

Perspective

Artificial Intelligence in Autonomous Weapon Systems: Legal Accountability and Ethical Challenges

Ibrar Ahmad^{1*} , Laila Ahmad², Naila Irshad³ and Muhammad Talha⁴

¹School of International Law, Southwest University of Political Science and Law, China

²School of Economics, Southwest University of Political Science and Law, China

³University of Gujrat, Pakistan

⁴Government Post Graduate College Mardan, Pakistan

* Corresponding Email: ibrarahmad557@gmail.com (I. Ahmad)

Received: 23 October 2024 / Revised: 26 December 2024 / Accepted: 19 February 2025 / Published online: - 28 February 2025

This is an Open Access article published under the Creative Commons Attribution 4.0 International (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/>). © Journal of Engineering, Science and Technological Trends (JESTT) published by SCOPUA (Scientific Collaborative Online Publishing Universal Academy). SCOPUA stands neutral with regard to jurisdictional claims in the published maps and institutional affiliations

ABSTRACT

Autonomous Weapon Systems (AWS) are reshaping modern warfare, offering enhanced operational efficiency but raising significant legal, ethical, and regulatory concerns. Their capacity to engage targets without human intervention creates an accountability gap, challenging the application of International Humanitarian Law (IHL). The current legal frameworks are incompetent to define meaningful human control. That complicates the attribution of responsibility when AWS violate human rights. Ethical challenges, including the dehumanization of warfare, algorithmic biases, and indiscriminate targeting, jeopardize civilian protection. Moreover, the proliferation of AWS amplifies global security risks, particularly with their potential misuse by non-state actors. This paper critically examines these challenges, evaluating current legal frameworks, ethical considerations, and regulatory inconsistencies. It proposes war torts, corporate accountability, transparency measures, and binding international treaties to address governance gaps. Supports international cooperation and oversight mechanisms is essential to ensure AWS comply with IHL and human rights law. This research contributes to the global discourse on autonomous warfare, offering practical policy recommendations for ethical and legal governance.

Keywords: Artificial Intelligence; Autonomous Weapons System; International Law; Proliferation

1. Introduction

The fast development of autonomous weapon systems (AWS) transforms traditional war practices. AWS operates independently because these systems recognize and strike targets without requiring human intervention [1]. The autonomous capability brings important benefits including high accuracy, reduced personnel danger and better resource management [2]. The advantages of these systems come at the expense of critical disadvantages. AWS create multiple complicated issues because they execute deadly actions without human supervision. In 2020, a drone strike in Libya marked the first reported use of an AWS in combat, igniting global debates about accountability, compliance with international humanitarian law (IHL), and the moral implications of delegating life-and-death decisions to machines [3]. The growing adoption of AWS technologies threatens to reduce legal compliance while reducing human dignity and destabilizing princi-

ples [4]. The challenges require both enhanced regulatory frameworks and fundamental reforms of accountability frameworks for warfare systems controlled by artificial intelligence.

The accountability gap represents a legal and ethical conundrum because AWS violations of both IHL and human rights remain without responsible parties [5]. Autonomous systems present a problem when traditional legal concepts of mens rea (intent) and actus reus (action) are designed for human decision-makers. The absence of consensus about "meaningful human control" stands as an obstacle to AWS regulation because the concept lacks a clear definition [6],[7]. A programming failure that leads an AWS to strike a civilian building produces three possible defendants: the developer the military commander or the government. Without well-defined liability protocols, victims cannot pursue legal recourse that subsequently degrades trust in existing laws. The traditional military hierarchy faces disruption through AWS while states find it challenging to assign responsibility because of these systems'

unique operational characteristics [8]. IHL alongside other legal frameworks fail to provide sufficient solutions for addressing the distinctive challenges created by AWS. According to Boothby the application of distinction and proportionality principles proves challenging for autonomous weapons systems that function independently [9]. AWS systems experience difficulties distinguishing between armed combatants and ordinary innocent civilians which can result in IHL violations [10]. Machines cannot perform human-level assessments of moral and strategic factors [11],[12]. That constitutes proportionality because this judgment process depends on human decision-making abilities[13]. The rising concept of “meaningful human control” shows potential in solving legal concerns but its unclear definition and irregular applications have delayed progress [14]. The absence of clear guidelines creates two major problems: reduced accountability and unexpected governance gaps which prevent the world from properly responding to AWS threats.

