UDC 341.3:623.4:004.8
DOI: 10.63341/naia-herald/3.2025.09

Human element in algorithmic warfare: Legal foundations and fault lines

Tetiana Hudima*
Doctor of Law, Senior Researcher
State Organisation "V. Mamutov Institute of Economic and Legal Research of the National Academy of Sciences of Ukraine"
01032, 60 Taras Shevchenko Blvd., Kyiv, Ukraine
https://orcid.org/0000-0003-1509-5180

■ **Abstract.** The rapid advancement of artificial intelligence technologies is reshaping the landscape of modern warfare, giving rise to autonomous weapons systems capable of operating with minimal or no human intervention. The study provided a comprehensive legal and policy analysis of the challenges posed by AWS to international humanitarian law, international human rights law, and global security. Based on doctrinal sources, state practice, and armed conflicts, including in Libya, Ukraine, and the Middle East, the study examined key issues such as distinction, proportionality, accountability, and the erosion of human control. The study assessed current international efforts, including discussions within the framework of the UN Convention on Certain Conventional Weapons, and outlines the growing normative consensus around the principle of meaningful human control. The study argued for a multi-layered regulatory approach, combining a legally binding international treaty with national legislative reforms, mandatory legal reviews, and transparency measures such as international registries and independent monitoring bodies. The study also proposed the development of testing standards for AWS and calls for a temporary moratorium on the use of fully autonomous lethal systems until appropriate legal safeguards are in place. In of the context of growing concerns regarding responsibility attribution and real-time legal compliance, the study introduced the concept of "embedded legality" as a forward-looking governance paradigm. This approach reframed compliance not merely as ex post legal review, but as a process of embedding international humanitarian law directly into the design architecture of AWS. The codification of legal principles such as distinction and proportionality into algorithmic decision-making was proposed as both a technical and normative safeguard. The article argued that this paradigm offered a viable pathway to operationalise IHL in increasingly autonomous systems and should be institutionalised through binding domestic and international standards. The study concluded that the law must correlate to technology: legal norms are essential to ensure that AI-enhanced military capabilities are governed by principles of humanity, accountability, and the rule of law. In an era of increasingly automated warfare, legal and ethical governance must remain paramount

■ **Keywords:** autonomous weapons systems; artificial intelligence; meaningful human control; military accountability; legal regulation; national security; embedded legality

■ Introduction

The swift development of artificial intelligence (AI) technologies is profoundly transforming modern armed conflicts, introducing new forms of warfare that go beyond the scope of traditional international humanitarian law. One of the most alarming aspects of this transformation is the deployment of autonomous weapons systems (AWS) capable of making decisions to use lethal force without direct human involvement. The first verified instances of combat deployment of such systems have already

■ **Suggested Citation:**
Hudima, T. (2025). Human element in algorithmic warfare: Legal foundations and fault lines. *Scientific Journal of the National Academy of Internal Affairs,* 30(3), 9-22. doi: 10.63341/naia-herald/3.2025.09.

■ *Corresponding author

■ Received: 18.06.2025; Revised: 02.09.2025; Accepted: 29.09.2025

Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/)

underscored the scale of potential risks. In 2020, the Turkish-manufactured Kargu-2 drone (Nasu, 2021), was reportedly used in Libya in fully autonomous mode, engaging human targets without real-time operator control – effectively marking the first documented case in which a machine independently decided to apply lethal force. The full-scale war in Ukraine (2022-2025) further illustrates this trend, as drones and robotic platforms with autonomous capabilities (Geneva Academy, n.d.), have been increasingly integrated into the military arsenals of modern states.

At the same time, the legal dimension of this phenomenon remains underdeveloped and fragmented. The absence of clear international legal norms concerning the design, testing, and deployment of lethal autonomous weapons systems (LAWS) generates a range of challenges – from ensuring compliance with the principle of distinction to the problem of accountability in cases where algorithmic error leads to the unlawful targeting of civilians. As M. Wareham (2021), Director of the AI Division at Human Rights Watch, has emphasised, autonomous weapons represent "one of the most urgent threats to humanity today". A similar view was expressed by United Nations Secretary-General António Guterres, who has described such systems as "politically unacceptable and morally repugnant", calling for their total ban (Gunawan *et al.*, 2022). The adoption of the UN General Assembly Resolution on LAWS on 2 December 2024[1], supported by 166 states (American Society of International Law, 2023), confirms a growing international consensus on the need to develop new legal mechanisms for regulating this domain. In the context of ongoing armed conflicts, particularly in Ukraine and the Gaza Strip, the urgency of addressing this issue becomes even more apparent.

While the deployment of autonomous systems in armed conflicts is prioritised, there is a growing trend toward their use within domestic settings, particularly in law enforcement. This development expands the spectrum of legal risks, implicating not only the norms of international humanitarian law but also fundamental human rights, including the right to life and access to justice. Accordingly, the legal analysis of AI-enabled autonomous weapons is not only timely but critically necessary for safeguarding the fundamental principles of international humanitarian law and international human rights law, ensuring accountability, and preventing emerging threats to both international and domestic security. E.H. Christie *et al.* (2024), I.V. Sancar (2024) and K.E. Vuyk (2024) explored issues such as explainability, traceability, bias, and the operational unreliability of autonomous systems. These studies advocate hybrid approaches, including experimental deployment phases with guaranteed meaningful human control. These challenges acquire heightened significance in the context of global technological competition.

The study aimed to conduct a comprehensive analysis of the legal regulation of artificial intelligence based autonomous weapons and to develop practical recommendations for its improvement. Achieving this objective will contribute to the formulation of balanced legal responses that reconcile technological innovation in the defence sector with compliance with international law and human rights standards.

Literature Review

Over the 2010-2020, the issue of "AWS" was addressed by scholars, international lawyers, military experts, and human rights advocates. Early studies and reports identified both legal and ethical challenges posed by such technologies. Among earliest studies, the United Nations Special Rapporteur on extrajudicial executions, C. Heyns (2013), warned that autonomous drones could violate the right to life and human dignity, calling for a global moratorium on their development and deployment. In the report "Losing humanity", Human Rights Watch (2012) was among the first to raise the concern of a potential "accountability gap", whereby no individual could be held legally responsible for the actions of an autonomous system. The concept was further developed by T. Chengeta (2016) in an analysis of how existing regimes of legal responsibility under international law does not relate the technological realities of autonomous weapons. Conversely, a range of military analysts and legal scholars argued that emerging technologies can be accommodated within the current legal framework. For instance, M. Schmitt (2013) concluded that AWS are not per se unlawful, and that autonomy, in and of itself, does not constitute a violation of the prohibitions on means and methods of warfare. M. Schmitt (2013) argued that if a weapon is properly designed and lawfully employed, its autonomous nature does not preclude compliance with the core principles of international humanitarian law (IHL). This position has been supported by other experts, highlighting the potential of artificial intelligence to one day reduce human error on the battlefield. At the same time, a substantial body of legal scholarship has drawn attention to the current limitations of AI technology. E. Winter (2022) examined the capacity of AWS to comply with IHL principles and concluded that, at present, such systems are unable to reliably meet the requirements of distinction, proportionality, and precaution – primarily due

[1] Resolution of the United Nations General Assembly No. 79/62 "Lethal Autonomous Weapons Systems". (2024, December). Retrieved from https://documents.un.org/doc/undoc/gen/n24/391/35/pdf/n2439135.pdf.

to insufficiently advanced AI and the lack of contextual awareness. In other words, current "intelligent" combat systems are not yet capable of independently making targeting decisions without a high risk of violating the laws of armed conflict.

