GLOBAL INTEGRATION OF AI IN MODERN WARFARE: ANALYSING LEGAL VULNERABILITIES TOWARDS HUMAN RIGHTS AMID GEOPOLITICAL ESCALATIONS

Dr. Ausaf Ahmad Malik[*]
Dr. Abhilash Aggarwal[**]

Abstract

The rapid integration of artificial intelligence (AI) into modern warfare, exemplified by autonomous drones in Ukraine and algorithmic targeting in Gaza, heralds a transformative yet perilous era for global security. This study examines how AI's proliferation driven by geopolitical escalations like the US-China arms race and conflicts in Ukraine and Gaza exposes critical vulnerabilities in international humanitarian law (IHL) and international human rights law (IHRL). Through a doctrinal and comparative methodology, analyzing texts like the Geneva Conventions and UN resolutions alongside national policies, the paper identifies accountability gaps in "black box" algorithms, compliance failures in distinction and proportionality, and human rights assaults on life, dignity, and non-discrimination. Geopolitical rivalries hinder binding regulations, fueling proliferation to non-state actors and amplifying civilian harms. Drawing on 2025 reports from Human Rights Watch and UNIDIR, the study proposes a binding UN treaty on lethal autonomous weapons by 2026, mandatory bias audits, strengthened export controls, updated domestic laws and multi-stakeholder coalitions to mitigate risks. Without urgent reforms, AI's unchecked evolution threatens to erode human rights in a volatile world, necessitating a reimagined legal framework to preserve humanity amid technological warfare.

Keywords: Artificial Intelligence, Geopolitical Escalations, Human Rights, International Humanitarian Law Warfare

INTRODUCTION

In the shadowy trenches of Ukraine's frontlines, where the hum of drones has become as ubiquitous as artillery fire, a stark statistic underscores the transformative power of *artificial intelligence* (AI) in modern conflict.[1] Ukrainian tactical drones, increasingly augmented by AI for target recognition and autonomous navigation, are now responsible for inflicting roughly two-thirds of Russian losses, rendering them twice as effective as any other weapon in Kyiv's arsenal.[2] This revelation, drawn from a 2025 analysis by the *RAND* Corporation, exemplifies how AI-driven technologies such as swarming drones that coordinate attacks without constant human input and algorithmic systems that process vast datasets for precision targeting are reshaping warfare.[3] No longer confined to science fiction, these innovations have escalated from isolated experiments to battlefield realities, as evidenced by Ukraine's

[*] Professor, UILS, Chandigarh University, Mohali, Punjab
[**] Assistant Professor, Christ University, Pune

[1]David Kirichenko, "The Rush for AI-Enabled Drones on Ukrainian Battlefields",*Lawfare* (Dec. 5, 2024) *available at:*https://www.lawfaremedia.org/article/the-rush-for-ai-enabled-drones-on-ukrainian-battlefields (last visited on July 21, 2025).

[2]Daniel Boffey, "Killing machines: how Russia and Ukraine's race to perfect deadly pilotless drones could harm us all",*The Guardian*, Jun.25, 2025, section World news.

[3]Zachary Burdette, Dwight Phillips, Jacob L. Heim, *et.al*, "An AI Revolution in Military Affairs? How Artificial Intelligence Could Reshape Future Warfare", *RAND Corporation*, Working Paper No. WR-A4004-1 (June, 2025).

DOI NO. - 10.5958/2582-7529.2025.00001.8

explosive growth in drone production from just six manufacturers in 2022 to over 200 by mid-2025, with projections exceeding 2.5 million units deployed this year alone.[4] Such examples, including Israel's reported use of AI-powered "Lavender" systems to generate 37,000 targets per hour in Gaza operations, highlight not only the tactical advantages but also the profound ethical and legal perils of delegating life-and-death decisions to machines.[5]

At its core, AI in the military context encompasses a spectrum of applications designed to augment or automate human capabilities across diverse domains. This includes intelligence gathering through machine learning algorithms that sift petabytes of surveillance data for patterns[6]; logistics optimization via predictive analytics that forecast supply needs in real-time[7]; cyber operations where AI detects and counters intrusions autonomously[8]; decision-support systems that simulate scenarios for commanders[9] and most controversially, lethal autonomy in weapons like *autonomous weapons systems* (AWS) or "killer robots," which can select and engage targets without meaningful human oversight.[10]