The ethical challenges of AWS create supplementary difficulties. Machine-based selection of lethal choices in warfare threatens to dehumanize combat operations. The absence of empathy and moral judgment together with an inability to grasp complex human life characteristics makes machines unable to make ethical warfare choices [15],[16]. Technological advancement results in organised forces more easily and causes more destruction and suffering [17]. The susceptibility of AI algorithms to biases represents an additional threat because they might enable processor targets along with causing unacceptable damage to particular populations [18],[19]. AWS systems remove moral accountability from life-and-death decisions according to deontological ethics [20]. The AWS achieves harm reduction outcomes by maintaining soldier survivability [21]. The potential benefits from AWS systems remain untapped because of unresolved ethical and legal issues they generate. Achieving a balance between technological development and moral standards exists as both a practical requirement and a formal moral duty. At the international level regular progress towards AWS regulation remains challenging because of global political disharmony coupled with national interests. Under the United Nations Convention against Certain Conventional Weapons (CCW) countries try to find solutions but agreement remains doubtful [22]. Most nations support the principle of human control over AWS. However, they cannot agree on what meaningful human control requires nor how to implement it [23]. China demonstrates this contradiction between global commitments to AWS bans and its ongoing substantial investment in military AI systems [24]. The disagreements about AWS frameworks highlight the pressing demand for binding international rules that protect human rights [25].

The analysis of this study focuses on these problems through an investigation of AWS accountability gaps together with existing legal framework inadequacies and ethical concerns. The paper evaluates three solution approaches by analysing war torts alongside transparency measures and corporate accountability while examining their respective strengths and limitations. The research examines global initiatives to control AWS under international law. In response to AWS challenges, this paper proposes a framework that maps legal rules to ethical values and regulations. This guide shows that technological advancement must be complemented with institutional responsibility and human dignity while presenting ways to maintain proper autonomous technology usage. The research findings can therefore be used for future governmental action on how to regulate this rapidly emerging area.

Key Research Questions:

How do autonomous weapon systems (AWS) create legal and ethical problems regarding IHL compliance and accountability issues?

What changes should be made to current legal structures to control AWS technology while holding those who break rules accountable?

The research addresses an expanding body of AWS studies through a proposed framework that integrates legal analysis with ethical matters and regulatory considerations. This work presents actionable solutions through war torts and corporate accountability. To bridge liability gaps while maintaining compliance with International Humanitarian Law. The research findings will help shape current discussions and future regulatory efforts within this fast-developing domain.

2. Literature review

The deployment of AWS has created legal, and ethical dilemmas and regulatory questions like no other conventional technology. Exclusively operated weapon systems present new challenges to traditional approaches to liability and International Humanitarian Law implementation.

2.1. Accountability Gaps in AWS and IHL Compliance

Multiple studies indicate significant deficiencies exist while dealing with the accountability gap; such as ethical challenges and regulatory discrepancies. The research reviews current studies to determine knowledge gaps before showing how this paper addresses those deficiencies. According to Crotof, AWS disrupts the current legal frameworks because these systems eliminate humans from making key decisions [26]. When IHL and human rights violations occur without proper accountability systems, then it becomes difficult to prosecute because victims cannot access legal remedies [27]. The automatic nature of AWS systems generates ambiguous boundaries of responsibility just like who bears legal accountability developers, commanders, or the states [28]. Verdiezen et al., demonstrate that meaningful human control demands technical monitoring combined with active human oversight to guarantee compliance with IHL [29]. The current literature failed to explore this conception, which indicates a significant deficiency in existing knowledge. This research examines the accountability gap through critical analysis followed by proposals for war torts and improved oversight systems. This research examines which mechanisms help to identify responsible parties while guaranteeing legal redress for violations committed by AWS.

2.2. Ethical Concerns: Lethal Decision-Making by Machines

The concern about the moral dimensions arises from having machines handle important death-dealing decisions. Some critics maintain that when AWS assumes lethal decision power, it removes the human effort in making judgements to determine life and death matters. According to Sparrow, machines do not possess empathy and the ability to reason ethically as mandatory elements for decision-making [30]. The way autonomous weapons operate creates doubts about both discriminatory targeting methods and unintended harm that primarily affects vulnerable groups [31],[32].