Substantial number of studies address the intersection of human rights and ethics. Numerous scholars (Sparrow, 2007; Sharkey, 2008; Asaro, 2012) have argued that delegating the power to kill to machines undermines human dignity, as life-and-death decisions are made in the absence of human moral judgment. This concern also underpins the advocacy efforts of the Campaign to Stop Killer Robots, a coalition coordinated by Human Rights Watch. Its representative, M. Wareham, (2021), has repeatedly emphasised the global threat posed by such technologies and voiced disappointment over the continued reluctance of leading states to take meaningful action to address the issue (Human Rights Watch, 2012).

The discourse surrounding "meaningful human control" is also based on human rights-oriented literature. Experts proposed the concept as an ethical baseline – asserting that weapons should not be permitted to make the decision to kill without human involvement (Article 36, 2013; Docherty, 2014). This idea was later taken up by the International Committee of the Red Cross (ICRC) (2016) and several states, which have advocated for its inclusion in international negotiations (United Nations, 2019). A related strand of scholarship has examined diplomatic efforts and legal initiatives in this area. E. Rosert & F. Sauer (2020) and F. Sauer (2020) analysed the trajectory of negotiations under the Convention on Certain Conventional Weapons (CCW)[1] and the role of humanitarian organisations. The studies note that the process has been slow due to deep divisions among states, and despite numerous meetings of the CCW Group of Governmental Experts, consensus on a binding legal instrument has not yet been reached. At the same time, following the study by A. Wilner & C. Babb (2021), delays may prove dangerous, as technological advancements exceed the scope of territorial and regulatory boundaries and risk undermining existing legal norms. The most current research mentioned in the previous section (Christie *et al.*, 2024; Sancar, 2024; Vuyk, 2024) broadens the discussion and proposes hybrid implementation models with mandatory human control at every stage. Fllowing D. Garcia (2024), without the development of mechanisms for "common good governance", the accelerating AI arms race may weaken strategic stability and erode international legal frameworks.

Thus, the literature review reveals two polar positions – ranging from calls for an outright ban on LAWS based on ethical concerns to arguments asserting that existing law is sufficient. At the same time, there is a shared recognition of the need for concrete legal measures to prevent uncontrolled risks. The present study builds on these contributions, seeking to synthesise them and offer balanced legal responses.

Materials and Method

This study employed a combination of general scientific and specialised legal research methods. The primary method was formal legal analysis, prioritising international humanitarian law and human rights law[2,3] provisions relevant to autonomous weapons, as well as documents, drafts, and recommendations issued by international organisations. A comparative legal method was also applied to examine the approaches of different states (particularly those of the United States, China, and various European countries) to the regulation of AI-enabled weapons. This included analysis of national doctrines and policy instruments, such as the U.S. Department of Defense Directive No. 3000.09[4] on autonomy in weapons systems.

The case study method was used to examine real-world incidents involving the use of autonomous weapons (e.g. in Libya, Ukraine, and the Middle East) to assess their legal implications. Information about these incidents was obtained from open sources (The Associated Press, 2020; CSIS, 2020; Clarke, 2024; United Nations, 2024). The selected body of international and national sources was central in shaping the conceptual and legal structure of this study. The official reports of the Group of Governmental Experts on LAWS (United Nations, 2019; United Nations, 2021; United Nations, 2022) were used to trace the evolution of the international discourse on the human role in the use of autonomous weapon systems, particularly in relation to the requirement of "meaningful human control". These documents provided foundational insights into the legal risks posed by removing human judgment from lethal decision-making processes and was used as a reference point for assessing normative fragmentation across states. The 2020 working paper (United Nations, 2020) was used to identify the early framing of legal and ethical dilemmas, offering a structured basis for analysing the gaps in current international humanitarian law with regard to algorithmic systems. National-level contributions enriched the study by providing

[1] Convention on Certain Conventional Weapons. (2001, December). Retrieved from https://treaties.unoda.org/t/ccw.
[2] Additional Protocol to the Geneva Conventions, Relating to the Protection of Victims of International Armed Conflicts (Protocol I). (1977, June). Retrieved from https://zakon.rada.gov.ua/laws/show/995_199#Text.
[3] Convention on Certain Conventional Weapons. (2001, December). Retrieved from https://treaties.unoda.org/t/ccw..
[4] U.S. Department of Defense Directive No. 3000.09 "Autonomy in Weapon Systems". (2012, November). Retrieved from https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf.

comparative perspectives. France's official position (France's national position…, 2023) was used to demonstrate a restrictive interpretation of autonomy in weapons systems, while the Netherlands' letter to Parliament (Netherlands Government, 2022) illustrated a more permissive regulatory model that still emphasises human oversight.

All sources were used in a multi-layered analysis of the legal foundations underpinning algorithmic warfare, exposing the risks associated with the erosion of human agency in lethal operations. The findings were interpreted using a normative-analytical approach, whereby each observed fact or argument was evaluated against applicable international legal norms. This interdisciplinary methodology, situated at the intersection of international law, security, and technology, can be used in the development of well-founded conclusions and policy recommendations.

Results

The emergence of autonomous weapons confronts states with a fundamental dilemma: how to integrate artificial intelligence into military operations in a way that enhances security, while simultaneously ensuring respect for human rights. From the standpoint of international law, the right to life is both fundamental and inalienable. Even in times of armed conflict, states remain bound by the obligation to respect human life. No considerations of military necessity can justify arbitrary killings of civilians or captured combatants (Geneva Academy, n.d.). An autonomous system operating without human control could, in theory, conduct an unauthorised killing in violation of the right to life and human dignity. For instance, the deployment of robots by police or intelligence agencies to eliminate suspects without judicial oversight would amount to an extrajudicial execution, which is expressly prohibited under international human rights law. Former UN Special Rapporteur on extrajudicial executions, Agnès Callamard, warned that the use of AWS in law enforcement could result in violations of the right to bodily integrity and human dignity (Geneva Academy, n.d.). The use of autonomous systems for targeted killings (for example, within the framework of counterterrorism operations) carries the risk of widespread rights violations, particularly affecting vulnerable populations. Historically, the human element in the application of force has served as a safeguard of deliberation and accountability. In contrast, removing human involvement from strike decisions may lead to unpredictable and disproportionate outcomes. A crucial issue concerns accountability: in the event of an error by an autonomous system, such as a strike on civilians, a fundamental legal question of responsibility is relevant The absence of identifiable perpetrator undermines the principle of accountability, which is foundational to international law (Geneva Academy, n.d.). A victim of an arbitrary killing done by a robot must have the right to an investigation and to justice; otherwise, the very concept of human rights is fundamentally undermined.