The pace of global adoption has accelerated dramatically, propelled by major powers investing billions in AI militarization. The *United States*, through initiatives like the *Replicator Initiative,* aims to deploy swarms of low-cost, AI-enabled drones to counter adversaries[11], while *China's* "intelligentized warfare" doctrine integrates AI into everything from swarm tactics to command structures.[12]*Russia* and emerging players like *Iran* are similarly advancing, with AI-enhanced drones proliferating in conflicts from *Ukraine* to the *Middle East*, signalling a paradigm shift where technological edge supplants sheer manpower.[13]

Yet, this integration poses a central dilemma i.e., how does the embedding of AI in warfare, especially amid fiercely contested geopolitical landscapes, undermine the efficacy of established *international humanitarian law* (IHL) and *international human rights law* (IHRL) in safeguarding fundamental rights? Core vulnerabilities abound, including accountability gaps in "black box" algorithms that obscure decision-making processes, biases in training data leading to discriminatory targeting and the erosion of IHL principles like ‘distinction’ and ‘proportionality’.[14]*Human Rights Watch*(HRW) in its April 2025 report, "A Hazard to

[4]Mariam Halstian, “A First Point View: Examining Ukraine’s Drone Industry”,*Georgetown Security Studies Review*, 2025, *available at:* https://georgetownsecuritystudiesreview.org/2025/05/15/a-first-point-view-examining-ukraines-drone-industry/ (last visited on July 24, 2025).

[5]EmelieAndersin, “The Use of the ‘Lavender’ in Gaza and the Law of Targeting: Ai-Decision Support Systems and Facial Recognition Technology”, 1 *Journal of International Humanitarian Legal Studies* 1–35 (2025).

[6]Anthony King, “Digital Targeting: Artificial Intelligence, Data, and Military Intelligence,” 9 *Journal of Global Security Studies* ogae009 (2024).

[7]G. SakthiBalan, V. Santhosh Kumar and S. Aravind Raj, “Machine learning and artificial intelligence methods and applications for post-crisis supply chain resiliency and recovery”, 10 *Supply Chain Analytics* 100121 (2025).

[8]Nachaat Mohamed, “Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms”,*Knowledge and Information Systems* (2025).

[9]Anna Nadibaidze, “Do AI Decision Support Systems ‘Support’ Humans in Military Decision-Making on the Use of Force?”,*Opinio Juris*, 2024, *available at:* https://opiniojuris.org/2024/11/29/do-ai-decision-support-systems-support-humans-in-military-decision-making-on-the-use-of-force/ (last visited on July 24, 2025).

[10]Stephen Harwood, “A cybersystemic view of autonomous weapon systems (AWS)”, 205 *Technological Forecasting and Social Change* 123514 (2024).

[11]Miriam McNabb, “The Drones the US Military is Looking for Now”,*Drone Life*, 2025, *available at:*https://dronelife.com/2025/05/07/the-attritable-drone-systems-the-us-military-is-looking-for-now/ (last visited on July 24, 2025).

[12]John Lee, “‘Overtaking on the Curve’? Defense AI in China” in *The Very Long Game* 465–86 (Springer Nature Switzerland, 2024).

[13] Jeremy Julian Sarkin and Saba Sotoudehfar, “Artificial intelligence and arms races in the Middle East: the evolution of technology and its implications for regional and international security”, 40 *Defense & Security Analysis* 97–119 (2024).

[14] Tonni Das Jui and Pablo Rivas, “Fairness issues, current approaches, and challenges in machine learning models”, 15 *Int. J. Mach. Learn. & Cyber* 3095–125 (2024).

DOI NO. - 10.5958/2582-7529.2025.00001.8

Human Rights," warns that AWS risks dehumanizing conflict by reducing individuals to data points, potentially violating rights to life, dignity and remedy under frameworks like the *International Covenant on Civil and Political Rights* (ICCPR).[15] These issues are compounded by the absence of binding global regulations, leaving a patchwork of non-enforceable guidelines that fail to address AI's unpredictability in dynamic environments.

This dilemma is inextricably linked to geopolitical escalations, which serve as both catalysts for AI adoption and barriers to compliance. The 'US-China rivalry' fuels an AI arms race, with export controls on dual-use technologies intensifying proliferation risks, while the 'Russia-Ukraine war' tests AI in real-time attrition battles, and regional flashpoints like Gaza expose algorithmic biases in asymmetric conflicts.[16] Such tensions hinder multilateral efforts, as seen in stalled UN talks on *lethal autonomous weapons* systems (LAWS) in May 2025, where consensus eludes amid vetoes from major powers.[17]

Research Questions

This paper interrogates these dynamics through key research questions:

a. What are the specific applications of AI in modern warfare and how do they impact the conduct of hostilities?
b. Where do existing IHL and IHRL frameworks exhibit vulnerabilities when applied to AI-enabled warfare?
c. How do geopolitical escalations exacerbate these legal vulnerabilities and impede effective regulation?
d. What are the concrete human rights implications arising from these vulnerabilities?
e. What pathways exist for mitigating these risks and strengthening legal resilience?