2.3. Algorithmic Biases and Their Ethical Implications

The built-in biases within AI algorithms function to intensify the above-mentioned ethical challenges. Studies show that algorithmic biases produce discriminatory results that violate fundamental principles of fairness and justice in military conflicts [33]. AWS may reduce the total amount of harm to soldiers through protective measures, but their ethical problems need resolution before this potential benefit can materialise [34]. Current research shows that establishing complete ethical frameworks requires human control together with rational moral processes and IHL compliance.

This research develops previous arguments by demonstrating that ethical guidelines must be implanted throughout AWS design stages and operational phases. This research covers the identified ethical gaps that appear throughout existing literature. The global regulations of AWS face numerous considerable obstacles.

2.4. Regulatory Challenges and Global Governance of AWS

The United Nations Convention on Certain Conventional Weapons (CCW) stands at the centre of international discussions about regulating autonomous weapon systems. According to Docherty, the international community struggles to reach an agreement on fundamental issues, including the definition of meaningful human control [35]. National security priorities, along with technological progress, result in opposing viewpoints between states that prefer human control of AWS systems. Due to these regulatory inconsistencies, there are gaps in global governance, the main obstruction to enforcing International Humanitarian Law standards [36]. The research addresses framework limitations by implementing international agreements together with mandatory operational guidelines. The research facilitates AWS regulatory development through standardized definitions and global collaboration platforms.

2.5. Security Risks and Misuse of AWS Technology

The AWS platform serves two functions which allow unauthorized groups including non-state actors and rogue states and criminal organizations to exploit these capabilities. Such risks intensify because no effective international system exists to monitor these developmental processes. The spread of AWS technology creates unstable situations in regions and intensifies existing humanitarian emergencies as Verdiesen et al., argue. The literature demonstrates the necessity of creating powerful universal agreements to regulate AWS use. Boothby explains how export control systems together with monitoring systems provide essential authorization control for these technologies [9]. International collaboration faces significant obstacles because states fail to work together. The research outcomes will help to define improved international standards for arms control as well as intergovernmental cooperation aimed at counteracting the misuse of AWS technologies. The research successfully balances the technological advancement and the security measures of the global world together with the humanitarian needs. Studies indicate that the regulatory structure of AWS is composed of several critical flaws. Business activities within AWS encounter challenges because of the absence of clear procedures since the current human rights and humanitarian protection frameworks do not have effective ways of sharing responsibility. Inadequate accountability systems that remove legal redress from the victims effectively lead to a fatal blow to the doctrines of the rule of law. Modern frameworks are lacking in creating enough ethical standards that address the ethical issues of the use of AWS technology in automated death decisions. International progress for effective frameworks remains low due to poor standard operational procedures of the regulatory institutions and the failure to develop standard definitions of human control. AWS technologies have relatively few restrictions that put into place risks that make non-state actors and rogue states use these technologies. It is a qualitative work, which focuses on ethical issues and legal analyses to provide solutions for the identified gaps. The combination of the legal parameters and ethical principles along with the regulatory safeguard provides an effective framework that ensures the protection of human value along with the humanitarian law standard for AWS.

3. Methodology

The study adopts the quantitative research method to examine the challenges that result from the use of autonomous weapon systems (AWS). The study focuses on the primary legal sources, the Geneva Conventions, the UN Convention on Certain Conventional Weapons (CCW) and International Committee of the Red Cross reports. The research gathers its information through the analysis of journal articles and case laws. The research explores the approaches in which autonomous systems are granted lethal decision-making power through an ethical perspective that is a blend of deontology and utilitarianism.

4. Analysis

The rapid development of Autonomous Weapon Systems (AWS) leads to various legal questions ethical challenges and regulatory framework difficulties. This scenario of operation autonomous systems raises fundamental questions regarding IHL compliance and accountability frameworks. Technological progress in this area creates complex circumstances involving legal liability, ethical matters and global security risks.