Conversely, states justify the development of AWS by invoking national security interests. Proponents of such technologies argue that these systems can save the lives of military personnel by replacing them in high-risk missions and by increasing the overall effectiveness of defensive operations. Autonomous drones do not experience fatigue, react faster than humans, and can operate in environments with high levels of radiation or chemical contamination – conditions in which human operators would not survive. For example, automated air defence systems such as Israel's Iron Dome and the U.S. Navy's Phalanx Close-In Weapon System (CIWS) can intercept incoming rockets or mortar shells within fractions of a second, a response that would be impossible under human control (Perrin, 2025). Such systems can enhance the protection of both civilians and military personnel by responding more effectively to sudden attacks. Moreover, autonomous platforms may reduce casualties among troops by conducting reconnaissance or strike missions without exposing soldiers to direct physical risk. From the perspective of state interests, a further strategic argument is often invoked: if a potential adversary is developing "killer robots", then inequality in this field may result in asymmetric vulnerability. This dynamic creates a security dilemma: states fear falling behind in military technological advancement and therefore accelerate domestic AI weapons programmes. Experts warn that autonomous systems are increasingly perceived by governments as "revolutionary" tools for achieving military superiority, a perception that is already fuelling an arms race.

As of May 2025, reports suggest that both Russia and Ukraine have likely employed autonomous weapons on the battlefield, while active development is underway in China, Israel, South Korea, and the United States (Hoppenbrouwers, 2024; Clarke, 2024; O'Grady *et al.*, 2025). Thus, the national security-oriented approach tends to favour minimal regulation, as states prioritise the technology without forfeiting strategic advantages. This stands in contrast to humanitarian calls for an outright ban on such systems. As a result, a normative conflict emerges: the primacy of human rights versus the primacy of national security. Resolution of this tension requires the development of legal norms that, on the one hand, impose limits to protect individuals from uncontrolled risks, and on the other, provide frameworks for the legitimate use of AI in defence contexts.

International legal mechanisms for risk prevention. There is currently no global treaty specifically regulating AWS. However, such systems fall within the scope of general norms of IHL and international human rights law (IHRL) (Perrin, 2025). All states recognise that there must be no legal vacuum: the UN Charter, the Geneva Conventions, the rules on state responsibility, and other applicable instruments of international law are fully applicable to AWS. In the context of armed conflict, the fundamental principles of IHL are central. States are obliged to ensure that any weapon they deploy complies with the principles of distinction, proportionality, and precaution. This obligation is reaffirmed in Article 36 of Additional Protocol I[1], which requires a legal review of any new weapon, means, or method of warfare to determine whether its use would be prohibited under existing international law. If the use of a weapon in certain circumstances would be inconsistent with legal norms, the state must refrain from employing it in that manner. This requirement is particularly relevant in the context of AWS, which must undergo legal review prior to deployment. For instance, both the United States and NATO have established procedures whereby military legal advisers assess the compliance of proposed systems with IHL obligations (Schmitt, 2013). If a system is deemed uncontrollable or unpredictable, its use in combat must be considered unlawful. Such pre-emptive legal scrutiny would prevent the deployment of systems that are inherently incapable of complying with the law. During the actual use of AWS, commanders remain bound by the same core principles: they must select targets and means of attack in a manner that avoids civilian casualties and ensures proportionality. In practical terms, this requires that human operators retain sufficient control and situational awareness, even when employing an autonomous system (Perrin, 2025). For example, if a robot is tasked with patrolling a designated area and automatically engaging targets, the commander must restrict that area to zones where only combatants are present to prevent any interaction between the system and civilians. Furthermore, the commander is obliged to retain the ability to intervene or deactivate the system in the event of malfunction or unlawful conduct (United Nations, 2024). These requirements function as "safeguard" mechanisms under international humanitarian law, intended to mitigate the risks associated with autonomous operations.

Notably, most states acknowledge that while existing IHL is applicable to AWS, it may require further clarification. Since 2014, discussions have been ongoing within the framework of the Convention on CCW regarding the possible development of new norms specific to LAWS. The CCW Group of Governmental Experts has produced eleven guiding principles. Among these are the enduring human responsibility for decisions on the use of force; the requirement that AWS must comply with international legal norms; and the necessity of "context-appropriate" human control over such systems (Perrin, 2025). However, these principles are not legally binding. Negotiations on a specific treaty have so far yielded no concrete results, as states remain divided. Some, such as Austria, Mexico, and the Holy See, have called for a preventive ban on autonomous weapons, while others, including the United States, Russia, and Israel, oppose such prohibitions and advocate instead for non-binding guidelines. Due to the CCW's consensus rule, the process has effectively stalled (Perrin, 2025). In this context, in December 2024, the United Nations General Assembly took an unprecedented step by adopting a resolution that effectively renewed the debate at the highest political level. The Resolution[2] received near-unanimous support (with only three states voting against) and proposed a "two-tiered approach": to prohibit the most dangerous types of LAWS while subjecting others to strict regulation under international law. It also recommended that states begin developing elements of a legally binding instrument in preparation for the 2026 CCW Review Conference (Perrin, 2025). In May 2025, negotiations on the regulation of autonomous weapons were held at the United Nations, yet reaching consensus among key states such as the United States, Russia, and China remains a significant challenge (Le Poidevin, 2025). Nonetheless, these developments reflect growing political momentum toward the creation of a new treaty or protocol. Future international legal mechanisms may evolve along the following trends: (a) establishment, at the treaty level, of minimum requirements for human control across all systems; (b) prohibition of fully autonomous weapons that select and engage human targets without human intervention; and (c) codification of the principle of state responsibility for the consequences of AWS deployment.

Outside the context of armed conflict, IHRL is critical. As noted earlier, any use of lethal force by the state in peacetime is governed by human rights law, both international and domestic. Accordingly,

[1] Additional Protocol to the Geneva Conventions, Relating to the Protection of Victims of International Armed Conflicts (Protocol I). (1977, June). Retrieved from https://zakon.rada.gov.ua/laws/show/995_199#Text.
[2] Resolution of the United Nations General Assembly No. 79/62 "Lethal Autonomous Weapons Systems". (2024, December). Retrieved from https://documents.un.org/doc/undoc/gen/n24/391/35/pdf/n2439135.pdf.

the integration of autonomous systems into law enforcement activities would require legislative adjustments to ensure compliance with these standards. Several international bodies have already addressed the issue in advance. In 2017, the UN Human Rights Council adopted a resolution emphasised that autonomous systems must comply with IHRL and that states must retain control over their use. Similarly, in the 2022 report A New Agenda for Peace, the UN Secretary-General noted that the uncontrolled spread of military technologies, including AI, poses a threat to human rights (United Nations Secretary-General, 2023). A normative approach is thus taking shape in which core human rights principles, such as the right to life and human dignity, must be integrated into the legal frameworks governing AWS. This could be reflected in a future treaty, for example, through a preambular recognition that decisions over life and death must remain subject to human judgement, in accordance with the imperatives of human dignity.

