in a state's capacity to remain operational when others control the networks that sustain it.

Contemporary warfare presents a fundamental paradox: never before have military decisions been so fast and technologically sophisticated, and never before has it been so difficult to clearly identify who is responsible for them.

Artificial intelligence does not eliminate human responsibility; it redistributes, fragments, and obscures it. Yet ultimately, war still depends on a human decision: to authorize, accept, or execute actions with irreversible consequences.

If responsibility is fully diluted, not only is the law of war weakened, but also its moral foundation. The challenge is not technological—it is institutional: redefining responsibility before the speed of war makes it irretrievable.

References

- Al Jazeera. (2022-2026). *Iran military capabilities and GPS interference analysis*. <https://www.aljazeera.com/>
- ARKIN, Ronald. C. (2013). *Governing lethal behavior in autonomous robots*. CRC Press. <https://doi.org/10.1201/9781420085952>
- BBC News. (2022). *Iran and alternative financial systems: How Tehran bypasses sanctions*. <https://www.bbc.com/news>
- Bank for International Settlements (BIS). (2023). *The future of the monetary system*. <https://www.bis.org/>
- BEN-MEIR, Alon. (2022). *Drone warfare and emerging technologies in the Middle East*. Middle East Security Review.
- BRUNDAGE, Miles, Shahar AVIN, Jack CLARK, Helen TONER, Peter ECKERSLEY, Ben GARFINKEL, Allan DAFOE, Paul SCHARRE, Thomas ZEITZOFF, Bobby FILAR, Hyrum ANDERSON, Heather ROFF, Gregory C. ALLEN, Jacob STEINHARDT, Carrick FLYNN, Seán Ó HÉIGEARTAIGH, SJ BEARD, Haydn BELFIELD, Sebastian FARQUHAR, Clare LYLE, Rebecca CROOTOF, Owain EVANS, Michael PAGE, Joanna BRYSON, Roman YAMPOLSKIY, Dario AMODEI. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. *arXiv*. <https://arxiv.org/abs/1802.07228>
- Center for Strategic and International Studies (CSIS). (2023). *Electronic warfare and GPS vulnerabilities in modern conflict*. <https://www.csis.org/>
- CHATZKY, Andrew., & MCBRIDE, James. (2022). *The U.S. dollar's role in the global economy*. Council on Foreign Relations. <https://www.cfr.org/>
- Constitution of the United States. (1787/1789). (Relevant amendments and articles on war powers).
- CRAWFORD, Kate. (2022). *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. Perspectives on Science and Christian Faith. 74. 61-62. 10.56315/PSCF3-22Crawford.
- CROOTOF, Rebecca. (2016). *The killer robots are here: Legal and policy implications*. *Cardozo Law Review*, 36(5), 1837–1915. <https://ssrn.com/abstract=2534567>
- CUMMINGS, Mary. L. (2017). *Artificial intelligence and the future of warfare*. Chatham House.
- Departamento de Defensa de Estados Unidos. (2022). *Responsible artificial intelligence strategy and implementation pathway*. U.S. Department of Defense.
- Department of Defense. (2025). *Global Positioning System Standard Positioning Service Performance Standard* (5th ed.). U.S. Government. <https://www.gps.gov/>
- DREZNER, Daniel. W. (2021). *The United States of sanctions: How financial power shapes foreign policy*. *Foreign Affairs*, 100(5), 142–154.
- FARRELL, Henry., & NEWMAN, Abraham. L. (2019). *Of privacy and power: The transatlantic struggle over freedom and security*. Princeton University Press. <https://doi.org/10.1515/9780691189956>
- FARRELL, Henry., & NEWMAN, Abraham. L. (2019). *Weaponized interdependence: How global economic networks shape state coercion*. *International Security*, 44(1), 42–79. https://doi.org/10.1162/isec_a_00351
- FERNÁNDEZ RODRÍGUEZ, Juan, Carlos., & LIZ RIVAS, Lenny. (2023). *El terrorismo: aspectos psicosociales en el proceso de radicalización*. Thomson Reuters Aranzadi. Pp. 270-287. <https://doi.org/10.5281/zenodo.14540821>
- International Crisis Group. (2022). *Iran's economic resilience and regional implications*. <https://www.crisisgroup.org/>
- International Committee of the Red Cross. (1949). *Geneva Conventions and Additional Protocols*. <https://www.icrc.org>