4.1. Accountability and Legal Responsibility

The literature shows substantial concern about AWS operations due to insufficient responsibility tracking systems. The ICRC (2016) clarifies that due to unclear accountability guidelines, the violations of IHL or human rights standards face difficulties [37]. AWS operations frequently lack meaningful human control which makes it difficult to determine legal accountability for violations. A lack of personal responsibility raises critical difficulties for those seeking justice [38]. Traditional legal concepts which include mens rea and actus reus fail to work properly when used to analyze autonomous systems operation. The accountability deficit is an important issue as it comes from the lack of assigning human agency in the case of AWS. Even in human-controlled military systems, responsibility can be attributed; however, AWS complicate this issue by operating autonomously. The consequent confusion of who is to blame, most especially when the actions of AWS are damaging or against the law, erodes the efficiency of legal systems. Interestingly, human intervention is important in addressing these challenges since it guarantees that decision-making can always be traced to humans. According to McDougall, the number of human actors involved in each system is the best way to assign responsibility when there are AWS violations [39]. Verdiesen et al. claimed a high level of proactive human oversight measures that would guarantee accountability. While McDougall concentrates on the role of human control in situations that require accountability. Verdiesen suggests enhancing the framework of technical and potentially reportable and manageable mechanisms, including human supervision. There is a gap in the current legal frameworks; there is no precise definition of meaningful human control. Such a situation creates confusion that arises and hinders any attempts by the states and international organisations for improved accountability. The lack of a standard for AWS responsibility poses no action against the perpetrators and undermines IHL compliance.

4.2. Ethical Implications

It is hard to describe the ethical potential of AWS, although the issue of lethal choices is rather crucial here. McDougall claims that to become effective killers, AWS does not need practical moral reasoning when it comes to choosing between life and death[40]; which could entail disproportionate lethal force and additional suffering. In the same manner, Verdiesen et al., note that AWS might dehumanise warfare by bringing the lethal force to a higher level while decreasing the moral aspects of warfare and raising the probabilities of discriminative targeting. The autonomous weapons sys-

tem (AWS) faces a serious ethical issue because it lets machines autonomously determine when to kill the targets. Due to their programming, AWS lack the built-in ability that human soldiers possess to analyse moral effects before making decisions. AWS systems cannot make judgements about human life, which demonstrates their inadequate ability to perform critical decisions. Discriminatory targeting poses a serious ethical problem because AWS algorithms could display bias that causes human rights violations resulting in excessive harm to civilian populations. The authors agree ethical frameworks are essential; however, they implement different strategies to enforce humanitarian principles with AWS. McDougall proposes new ethical guidelines for military use, while Verdiesen et al. emphasize that frameworks must be created to direct AWS operations. This shows an important lack of ethical oversight for AWS, which especially affects its ability to make moral decisions automatically. The absence of ethical guidance creates a situation that can harm humans by violating both human dignity standards and human rights. An urgent need exists to establish ethical regulations that will protect humanitarian law while upholding human values during AWS deployment.

4.3. Regulation of Autonomous Weapon Systems

The current legal systems fail to control AWS because these systems operate independently. Due to its imprecise definition of human oversight, the UN Convention on Certain Conventional Weapons (CCW) covers some issues but achieves no agreement (ICRC, 2016). States advocate for different approaches regarding military technology autonomy because some states want strict regulations, but others prioritize operational effectiveness. The conflict between human oversight and autonomy represents a worldwide dispute about the proper position of technology within military operations. Advanced technological states stand against strict regulation because they believe enhanced autonomous warfare capabilities lead to better military performance. States focused on human rights and International Humanitarian Law require human involvement for both legal compliance purposes and to prevent violations. According to Verdiesen et al., the regulation of AWS requires robust human oversight because clear guidelines serve to protect against IHL violations. The ICRC supports international cooperation to develop common standards for AWS yet McDougall indicates that technical limitations must be resolved to maintain compliance with IHL. The inability to agree upon specific human intervention standards continues to block effective AWS regulation methods. Modern autonomous technology moves too quickly which renders existing legal frameworks outdated; while preventing them from guaranteeing both International Humanitarian Law compliance and human rights protection in autonomous warfare.

4.4. The Threats and Global Security

The increasing adoption of AWS technologies generates substantial threats to worldwide security. According to Sending Up a Flare (2020), AWS demonstrates dual-use capabilities that non-state actors rogue states and criminal organizations could acquire [41]. The uncontrolled expansion of AWS technologies creates conditions which amplify humanitarian disasters and diminish world peace stability. The rapid expansion of AWS systems creates an important security concern for international stability. Systems controlled by non-state actors may be utilized in ways that break IHL and human rights law. Conflicts will experience increased humanitarian suffering when AWS technology gets deployed to regions without established protections under International Humanitarian Law. Research shows how widespread AWS system deployments create safety risks. The authors at Verdiesen et al., advocate for international governance structures to manage AWS distribution yet Sending Up a Flare (2020) argues global institutions

need to track non-state actors to prevent misuse. The world currently operates without defined regulatory frameworks that would manage the international distribution of AWS technology. International supervision of non-state actors remains absent which allows these technologies to flow freely while creating unpredicted future uses and volatile diplomatic relationships.