The issue of responsibility and legal accountability warrants separate consideration. If an autonomous system causes an unlawful death, victims are entitled to justice. In the context of armed conflict, such an incident may constitute a war crime – either as an intentional or negligent killing of protected persons. However, the issue of accountability for the murder by the machine remains relevant. The traditional mechanism is command responsibility. A commander may be held liable for the actions of subordinates if the violations was known and no preventive actions or punishment were undertaken. In the case of AWS, however, the role of the "subordinate" is performed by a machine, raising novel challenges for the doctrine of command responsibility. Many scholars argue that commanders and operators must nonetheless bear full responsibility for the consequences of deploying autonomous systems (Gunawan *et al.*, 2022). In effect, the decision to deploy an AWS is itself an act attributable to the commander; thus, if the system commits a war crime, responsibility lies with the commander or, more broadly, with the state. The challenge, however, lies in the evidentiary difficulties of attributing individual fault, particularly when the system's behaviour was unpredictable due to algorithmic complexity. One proposed solution is the explicit inclusion in a future treaty of a rule assigning full responsibility for the use of AWS to the state and its authorised agents. This would mean that, irrespective of the degree of autonomy involved, the human commander (or operator) is considered the legal subject who "directed" the weapon, and may be held accountable in the same way as for the actions of human subordinates. Such a provision would help close a potential accountability gap. Several states have already affirmed in their national positions that "a human must always remain responsible for the actions of a weapon". International law thus appears to be moving toward the affirmation that autonomous weapons do not entail automatic impunity.

National legal mechanisms. At the national level, no domestic legal systems have yet adopted specific legislation that explicitly prohibits or authorises the use of lethal AWS, largely due to the classified nature of defence programmes and the novelty of the issue. Nevertheless, several states have developed policies and doctrines that indirectly regulate the integration of artificial intelligence into weapons systems. A notable example is the United States, where the Department of Defense issued Directive No. 3000.09[1] as early as 2012, with a revised version adopted in 2023. This directive stipulates that the development and use of autonomous and semi-autonomous systems must preserve an "appropriate level of human judgment" over each decision to apply force (Garamone, 2023). In effect, U.S. policy requires that a human operator remain within the decision-ma king loop for all critical decisions involving the use of force. Moreover, any new AWS in the United States must undergo rigorous testing and high-level approval. The directive mandates that proposed systems be reviewed by a senior-level oversight body before deployment or operational integration (Garamone, 2023). The goal is to ensure that the system operates reliably and in compliance with legal standards. Similarly, the United Kingdom's Ministry of Defence has declared that all domestic weapon systems will operate under "responsible human control" (House of Lords UK, 2024). In the official position issued in 2018, France also emphasised that it does not intend to deploy fully autonomous systems without human involvement (France's national position…, 2024). Germany (Autonomous Weapons, 2025) and the Netherlands (Netherlands Government, 2022) have endorsed international declarations affirming the necessity of "meaningful human control". Thus, a range of democratic states are already de facto limiting the autonomy of weapons systems through political commitments and military policy instruments. It is worth noting that some states (such as Russia and China) have made few public statements on this issue, yet are actively developing relevant technologies. In such cases, international law serves as the primary safeguard, as domestic legal lacunae may result in external consequences (Boulanin & Verbruggen, 2017). National mechanisms may also include export controls: for instance, several countries, including the United States

[1] U.S. DOD Directive No. 3000.09 "Autonomy in Weapon Systems". (2012, November). Retrieved from https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf.

(Shibolet. Law Firm, 2025) and EU member states (European Commission, 2024), have updated their military control lists to enhance oversight of drone exports and AI-related components that could be used in lethal systems. These measures aim to prevent autonomous technologies from falling into the hands of malign actors or terrorist groups.

In summary, national regulation remains fragmented. Leading democratic states have incorporated requirements for human control and weapons review procedures into their military doctrines, while others have taken advantage of the absence of prohibitions to pursue more experimental approaches. In the future, it is expected that states will incorporate international treaty norms (once adopted, or even in anticipation of them) into domestic legislation. This may include, for example, the criminalisation of the development of fully autonomous "killer robots" or the introduction of licensing regimes for military AI research and development. Such steps would help establish a coherent legal space in which the rules of engagement are defined and universally comprehended.

Practical case studies of autonomous weapons use. To further analyse legal implications, it is necessary to examine several documented instances in which autonomous or semi-autonomous weapons systems have been employed by various states. As previously noted, in March 2020, during the civil conflict in Libya, forces of the Government of National Accord, supported by Turkey, deployed STM Kargu-2 loitering munitions against fighters of the Libyan National Army, led by General Haftar. According to a UN Panel of Experts report, these drones were programmed to engage targets without requiring a data connection to a human operator, "effectively operating in a true "fire, forget, and find" mode" (Nasu, 2021). This indicates that the drones independently identified and engaged targets, making autonomous decisions to strike. Although no confirmed casualty figures were reported, the very occurrence of an autonomous combat attack sparked significant international concern. From a legal standpoint, the incident raised several issues. Firstly, compliance with IHL must be considered. Could the Kargu-2 system distinguish between combatants and persons hors de combat? Was the principle of proportionality observed – i.e., was excessive harm avoided? If the drone had killed an unarmed individual or a civilian, such action would have constituted a violation of IHL, raising the question of who bears responsibility – the operator (if one was not in control at the time of the strike), or the commander who authorised the use of the system in autonomous mode. Secondly, the question of accountability arises. The UN report (United Nations Security Council, 2021) was unable to confirm whether any fatalities were caused directly by the drone's actions. Had it been established that a war crime had been committed by the autonomous system, legal accountability could only extend to the individuals who authorised its deployment or were involved in its development. This case has reinforced calls for banning "human-out-of-the-loop" systems, as it demonstrates that such technologies have already reached the battlefield, while effective accountability mechanisms remain underdeveloped. In response to the incident, during UN meetings held in 2021-2022, several states cited the Libya case as evidence of the urgent need for legally binding rules to prohibit similar uses of autonomous systems in the absence of direct human control.

Israel has long been a supplier of autonomous loitering drones. A well-known example is the IAI Harpy, developed in the 1990s as a fully autonomous anti-radiation munition. The Harpy is programmed to patrol a designated area, autonomously detect enemy radar signals, and dive toward the source to destroy it (Perrin, 2025). This is a classic "fire-and-forget" system: the operator launches the drone into a designated area, after which it operates independently, without further commands. Such systems (including the Harpy and its upgraded version, the Harop) have been exported to several countries, including India, South Korea, and Turkey, and were reportedly used by Azerbaijan during the 2020 Nagorno-Karabakh conflict (CSIS, 2020). The legal assessment of such systems is twofold. On the one hand, the Harpy is designed to strike strictly military objectives (specifically, radar installations) which are, by their nature, legitimate targets under international humanitarian law. Its algorithms are configured to detect specific enemy air defence signals, reducing the probability of striking a civilian object relatively low. This differentiates it from a general-purpose "killer robot" that autonomously seeks human targets. On the other hand, the Harpy's autonomy means that no human verifies the target prior to attack. If an adversary turns off their radar and another transmitter operating on the same frequency is present in the area, the drone may mistakenly strike a non-combatant object. In theory, this could include a civilian radar beacon or other non-military equipment. In such cases, compliance with the principle of distinction may be questioned. Therefore, even highly specialised autonomous systems carry a risk of error. One possible regulatory safeguard would be to require states to deploy such drones only in areas where civilian presence can be reliably excluded and only against actively functioning military targets. Notably, the Harpy has been in service for many years, and no serious incidents have been reported, suggesting that user states likely implement certain precautionary measures. Nevertheless, the fact that more than ten countries currently possess a fully autonomous offensive drone (Hammes, 2023), highlights a broader point:

the era of autonomous weapons has already arrived, and international law must keep pace by establishing clear rules governing their use.