- LI, X., & CHENG, Y. (2021). Artificial intelligence and military modernization in China. *Journal of Strategic Studies*, 44(3), 1–25.
- KLEIN, John. (2023). *Cyber, satellites, and geopolitics: Modern strategic infrastructure*. *Journal of Strategic Studies*, 46(4), 789–812. <https://doi.org/10.1080/01402390.2023.XXXXX>
- MARTINO, Luigi., & PAYÁ SANTOS, Claudio. Augusto. (2026). Intelligence Failures: An Exploration of Key Theories. *Revista Científica General José María Córdova*, 24(53), 105–132. <https://doi.org/10.21830/19006586.1485>
- MAZZETTI, Mark, NICAS, Jack., BARNES, Julian. E., & WONG, Edwar. (2022). *The role of Starlink in the war in Ukraine*. The New York Times. <https://www.nytimes.com/>
- MAZURIER, Pablo, & PAYÁ SANTOS, Claudio. Augusto. (2018). *Amenazas híbridas: teoría de la hibridez y nuevo orden internacional*. Thomson Reuters Aranzadi.
- Military Aerospace. (2023). *China's BeiDou navigation system and military applications*. <https://www.militaryaerospace.com/>
- NATO. (2023). Artificial intelligence in defence: NATO policy guidelines. North Atlantic Treaty Organization. <https://www.nato.int>
- NYE, Joseph. S. (2011). The future of power. Public Affairs.
- Reuters. (2023). *Iran expands trade in non-dollar currencies amid sanctions*. <https://www.reuters.com/>
- PAYÁ SANTOS, Claudio. Augusto., MARTINO, Luigi., SANZ GONZALEZ, Roger. S., & DELGADO MORÁN, Juan. José. (2026). Brechas tecnológicas y seguridad: desafíos para las fuerzas del orden y la seguridad pública. En *Influencia de la IA en la gobernanza y el derecho en la era digital* (pp. 169-192). *IGI Global Scientific Publishing*. <https://doi.org/10.4018/979-8-3373-4480-5.ch007> PMCID:PMC12552217
- PAYÁ SANTOS, Claudio. Augusto., Luigi MARTINO., IBAÑEZ LOPEZ, Raquel., SANZ GONZALEZ, Roger. (2025). Cognitive Warfare: The Mind as a Battlefield. *EKSPLORIUM Buletin Pusat Teknologi Bahan Galian Nuklir*, 46(1), 1243-1270. <https://doi.org/10.52783/eksplorium.146>
- PAYÁ SANTOS, Claudio. Augusto. (2017). Sesgos cognitivos en el análisis de inteligencia, *Estudios en Seguridad y Defensa*, 12(23), pp. 63–80. doi: 10.25062/1900-8325.240.
- SOUTO ROMERO, Mar., ARIAS OLIVA, Mario., LÓPEZ-GALIACHO PERONA, Juan. Luis., & PAYÁ SANTOS, Claudio. Augusto. (2025). Geoeconomics: The new logic of global confrontation. *Revista Científica General José María Córdova*, 23(51), 731–750. <https://doi.org/10.21830/19006586.1510>
- RUSSELL, Stuart., & NORVIG, Peter. (2021). Artificial intelligence: A modern approach (4th ed.). Pearson.
- SCHARRE, Paul. (2018). *Army of none: Autonomous weapons and the future of war*. W. W. Norton & Company.
- SCHMITT, Michael. N. (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press. <https://doi.org/10.1017/CBO9781139169288>
- SINGER, Peter Warren. (2009). *Wired for war: The robotics revolution and conflict in the 21st century*. Penguin Press.
- The New York Times. (2023, January 15). U.S. strikes school in Minad, Iran: Investigations underway. <https://www.nytimes.com>
- War Powers Resolution, 50 U.S.C. §§ 1541–1548 (1973).
- Wired. (2023, March 2). Anthropic vs. the Pentagon: AI ethics in defense contracting. <https://www.wired.com>