5. Discussion

The study explores the accountability frameworks and IHL regulatory structures to examine the challenges of Autonomous Weapon Systems. The constant pace of development of AWS systems results in unpredictable situations. Such as limitless ethical responsibilities the lack of adequate legislation and regulation, and insufficient mechanisms of control. AWS technologies contribute to the development of more perilous international security conditions with their expansion of international operations. This study indicates the necessity of elaborating precise legal norms as well as comprehensive ethical standards and international collaboration frameworks to address these emerging issues.

5.1. Ethical and Accountability Challenges of AWS

The AWS technologies contribute to the distressing international security situations with their increase in international operations. This study outlines the need to formulate concrete legal frameworks, comprehensive ethical standards, and international collaboration protocols to meet these emerging concerns. The analysis reveals that the chasing of accountability gaps is the most important issue interpreted by the research on AWS. An autonomous execution of AWS with no human oversight creates an almost impossible task of attribution for any probable human rights or International Humanitarian Law violations. As an example "In the case of the 'Sentry' project by the US military, accountability became problematic with AWS obtaining autonomy in decision-making that led to civilian casualties, but human commanders were absent from overseeing the actions of the machines." The analysis reveals that tracking responsibility gaps are the most significant critical issue that research uncovers in AWS. Lack of human control over AWS means that finding those responsible for human rights or International Humanitarian Law violations becomes nearly impossible when systems are fully autonomous. Human supervision failures are the primary barriers to identifying the responsible entities during autonomous system misuse or harming events. The vagueness of the definitions of meaningful human control leads to legal ambiguity which denies victims adequate justice while at the same time degrading the IHL compliance system performance.

5.2. Human Control and IHL Compliance

The issues of ethical concern in AWS require similar treatment. Lethal decision-making computer systems pose a risk whenever there is no human moral input involved in the process. Because the lack of moral input leads to prejudice targeting and war desensitization. AWS systems are not capable of assessing human costs from decisions that generate enormous violence and additional suffering as stated by McDougall in 2023. Military conflict zones would grow significantly because IHL compliance does not exist or is limited in these areas and biased algorithms meet human rights violations. While the UN Convention on Certain Conventional Weapons (CCW) attempts to govern AWS, it does not even establish baseline norms for human-machine interactions after adhering to the norms of International Humanitarian Law. The fast-changing nature of technology also slows down the formulation of standard laws because states have no conventions regarding AWS control. For instance, the failure to explain what constitutes 'meaningful human control' in the CCW framework led to instances. In the

course of the conflict in Libya, a fully robotic AWS targeted civilian infrastructure without definitive human control." This example gives a real-world context to how a lack of clearly defined human control translates into operational failures.

5.3. International Humanitarian Law and Regulatory Gaps

The AWS technologies have continued to grow, and the current surge is a significant threat to international security. The increased availability of AWS technology systems creates a great number of security threats that enable non-state actors, and rogue states, criminal organizations to exploit these systems. The lack of international regulations in the framework of global governance would allow for numerous serious violations of IHL and create regional insecurity, and humanitarian crises. This research follows McDougall's and Verdiesen et al.'s position that AWS systems should not have moral reasoning abilities. Two of the ethical issues noted by both research studies are the dehumanization of warfare targets. This means that McDougall military ethics required fundamental changes still Verdiesen emphasizes the creation of such standards that would support AWS's compliance with humanitarian objectives. The study supports Verdiesen et al.'s and the (ICRC's 2016) view on having standard international regulation and collective effort. In 2021, the UN debated the incorporation of AWS into international law but failed to propose a definition of "meaningful human control. Thus, it has further delayed the implementation of a binding treaty. AWS hence becomes one more arena for further regulatory delay, now owing to the lack of an international consensus in favor of its existence.