Many armed forces around the world deploy stationary or ship-based weapon systems that automatically engage enemy targets. Examples include the U.S. Phalanx CIWS, which is installed on naval vessels and military bases for intercepting missiles, and Israel's Iron Dome, designed to counter artillery shells and rockets. These systems operate with a high degree of autonomy due to the speed at which incoming threats must be neutralised – manual control would be insufficient. The legal framework[1] governing their use typically operates is as follows: an operator activates the automatic mode when an incoming munition is detected, and the system then independently decides when to fire. Notably, the targets in these scenarios are not humans but incoming munitions or rockets – objects that are not protected under IHL. This distinction is significant: such systems do not make decisions over human life or death, but rather intercept hostile projectiles. IHL does not prohibit the use of automation against inanimate military objects. Nonetheless, incidents have occurred. During the 2003 Gulf War, the automated Patriot PAC-2 system mistakenly shot down a British fighter jet, misidentifying it as an enemy missile. Subsequent investigations revealed a failure in the "friend-or-foe" recognition system (Piller, 2003). This incident demonstrated that even defensive AWS requires human oversight – at minimum, the capacity for emergency shutdown or intervention. Since then, operational protocols have been improved. For instance, current Patriot system crews are bound by strict rules regarding target identification, and in cases of uncertainty, human confirmation is required before engagement. From a legal perspective, such incidents are generally classified as accidents or tragic mistakes, since there was no intent to violate IHL. Nonetheless, it is evident that full autonomy, even in narrowly defined operational roles, can cause dangerous consequences. To prevent such outcomes in the future, legal instruments could include a requirement for a so-called "kill switch" – a human-operated mechanism to immediately deactivate the automated mode (United Nations, 2024), if the system behaves unpredictably.

Current armed conflicts reveal a growing trend in the deployment of autonomous and semi-autonomous systems. In the Russian war against Ukraine, both sides extensively employ unmanned aerial vehicles (UAVs) for reconnaissance and strikes. Some of these UAVs are equipped with artificial intelligence components. For example, the Russian Lancet-3 loitering munition reportedly possesses autonomous targeting capabilities: it can detect targets based on pre-programmed parameters and automatically guide toward them without requiring further human input (Perrin, 2025). Although it is likely that the final strike decision is still made by a human operator (at least according to publicly available Russian sources), this reflects a broader trajectory: an increasing number of functions are being delegated to algorithms. On the Ukrainian side, the military has reportedly been experimenting with systems that use computer vision to guide drones toward enemy equipment. In addition, both sides have reportedly employed robotic platforms for fire support, such as remotely operated turrets that, in theory, could also operate autonomously. While none of these cases resulted in known violations of international humanitarian law, they contribute to a growing legal grey area: it is becoming increasingly difficult to determine where "smart automation" ends and "lethal autonomy" begins. Contemporary conflicts indicate that the widespread use of even semi-autonomous systems is transforming the nature of warfare. Adversaries may begin to act more rapidly, and the pace of reciprocal strikes may accelerate to a level where human decision-making cannot keep up – posing serious challenges for escalation control. As noted in an analysis by the Geneva Academy, if decision-makers rely too heavily on fast-reacting autonomous systems, they may lose the ability to manage crises and control escalation when events unfold on the tactical level at speeds that outpace human intervention" (Geneva Academy, n.d.). This is not only a humanitarian concern but also a strictly military one: warfare itself may spiral beyond the control of the parties involved. The ongoing war in Ukraine has further demonstrated how rapidly technologies can proliferate – cheap drones and open-source software for autonomous navigation are now accessible not only to states, but also to non-state armed groups. The legal implication is evident: there is an urgent need to develop binding international rules, or future conflicts risk becoming testing grounds for unregulated autonomous systems.

Although autonomous weapons are most often discussed in military contexts, their potential deployment in domestic settings cannot be overlooked. In 2016, police in Dallas (USA) used a remotely operated robot to neutralise an armed suspect – effectively killing the perpetrator by detonating an explosive device attached to the robot (Solon, 2016). The device was remotely operated, and thus legal responsibility was on the human operator. However, in 2022, the authorities in San Francisco took the discussion

1 Additional Protocol to the Geneva Conventions, Relating to the Protection of Victims of International Armed Conflicts (Protocol I). (1977, June). Retrieved from https://zakon.rada.gov.ua/laws/show/995_199#Text.

further by considering whether to authorise the police to deploy robotic systems with lethal capabilities in certain emergency situations (The Associated Press, 2022). Initially, the proposal received approval from the city council, sparking widespread public outcry and leading to its withdrawal. Nonetheless, the precedent is significant: it marked the first attempt to legalise the use of robots with potential autonomous lethal capabilities in a civilian law enforcement context. The legal implications are clear – such actions fall under constitutional protections and statutory regulations concerning the use of force by police. In many jurisdictions, the law explicitly requires officers to issue a warning, attempt non-lethal measures, and assess the necessity of force before resorting to lethal means. A robot cannot autonomously fulfil these procedural safeguards. As a result, the integration of AI into law enforcement will require legal reform – at minimum, provisions must state that any decision to apply lethal force must rest with a human officer, and that the robot serves only as an instrument. Otherwise, there is a risk of violating the right to due process and the presumption of innocence, as machines would effectively be executing punishment without trial. This case underscores that the regulation of autonomous weapons must extend beyond the battlefield to address their potential deployment in domestic security contexts. While public backlash has constrained such initiatives, advancing technologies are likely to increase the temptation to use AI-driven systems for counterterrorism or public order enforcement.

The case studies examined above demonstrate that autonomous weapons are no longer theoretical – they are a present reality requiring urgent legal reflection. Each case reveals vulnerabilities in existing law: whether in distinguishing lawful targets, ensuring accountability, or adapting norms to the rapid tempo of modern combat. This analysis lays the groundwork for a set of recommendations aimed to mitigate the risks identified herein.

Discussion

The study results indicated that the existing regulatory vacuum in the field of LAWS could not be filled solely by a prohibitionist ethical approach or by mechanically applying the existing norms of IHL. While the academic literature has traditionally been divided between these two positions (Sharkey, 2008; Asaro, 2012; Schmitt, 2013), both empirical evidence and normative analysis revealed deeper structural inconsistencies within the current legal architecture. In particular, the assumption that existing IHL norms are sufficient to regulate LAWS lost credibility in the face of their real-world deployment, which exposed critical gaps in accountability and legal clarity (Winter, 2022; Nnamdi *et al.*, 2023; Clarke, 2024).

The notion that the core IHL principles of distinction, proportionality, and harm prevention can be technically encoded remains conceptually fragile. The principle of distinction, enshrined in Articles 48 and 51 of Additional Protocol I to the Geneva Conventions[1], requires human ethical judgement and contextual awareness that cannot be replicated by algorithmic means alone (Rosert & Sauer, 2020; Nnamdi *et al.*, 2023). As a result, contemporary LAWS were not capable of making legally informed decisions under conditions of normative ambiguity or complex combat environments. At the same time, the debate on permissible levels of autonomy is shaped not only by legal regimes but also by actors beyond intergovernmental institutions. As I. Bode (2024) demonstrated, narratives emerging from diplomats, arms manufacturers, and journalists significantly shape perceptions of autonomy, which in turn influence the legitimacy of regulatory strategies. This form of "normative constructivism" contributes to the fragmentation of the international legal order, as illustrated by Q. Qerimi's (2024) typology of state positions on LAWS. The classification outlines six regulatory strategies (ranging from total prohibition to conditional acceptance) and underscores the absence of a unified international consensus. Another layer of divergence lies in public perception: research by K. Arai & M. Matsumoto (2024) shows that support for LAWS varies depending on context, such as national defence or levels of civilian harm. This finding highlights the need to account for ethical context when designing regulatory frameworks.