Ultimately, the rapid global integration of AI into military systems, significantly accelerated by intense geopolitical competition, exposes critical vulnerabilities in the application and enforcement of IHL and IHRL, creating substantial and novel risks to fundamental human rights during armed conflict and security operations, necessitating urgent legal adaptation and strengthened accountability mechanisms.

Research Methodology

This study adopts a doctrinal methodology, rigorously examining primary legal texts such as the Geneva Conventions and Additional Protocols, alongside customary IHL principles, to evaluate AI's integration in AWS and their adherence to norms like distinction and proportionality. Complementing this, a comparative approach contrasts global frameworks like the UN resolutions on lethal autonomous weapons systems with national strategies, including US Department of Defensess directives as against China's "intelligentized warfare" policies, revealing regulatory divergences. Insights are enriched by recent reports, on AI's hazards to human rights, underscoring digital dehumanization and civilian harm risks in

[15] Bonnie Docherty, "A Hazard to Human Rights: Autonomous Weapons Systems and Digital Decision-Making",*Human Rights Watch* (2025).
[16] John Xavier, "The AI arms race gets personal",*The Hindu*, May 17, 2025, section Technology.
[17] Benjamin Perrin, "Lethal Autonomous Weapons Systems & International Law: Growing Momentum Towards a New International Treaty", 29(1)*ASIL Proceedings*(Jan. 24, 2025).

DOI NO. - 10.5958/2582-7529.2025.00001.8

algorithmic targeting. This hybrid framework facilitates a conceptual dissection of legal vulnerabilities amid geopolitical escalations.

LITERATURE REVIEW AND THEORETICAL FRAMEWORK

The scholarly discourse on AI in warfare has evolved rapidly from speculative ethics to urgent policy imperatives, reflecting the technology's swift integration into military operations amid escalating global tensions. Early literature, dating back to the 2010s, focused on the philosophical and ethical quandaries of delegating lethal decisions to machines, but recent works particularly those published in 2025, shift toward empirical analyses of real-world deployments, regulatory gaps, and geopolitical ramifications.

Pioneering voices like *Noel Sharkey* have long anchored the ethical debate on AI in warfare. As a roboticist and co-founder of the *International Committee for Robot Arms Control* (ICRAC), argued that LAWS are not inevitable but pose profound risks to IHL compliance. He critiqued the potential for robots to violate *jus in bello* principles, emphasizing that machines lack the moral agency to discern nuanced human contexts, such as distinguishing combatants from civilians in fluid environments.[18] Sharkey's influence persists in contemporary discussions, as a 2023 *Ethics and International Affairs* article references his call for bans on fully autonomous targeting, underscoring ethical mandates amid technological proliferation.[19]While, *RosBellaby's*2021 study in *Ethics and Behavior* further explores AI's limitations in ethical decision-making, warning that over-reliance on algorithms could erode human accountability in conflict zones.[20] These works laid the groundwork for viewing AI not merely as a tool but as a disruptor of warfare's moral fabric.

Building on this ethical foundation, human rights organizations have produced pivotal reports documenting LAWS tangible harms. HRW, a leading advocate for regulatory controls, released its landmark April 2025 report, dissects how AWS and algorithmic targeting dehumanize conflict. Drawing from incidents in Ukraine and Gaza, the report argues that AI systems risk violating core rights by reducing individuals to probabilistic data points, exacerbating issues like indiscriminate harm and biased outcomes.[21]This builds on HRW's broader *World Report, 2025*, which critiques global failures in upholding human rights amid technological militarization, including AI's role in surveillance and targeting.[22] Complementary analyses from the *International Committee of the Red Cross* (ICRC) and Amnesty International reinforce these concerns, with the ICRC's 2024 position paper emphasizing the need for human oversight to preserve humanitarian protections.[23]

Recent studies extend these critiques into operational and strategic realms. A July 2025 RAND working paper, hypothesizes that AI favors militaries emphasizing mass, deception and network resilience, but warns of escalation risks in peer conflicts.[24] Similarly, the *Center for Strategic and International Studies* (CSIS) June 2025 report, examines AI's biases in

[18] Noel E. Sharkey, "The Evitability of Autonomous Robot Warfare", 94 International Review of the Red Cross No. 886, 787–799 (2012).
[19] Mary Ellen O'Connell, "Banning Autonomous Weapons: A Legal and Ethical Mandate", 37 *Ethics & International Affairs* 287–98 (2023).
[20] Ross W. Bellaby, "Can AI Weapons Make Ethical Decisions?",40*Criminal Justice Ethics* 86–107 (2021).
[21] *Supra* note 15.
[22] Human Rights Watch, *World Report 2025: A Year of Reckoning* 546 (New York, 2025).
[23] Neil Davison, "Autonomous Weapon Systems under International Humanitarian Law" In *UNODA Occasional Papers No. 30* (International Committee of the Red Cross, 2018).
[24] *Supra* note 3.