The study revealed that there are differences in understanding the concept of meaningful human control definitions along with challenges toward international coordination in regulation. These are findings that show that the world requires good legal frameworks to deal with existing issues as evidenced by research findings. The findings of prior studies reveal that modern legal instruments do not allow for addressing the complex challenges that AWS systems entail. The accountability measures are still weak, and there are no agreed human control definitions, which is why AWS system governance remains unsuccessful. The human rights implications of machine-initiated and/or machine-executed lethal operations should be discussed by ethicists right away. The increasing integration of AWS technology systems presents new challenges to global security systems during their deployment around the world. AWS systems that are operational and provide access to non-state actors create multiple security threats that threaten worldwide peace systems.

6. Recommendations

6.1. Closing the Accountability Gap

There are clear expectations under interstate law that provide for human oversight across all AWS systems under AWS. Every functional aspect of the AWS systems requires a human-controlled interface protocol for monitoring the operator's activity. Two new war torts should be created as legislative instruments to define state liability in the event when autonomous warfare systems need to be adjusted beyond recognition. The elements of victim remedies when combined with enhanced accountability tools form a good solution.

6.2. Developing Ethical Guidelines

AWS lethal decision systems require full ethical frameworks as the foundation of their working processes when integrating moral reasoning at the stage of real-life implementation. Active human oversight should protect the operational architecture of AWS platforms because such processes should not be discriminative or de-

humanizing when war is waged. To achieve ethical consistency in the world, the world requires international organizations to devise ethical principles with international jurisdiction.

6.3. Strengthening Regulatory Frameworks

The current international legal systems do not have enough power to regulate the AWS systems operations. It is necessary to include standard operational conditions and compliance with the International Humanitarian Law standards in an international treaty to regulate AWS systems that need human control. International humanitarian law requirements only allow organizations to create AWS system operational procedures where AWS systems are defined as specifically as possible. Such operational standards with international support reflect the most critical priorities that the world community should focus on.

6.4. Mitigating Proliferation Risks

There is a need to have enhanced international architecture to control the security risks that accompany dual-use technology advanced through AWS systems. There is a need for implementation of the global monitoring protocols and export control systems to fight against breaches from rogue state actors and unauthorized non-state actors. The world needs collective action toward the cessation of wars employing AWS technology without undermining security systems in volatile areas. The systemic development of AWS technology challenges institutional control and ethical behavior benchmarks. There are important ethical challenges for autonomous systems that need solutions now and improvements in currently lacking legal frameworks. To preserve and protect human rights the members of the international community should establish general rules regarding AWS deployment that are aligned with the parameters of IHL. These technologies require higher levels of protection protocols and far improved weapons control mechanisms because of their global deployment capabilities. For the international community to get the maximum contributions to global security and peace there is the need to embrace general regulatory standards and ethical rules that eliminate the risks associated with AWS.

7. Conclusion

The scientific study was devoted to the identification of the main legal constraints ethical issues and regulatory challenges that are inherent in Autonomous Weapon Systems (AWS). It remains today's modern warfare system but it is still lacking adequate legal structures to meet new operation needs. Again during this analysis, there is a clear legal vacuum because definitions of AWS system responsibility for human rights abuse and International Humanitarian Law violations are still lacking. The criticism presented significant ethical issues with automated lethal decision systems, which entirely lack compassion and possess low average moral reasoning and human outcomes prediction capacities. The first and foremost risk of fully autonomous operations lies in the fact that it is unclear which organization has to take on the blame for actions initiated by the system. The current insufficient human-operated system capacities to adequately control autonomous processes give rise to AWS governance to proactively shape more legal solutions. The implementation of the globally agreed regulatory frameworks poses significant challenges for the adoption of opposed national positions on human system control. The absence of AWS operational standards leads to ethical issues of discrimination since algorithmic decisions create targets and dehumanise warfare capacities as well as exacerbate human rights abuses through biased actions. The AWS technologies are felt to pose significant threats to global security frameworks due to proliferation risks because of the following:

These technologies have two purposes at once, which pose enormous threats of misuse whenever they are employed by individual actors and non-adherent countries. AWS systems escalate and proliferate because there is no law to govern them and this deviously contributes to undermining regional security by generating more unlawful warfare scenarios that compromise IHL's role in preventing civilian victimization.