The deployment of the Kargu-2 drone in Libya, as documented in the report of the UN Security Council Panel of Experts (United Nations Security Council, 2021), brought renewed urgency to the issue of legal accountability in the context of increasing autonomy in combat systems. Despite the potential compliance with the principle of military necessity, the absence of clear evidence regarding human control over the decision-making process raised serious concerns about adherence to the standard of "meaningful human control" (International Committee of the Red Cross, 2021). This regulatory gap illustrated that the pace of technological advancement significantly outstripped the capacity of legal frameworks to respond to emerging challenges.

The international discourse on the legal governance of AWS remained fragmented. While some states, such as Austria and Mexico, supported the adoption of a legally binding treaty, others (including

[1] Additional Protocol to the Geneva Conventions, Relating to the Protection of Victims of International Armed Conflicts (Protocol I). (1977, June). Retrieved from https://zakon.rada.gov.ua/laws/show/995_199#Text.

the United States and Israel) employed a more cautious stance (United Nations Secretary-General, 2023; Qerimi, 2024). The persistent deadlock within the framework of the Convention on CCW highlighted the limitations of consensus-based diplomacy in the face of deep geopolitical divides. The juxtaposition between states such as the US, China, Israel, and Russia, opposing strict regulation, and others such as Austria, Mexico, or the Holy See, advocating for a total ban, prevented the formation of a unified regulatory framework (Qerimi, 2024).

In this context, national approaches gained increasing prominence. The US Department of Defense Directive No. 3000.09[1], France's official position advocating an "appropriate level of human control," and the recommendations of the House of Lords UK (2024) illustrated the emergence of internal regulatory models that could serve as a foundation for a future global regime. This evolution from consensus-based to polycentric norm-making reflected a potential pathway towards the gradual codification of new international standards.

As T.F.A. Watts & I. Bode (2024) argued, perceptions of autonomous systems are shaped by cultural narratives, notably the recurring metaphor of the "Terminator" as a hyper-precise guardian-machine executing human intent. Such imaginaries served to legitimise political strategies of underregulation. Real-world examples of AWS implementation in law enforcement (such as the Dallas police incident (Solon, 2016) or debates in San Francisco (Associated Press, 2022)) pushed the issue outside the battlefield and into the realm of domestic security. This expansion necessitated the integration of IHRL, especially the right to life and guarantees of due process.

At the core of the regulatory discourse remained the concept of meaningful human control; however, no universally accepted definition or operational mechanism has yet emerged. B. Perrin (2025) proposes a multi-layered accountability model encompassing Article 36 of Additional Protocol I[2] legal reviews, transparency requirements, and criminal liability for negligent delegation of lethal decision-making functions. In this context, the model introduced by T. Zurek *et al.* (2023) provided a particularly illustrative conceptual framework. It presented a hybrid architecture for an autonomous combat system designed to comply with IHL. The proposed framework integrated five key legal tests (including proportionality, harm minimisation, and the duty to take precautionary measures (Article 57) within a formalised logical structure that could be used for potential software-based implementation. The tension between direct human control and partially automated evaluation of the legality of combat decisions was emphasised. By combining a knowledge-driven architecture with normative constraints, this model constituted a valuable conceptual contribution to the discourse on the legal accountability of autonomous systems.

The cumulative evidence presented in this study suggests that legal accountability for autonomous weapons cannot be sustained by traditional doctrines alone. Instead, an emerging solution lies in the concept of embedded legality: the technical integration of international legal norms, such as proportionality, distinction, and precaution, into the very architecture of autonomous systems. This approach transcends reactive legal enforcement and instead redefines legality as a design imperative. By embedding legal safeguards into system behaviour, and by ensuring that these norms are encoded as operational constraints, states can move toward a proactive model of legal compliance. This reconceptualisation may guide future regulatory instruments, offering a constructive path between the extremes of prohibition and deregulation. In conclusion, contemporary debate on LAWS cannot be reduced to the binary of prohibition versus permission. Instead, it must be grounded in the construction of a multi-layered regulatory framework capable of addressing the ethical, legal, and security challenges posed by the evolution of autonomous military technologies.

Conclusions

The study examined the legal and ethical implications of deploying AWS, emphasising whether existing frameworks under IHL and IHRL remain adequate to ensure accountability, legality, and civilian protection. The research confirmed that key IHL principles, such as distinction, proportionality, and precaution, are difficult to implement algorithmically, while traditional doctrines of command responsibility and weapons review lack the capacity to govern systems operating without real-time human oversight. Drawing on case studies from Ukraine, Libya, Israel, and the United States, the analysis revealed a growing legal vacuum concerning the attribution of responsibility in machine-led targeting. The ongoing war in Ukraine, where AI-enabled systems have been deployed with unclear command chains and limited post-hoc attribution, underscores the urgency of enforceable safeguards and exposes the limitations of existing legal architectures.

[1] U.S. DOD Directive No. 3000.09 "Autonomy in Weapon Systems". (2012, November). Retrieved from https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf.
[2] Additional Protocol to the Geneva Conventions, Relating to the Protection of Victims of International Armed Conflicts (Protocol I). (1977, June). Retrieved from https://zakon.rada.gov.ua/laws/show/995_199#Text.

In response, the study proposes a shift in conceptual framing: the governance of AWS should not be confined to a binary choice between prohibition and permission, but reconceptualised as the construction of a multi-layered normative architecture. A central claim is that legal responsibility must be re-anchored from the human operator to the technical design of the system itself. Rather than treating the law as an external constraint-imposed ex post, this study argued that legal norms must be embedded into the algorithmic architecture ex ante – transforming IHL principles into functional design parameters. The proposed concept of "embedded legality" exceeds the scope of external normative oversight and entails the incorporation of legal norms directly into the technical design of autonomous weapon systems. It involves the codification of proportionality thresholds, precautionary criteria, and standards of human control as operational parameters embedded within the system's real-time decision-making logic. To operationalise this concept, national and international regulatory frameworks must require the integration of such legal constraints as a condition for the development, deployment, and export of AWS. This entails embedding IHL-based thresholds not only in technical specifications, but also in national legislation, certification protocols, and weapons review mechanisms.

The Russian war against Ukraine provides an empirical testbed for this reconceptualisation, demonstrating the risks semi-autonomous systems without institutionalised review mechanisms or binding standards of responsibility attribution. To address these challenges, the study proposes a tripartite national governance model: (1) a legally binding glossary to clarify key terms such as "autonomy", "meaningful human control" and others; (2) institutionalisation of a national weapons review mechanism in line with Article 36 of Additional Protocol I to the Geneva Conventions; and (3) targeted export controls for AI-enabled military systems that align security interests with humanitarian norms.

The findings suggest that effective AWS governance must integrate legal, ethical, and technical dimensions. Countries undergoing military digitalisation (such as Ukraine) bear both the responsibility and the opportunity to lead in designing legal frameworks that internalise humanitarian principles not only in institutional oversight, but also in system architecture. Future research should prioritise the doctrinal adaptation of command responsibility to autonomous decision-making systems, the development of enforceable legal glossaries, and cross-jurisdictional benchmarking of AWS governance models to ensure future compliance, legitimacy, and accountability.

Acknowledgements

This scientific work has been prepared within the framework of the research activities of the State Organisation "V. Mamutov Institute of Economic and Legal Research of the National Academy of Sciences of Ukraine".

Funding

The study was not funded.

Conflict of Interest

None.

References

[1] Arai, K., & Matsumoto, M. (2024). Public perceptions of autonomous lethal weapons systems. *AI and Ethics*, 4, 451-462. doi: 10.1016/j.clsr.2023.105854.

[2] Article 36. (2013). *Killer robots: UK government policy on fully autonomous weapons*. Retrieved from https://article36.org/wp-content/uploads/2013/04/Policy Paper1.pdf.

[3] Asaro, P. (2012). On banning autonomous weapon systems: Human rights, automation, and the dehumanization of lethal decision-making. *International Review of the Red Cross*, 94(886), 687-709. doi: 10.1017/S1816383112000768.

[4] Autonomous Weapons. (2025). *The political landscape: How nations are responding to autonomous weapons in war*. Retrieved from https://autonomousweapons.org/global-perspectives-on-regulation/.

[5] Bode, I. (2024). Emergent normativity: Communities of practice, technology, and lethal autonomous weapon systems. *Global Studies Quarterly*, 4(1), article number ksad073. doi: 10.1093/isagsq/ksad073.

[6] Boulanin, V., & Verbruggen, M. (2017). *Mapping the development of autonomy in weapon systems*. Solna: SIPRI.

[7] Chengeta, T. (2016). Accountability gap: Autonomous weapon systems and modes of responsibility in international law. *Denver Journal of International Law and Policy*, 45(1). doi: 10.2139/ssrn.2755211.

[8] Christie, E.H., Ertan, A., Adomaitis, L., & Klaus, M. (2024). Regulating lethal autonomous weapon systems: Exploring the challenges of explainability and traceability. *AI and Ethics*, 4, 229-245. doi: 10.1007/s43681-023-00261-0.

[9] Clarke, K. (2024). *Ukraine and the troubling future of A.I. warfare*. Retrieved from https://www.americamagazine.org/politics-society/2024/07/18/ukraine-lethal-autonomous-weapons-systems-pope-francis-un-international.

[10] CSIS. (2020). *The air and missile war in Nagorno-Karabakh: Lessons for the future of strike and defense*. Retrieved from https://surl.li/qbtkvd.
[11] Docherty, B. (2014). *The human rights implications of "killer robots"*. Retrieved from https://www.jurist.org/commentary/2014/06/bonnie-docherty-autonomous-weapons/.
[12] European Commission. (2024). *Exporting dual-use items*. Retrieved from https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items_en.
[13] France's national position submitted to the United Nations General Assembly on the Resolution No. 78/241 "Lethal Autonomous Weapons Systems". (2023). Retrieved from https://docs-library.unoda.org/General_Assembly_First_Committee_-Seventy-Ninth_session_%282024%29/78-241-France-EN.pdf.
[14] Garamone, J. (2023). *DoD updates autonomy in weapons system directive*. Retrieved from https://www.defense.gov/News/News-Stories/Article/Article/3278065/dod-updates-autonomy-in-weapons-system-directive.
[15] Garcia, D. (2024). *The AI military race: Common good governance in the age of artificial intelligence*. Oxford: Oxford University Press.
[16] Geneva Academy. (n.d.). *Sending up a flare: Autonomous weapons systems proliferation risks to human rights and international security*. Retrieved from https://surl.li/yozxlc.
[17] Gunawan, Y., Aulawi, M.H., Anggriawan, R., & Putro, T.A. (2022). Command responsibility of autonomous weapons under international humanitarian law. *Cogent Social Sciences*, 8(1), article number 2139906. doi: 10.1080/23311886.2022.2139906.
[18] Hammes, T.X. (2023). *Autonomous weapons are the moral choice*. Retrieved from https://www.atlanticcouncil.org/blogs/new-atlanticist/autonomous-weapons-are-the-moral-choice.
[19] Heyns, C. (2013). *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions*. Retrieved from https://digitallibrary.un.org/record/749635.
[20] Hoppenbrouwers, A. (2024). *The Global South and autonomous weapons controls*. Retrieved from https://www.armscontrol.org/act/2024-11/features/global-south-and-autonomous-weapons-controls.
[21] House of Lords UK. (2024). *Proceed with caution: Artificial intelligence in weapon systems. Report of Session 2023-24*. London: Authority of the House of Lords.
[22] Human Rights Watch. (2012). *Losing humanity: The case against killer robots*. Retrieved from https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots.
[23] International Committee of the Red Cross. (2016). *Autonomous weapon systems: Implications of increasing autonomy in the critical functions of weapons*. Retrieved from https://www.icrc.org/en/publication/4283-autonomous-weapons-systems.
[24] International Committee of the Red Cross. (2021). *Autonomous weapons: The ICRC recommends adopting new rules*. Retrieved from https://www.icrc.org/en/document/autonomous-weapons-icrc-recommends-new-rules.
[25] Le Poidevin, O. (2025). *Nations meet at UN for "killer robot" talks as regulation lags*. Retrieved from https://www.reuters.com/sustainability/society-equity/nations-meet-un-killer-robot-talks-regulation-lags-2025-05-12.
[26] Nasu, H. (2021). *The Kargu-2 autonomous attack drone: Legal & ethical dimensions*. Retrieved from https://lieber.westpoint.edu/kargu-2-autonomous-attack-drone-legal-ethical.
[27] Netherlands Government. (2022). *Letter to Parliament about autonomous weapon systems*. Retrieved from https://www.government.nl/documents/publications/2022/10/10/letter-to-parliament-autonomous-weapon-systems.
[28] Nnamdi, N., Eniola, B.O., & Abegunde, B. (2023). Examining Lethal Autonomous Weapons through the lens of international humanitarian law. *Scholars International Journal of Law, Crime and Justice*, 6(6), 329-338. doi: 10.36348/sijlcj.2023.v06i06.001.
[29] O'Grady, S., Khudov, K., & Korolchuk, S. (2025). *Ukraine scrambles to overcome Russia's edge in fiber-optic drones*. Retrieved from https://www.washingtonpost.com/world/2025/05/23/ukraine-russia-drones-fiberoptic-jamming/.
[30] Perrin, B. (2025). Lethal autonomous weapons systems & international law: Growing momentum towards a new international treaty. *ASIL Insights*, 29(1).
[31] Piller, C. (2003). *Vaunted Patriot missile has a "friendly fire" failing*. Retrieved from https://www.latimes.com/archives/la-xpm-2003-apr-21-war-patriot21-story.html.
[32] Qerimi, Q. (2024). Controlling lethal autonomous weapons systems: A typology of the position of states. *Computer Law & Security Review*, 59, article number 105854. doi: 10.1016/j.clsr.2023.105854.