This research investigates current AWS regulation methods with emphasis on the UN Convention on Certain Conventional Weapons (CCW) framework. These regulatory frameworks have some implementation issues owing to vague definitions and variable global applications that create unregulated oversight domains. Scholars and academics alike persist in their discussion of the best approach to AWS technology deployment through methods that either rely on human intervention for regulation or methods that entail ethical requirements that require human intervention for risk minimization. Multiple proposed solutions attempt to address the recognized issues. The development of precise human management guidelines for AWS operations by literature should precede international governments' regulatory standards. The development of war torts needs to occur to preserve state liability when human actors are not directly involved. Total ethical frameworks must be developed to allow AWS compliance with human rights obligations and protection of human dignity. Moral reasoning and human monitoring standards must become essential elements for the entire AWS development process beginning with design and extending to deployment stages. AWS technology proliferation needs worldwide agreements and global monitoring organizations to protect systems from unauthorized activities by non-state actors. AWS technologies demonstrate great military potential but need comprehensive ethical rules and regulatory adjustments to sustain their fast development through international collaboration. International standards need development to achieve responsible AWS deployment that upholds International Humanitarian Law standards and safeguards human rights with human dignity. The safe integration of artificial warfare systems requires worldwide military collaboration for developing standardized deployment protocols.

Declaration

Competing Interests: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Consent to Publish: Both authors are agreed to publish version of the manuscript in this journal.

Ethical Issues: There are no ethical issues. All data in this paper is publicly available.

Funding Statement: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Reference

- Benouachane, H., *Cyber Security Challenges in the Era of Artificial Intelligence and Autonomous Weapons*, in *Cyber Security in the Age of Artificial Intelligence and Autonomous Weapons*. 2025, CRC Press. p. 24-42.
- Vrontis, D., et al., *Artificial intelligence, robotics, advanced technologies and human resource management: a systematic review*. *Artificial intelligence and international HRM*, 2023: p. 172-201.
- Seixas-Nunes, A., *The Legality and Accountability of Autonomous Weapon Systems: A Humanitarian Law Perspective*. 2022: Cambridge University Press.
- Anderson, K. and M.C. Waxman, *Law and ethics for autonomous weapon systems: Why a ban won't work and how the laws of war can*. 2013.
- Quince, S., *The laws surrounding responsibility and accountability of autonomous weapons systems are insufficient: An analysis of legal and ethical implications of autonomous weapons systems*. *The Student Journal of Professional Practice and Academic Research*, 2021. **3**(1).
- Malygina, A. and S. Petersburg, *Autonomous Weapon System and Artificial Intelligence: The Problems of Arms Control*.
- Afzal, J., et al., *Review of Various Aspects of Digital Violence*. 2024.
- Shahid, D. and A. Jamil, *ASSESSING MILITARY NECESSITY OF AUTONOMOUS WEAPONS SYSTEMS (AWS) IN ARMED CONFLICTS: A CASE STUDY OF IRAN-ISRAEL*. *Margalla Papers*, 2024. **28**(2): p. 95-118.
- Boothby, W.H., *Weapons and the law of armed conflict*. 2016: Oxford University Press.
- Chengeta, T., *Measuring autonomous weapon systems against international humanitarian law rules*. *JL & Cyber Warfare*, 2016. **5**: p. 66.
- Afzal, J., W. Lumeng, and M. Aslam, *Assessment of tolerance, harmony and coexistence: a study on university students in Government College University, Faisalabad*. *Siazga Research Journal*, 2022. **1**(1): p. 06-10.
- Yongmei, C. and J. Afzal, *Impact of enactment of 'the prevention of electronic crimes act, 2016' as legal support in Pakistan*. *Academy of Education and Social Sciences Review*, 2023. **3**(2): p. 203-212.
- Veel, P.-E.N., *Incommensurability, proportionality, and rational legal decision-making*. *Law & Ethics of Human Rights*, 2010. **4**(2): p. 178-228.
- Horowitz, M.C. and P. Scharre, *MEANINGFUL HUMAN CONTROL in WEAPON SYSTEMS*. 2015.
- Wallach, W. and C. Allen, *Moral machines: Teaching robots right from wrong*. 2008: Oxford University Press.
- Afzal, J., *Implementation of digital law as a legal tool in the current digital Era*. 2024, Springer.
- Afzal, J., *Legal challenges regarding digital operations, in Implementation of Digital Law as a Legal Tool in the Current Digital Era*. 2024, Springer. p. 23-45.
- Afzal, J., *Digital Law Enforcement Challenges and Improvement, in Implementation of Digital Law as a Legal Tool in the Current Digital Era*. 2024, Springer. p. 47-78.
- Afzal, J., *Development of Legal Framework of Digital Laws, in Implementation of Digital Law as a Legal Tool in the Current Digital Era*. 2024, Springer. p. 139-154.
- Amoroso, D. and G. Tamburrini, *The Human Control Over Autonomous Robotic Systems: What Ethical and Legal Lessons for Judicial Uses of AI? New Pathways to Civil Justice in Europe: Challenges of Access to Justice*, 2021: p. 23-42.
- Schoenherr, J.R., *Meaningful Human Control of Autonomous Weapons Systems: Translating Functional Affordances to Inform Ethical Assessment and Design*, in *Cyber Security in the Age of Artificial Intelligence and Autonomous Weapons*. 2025, CRC Press. p. 173-199.
- Rosert, E. and F. Sauer, *Perspectives for Regulating Lethal Autonomous Weapons at the CCW: A Comparative Analysis of Blinding Lasers, Landmines, and LAWS*. Last modified, 2018.
- Crootof, R., *A meaningful floor for meaningful human control*. *Temp. Int'l & Comp. LJ*, 2016. **30**: p. 53.
- Bode, I., et al., *Prospects for the global governance of autonomous weapons: comparing Chinese, Russian, and US practices*. *Ethics and Information Technology*, 2023. **25**(1): p. 5.
- Tzimas, T. and T. Tzimas, *Legal Ramifications of the Use of AWS's - the Role of IHL and Human Rights*. *Legal and Ethical Challenges of Artificial Intelligence from an International Law Perspective*, 2021: p. 167-198.
- Pollard, M.J., *A Legal Framework for Regulating Autonomous Weapon System Deployments*. 2021, The University Of Buckingham.
- Afzal, J. and C. Yongmei, *Federal and provincial legislation regarding 'Right to Information' for good governance in Pakistan*. *Discover Global Society*, 2023. **1**(1): p. 12.
- Margulies, P., *Making autonomous weapons accountable: command responsibility for computer-guided lethal force in armed conflicts*, in *Research handbook on remote warfare*. 2017, Edward Elgar Publishing. p. 405-442.
- Verdiesen, I., F. Santoni de Sio, and V. Dignum, *Accountability and control over autonomous weapon systems: a framework for*