[33] Rosert, E., & Sauer, F. (2020). How (not) to stop the killer robots: A comparative analysis of humanitarian disarmament campaign strategies. *Contemporary Security Policy*, 42(1), 4-29. doi: 10.1080/13523260.2020.1771508.
[34] Sancar, I.V. (2024). How can we design autonomous weapon systems? *AI and Ethics*, 5(2), 967-975. doi: 10.1007/s43681-024-00428-3.
[35] Sauer, F. (2020). Stepping back from the brink: Why multilateral regulation of autonomy in weapons systems is difficult, yet imperative and feasible. *International Review of the Red Cross*, 102(913), 235-259. doi: 10.1017/S1816383120000466.
[36] Schmitt, M.N. (2013). Autonomous weapon systems and international humanitarian law: A reply to the critics. *Harvard National Security Journal*, 4.
[37] Sharkey, N. (2008). The ethical frontiers of robotics. *Science*, 322(5909), 1800-1801. doi: 10.1126/science.1164582.
[38] Shibolet. Law Firm. (2025). *Developments in global trade controls: January – March 2025*. Retrieved from https://www.shibolet.com/en/developments-in-global-trade-controls-january-march-2025/.
[39] Solon, O. (2016). *Use of police robot to kill Dallas shooting suspect believed to be first in US history*. Retrieved from https://www.theguardian.com/technology/2016/jul/08/police-bomb-robot-explosive-killed-suspect-dallas.
[40] Sparrow, R. (2007). Killer robots. *Journal of Applied Philosophy*, 24(1), 62-77. doi: 10.1111/j.1468-5930.2007.00346.x.
[41] The Associated Press. (2022). *San Francisco supervisors bar police robots from using deadly force for now*. Retrieved from https://www.npr.org/2022/12/06/1141129944/san-francisco-deadly-robots-police.
[42] United Nations Secretary-General. (2023). *Our Common Agenda Policy Brief #9: A New Agenda for Peace*. Retrieved from https://peacemaker.un.org/sites/default/files/document/files/2024/08/our-common-agenda-policy-brief-new-agenda-peace-en.pdf.
[43] United Nations Security Council. (2021). *Final report of the Panel of Experts on Libya established pursuant to Security Council Resolution 1973 (2011) addressed to the President of the Security Council*. Retrieved from https://docs.un.org/en/S/2021/229.
[44] United Nations. (2019). *Report of the 2019 session of the Group of Governmental Experts on Lethal Autonomous Weapons Systems*. Geneva: UNODA.
[45] United Nations. (2020). *Working paper: Towards a framework on LAWS*. Geneva: UNODA.
[46] United Nations. (2021). *Report of the 2021 session of the Group of Governmental Experts on LAWS*. Geneva: UNODA.
[47] United Nations. (2022). *Final report of the 2022 session of the GGE on LAWS*. Geneva: UNODA.
[48] United Nations. (2024). *Lethal autonomous weapons systems: Report of the Secretary-General*. Retrieved from https://documents.un.org/doc/undoc/gen/n24/154/32/pdf/n2415432.pdf.
[49] Vuyk, K.E. (2024). Why outlaw LAWS?: An argument for a probationary period for lethal autonomous weapons systems under meaningful human control. *University of Cincinnati Intellectual Property and Computer Law Journal*, 9(1), article number 1.
[50] Wareham, M. (2021). *Ringing the alarm on killer robots*. Retrieved from https://www.hrw.org/news/2019/11/20/ringing-alarm-killer-robots.
[51] Watts, T.F.A., & Bode, I. (2024). Machine guardians: The Terminator, AI narratives and US regulatory discourse on lethal autonomous weapons systems. *International Studies*, 59(1). doi: 10.1177/00108367231198155.
[52] Wilner, A., & Babb, C. (2021). New technologies and deterrence: Artificial intelligence and adversarial behaviour. In F. Osinga & T. Sweijs (Eds.), *NL ARMS Netherlands annual review of military studies 2020* (pp. 401-417). Hague: T.M.C. Asser Press. doi: 10.1007/978-94-6265-419-8 21.
[53] Winter, E. (2022). The compatibility of autonomous weapons with the principles of international humanitarian law. *Journal of Conflict and Security Law*, 27(1). doi: 10.1093/jcsl/krac001.
[54] Zurek, T., Kwik, J., & van Engers, T. (2023). Model of a military autonomous device following International Humanitarian Law. *Ethics and Information Technology*, 25, article number 15. doi: 10.1007/s10676-023-09682-1.

Роль людини в алгоритмічному веденні війни: правові засади та проблемні точки регулювання

Тетяна Гудіма
Доктор юридичних наук, старший дослідник
Державна установа «Інститут економіко-правових досліджень
імені В.К. Мамутова НАН України»
01032, б-р Тараса Шевченка, 60, м. Київ, Україна
https://orcid.org/0000-0003-1509-5180

■ **Анотація.** Стрімкий розвиток технологій штучного інтелекту радикально змінює характер сучасної війни, спричинюючи появу автономних систем озброєння, здатних діяти з мінімальним втручанням людини або повністю без такого втручання. У цій статті здійснено комплексний правовий і політико-правовий аналіз викликів, які такі системи становлять для міжнародного гуманітарного права, міжнародного права прав людини та глобальної безпеки. На основі доктринальних джерел, практики держав і подій у збройних конфліктах (зокрема в Лівії, Україні та на Близькому Сході) досліджено такі ключові питання – принципи розрізнення та пропорційності, проблему відповідальності та загрозу втрати людського контролю. У роботі обґрунтовано необхідність багаторівневого регулювання: від прийняття юридично зобов'язального міжнародного договору до реформування національного законодавства, впровадження обов'язкових юридичних експертиз, створення міжнародних реєстрів і незалежного моніторингу. Запропоновано також тимчасовий мораторій на використання повністю автономної летальної зброї до ухвалення належних правових гарантій і розроблення стандартів тестування. У висновку підкреслено: право не повинно відставати від технологій. Чітке правове регулювання є критично важливим, щоб гарантувати, що воєнні інновації слугують людству, а не загрожують йому. У контексті занепокоєнь щодо відповідальності та забезпечення дотримання права в режимі реального часу в дослідженні було запропоновано концепцію «вбудованої юридичності» як перспективну нормативну парадигму регулювання автономних систем озброєння. Такий підхід переосмислює забезпечення дотримання правових норм не як виключно постфактумний юридичний контроль, а як процес інтеграції міжнародного гуманітарного права безпосередньо в архітектуру проєктування автономних систем озброєння. Кодифікацію правових принципів, зокрема розмежування та пропорційності в алгоритмічну логіку ухвалення рішень окреслено як технічний і нормативний запобіжний захід. У статті констатовано, що зазначений підхід є дієвим шляхом до практичного впровадження норм міжнародного гуманітарного права в умовах зростання автономності систем і має бути інституціоналізований через обов'язкові національні та міжнародні стандарти. В умовах зростання автоматизації війни верховенство права та гуманність мають бути вищими за алгоритми

■ **Ключові слова:** автономні системи озброєння; штучний інтелект; суттєвий людський контроль; військова відповідальність; правове регулювання; національна безпека; вбудована юридичність