- comprehensive human oversight*. *Minds and Machines*, 2021. **31**(1): p. 137-163.
30. Sparrow, L.A., et al., *Towards Ethical AI Moderation in Multiplayer Games*. *Proceedings of the ACM on Human-Computer Interaction*, 2024. **8**(CHI PLAY): p. 1-30.
 31. Ahmad, I., A. Haider, and B. Zeb, *In the Name of Nature: The Legal Frontiers of Environmental Preservation*. *Journal of Asian Development Studies*, 2023. **12**(4): p. 401-411.
 32. Haider, A., N. Mathlouthi, and I. Ahmad, *Beyond the Books: Real World Challenges in Implementing Environmental Laws in Pakistan*. Available at SSRN, 2024.
 33. Hayes, P., I. Van De Poel, and M. Steen, *Algorithms and values in justice and security*. *Ai & Society*, 2020. **35**: p. 533-555.
 34. Weiss, T.G., *Military-civilian interactions: humanitarian crises and the responsibility to protect*. 2005: Rowman & Littlefield.
 35. Docherty, B., *Completing the package: The development and significance of positive obligations in humanitarian disarmament law*, in *Disarmament Law*. 2020, Routledge. p. 57-79.
 36. Haider, A., I. Ahmad, and M. Yaseen, *Jus Cogens and the Right to Self-Determination: A Study of its Peremptory Status and Erga Omnes Effects*. 2024.
 37. Bradley, M., *Protecting civilians in war: the ICRC, UNHCR, and their limitations in internal armed conflicts*. 2016: Oxford university press.
 38. Scheffler, S., *Boundaries and allegiances: Problems of justice and responsibility in liberal thought*. 2002: OUP Oxford.
 39. Weigend, T., *Convicting Autonomous Weapons? Criminal Responsibility of and for AWS under International Law*. *Journal of International Criminal Justice*, 2023. **21**(5): p. 1137-1154.
 40. Weigend, T., *Convicting Autonomous Weapons?* 2023.
 41. Lay, E. and M. Branlat. *Sending up a FLARE: enhancing resilience in industrial maintenance through the timely mobilization of remote experts*. in *5TH SYMPOSIUM ON RESILIENCE ENGINEERING MANAGING TRADE-OFFS*. 2014.