DOI NO. - 10.5958/2582-7529.2025.00001.8

sensitive applications, advocating for Department of Defense tools to mitigate them.[25]Other publications, such as the *Bulletin of the Atomic Scientists'* article, explore AI's potential to lower conflict thresholds through automated miscalculations[26], while a U.S. Army piece on generative AI poses questions about human roles in evolving warfare.[27] These works collectively illustrate a maturing field, shifting from abstract ethics to evidence-based assessments of AI's battlefield impacts, including drone swarms and predictive analytics in conflicts like Ukraine, where over 2.5 million AI-enhanced drones are projected for 2025 deployment.[28]

Theoretically, this literature is framed through the lenses of IHL and human rights, providing conceptual tools to dissect AI's vulnerabilities. Central IHL principles of 'distinction', 'proportionality' and 'precautions' in attack form the bedrock for evaluating AWS. Distinction mandates separating military targets from civilians, yet AI's reliance on pattern recognition struggles with contextual ambiguity, as noted in a study of 2022 testing AWS compatibility.[29] Proportionality requires balancing anticipated military advantages against civilian harm, a qualitative judgment AI cannot reliably perform due to its "black box" opacity, as analyzed in 2025, advocating operational safeguards.[30] Precautions demand constant care to minimize incidental damage, but autonomous systems may lack the adaptability for real-time reassessment, per *UN General Assembly* reports on LAWS.[31] These principles, enshrined in the Geneva Conventions and Additional Protocols, underscore AI's potential non-compliance, amplified in asymmetric warfare where data biases could systematize discrimination.

Complementing IHL, human rights theories emphasize inherent dignity under the *Universal Declaration of Human Rights* (UDHR) Article 1, which posits all humans as endowed with reason and conscience. AI's dehumanizing effects on treating people as algorithmic inputs threaten this dignity, as *AmandaSharkey* argues in 2018 study on AWS and human worth.[32] The right to life[33]and non-discrimination[34] are similarly imperiled, with HRW's 2025 report linking AI biases to disproportionate impacts on marginalized groups in conflict zones. This framework integrates *jus ad bellum* considerations, questioning AI's role in just war theory amid geopolitical pressures.

Research Gap

Despite these advancements, significant gaps persist, particularly in addressing geopolitical dimensions. Much literature treats AI vulnerabilities in isolation, underemphasizing how

[25] Carol Kuntz, "Artificial Intelligence and War: How the Department of Defense Can Lead Responsibly" In *Strategic Technologies Program Occasional Paper* (Center for Strategic and International Studies, 2025).
[26] Zachary Burdette *et.al*, "Six ways AI could cause the next big war, and why it probably won't", 81 *Bulletin of the Atomic Scientists* 305–12 (2025).
[27]Barlow and Allison Bender, "Innovating Defense: Generative AI's Role in Military Evolution" (*U.S. Army*, Jul. 1, 2025)*available at:* https://www.army.mil/article/286707/innovating_defense_generative_ais_role_in_military_evolution (last visited on July 23, 2025).
[28]"Puja Pandit, "How Drones and AI Are Transforming Conflict",*Vision of Humanity*, Jun. 17, 2025, *available at:*https://www.visionofhumanity.org/technology-and-modern-warfare-how-drones-and-ai-are-transforming-conflict/ (last visited on July 23, 2025)."
[29] Elliot Winter, "The Compatibility of Autonomous Weapons with the Principles of International Humanitarian Law", 27 *Journal of Conflict and Security Law* 1–20 (2022).
[30]Craig Martin, "Autonomous Weapons Systems and Proportionality: The Need for Regulation", 57 *Case Western Reserve Journal of International Law* 255 (2025).
[31] United Nations Secretary General, *Lethal Autonomous Weapons Systems*179, United Nations, UN Doc. A/79/88 (July 19, 2024).
[32] Amanda Sharkey, "Autonomous weapons systems, killer robots and human dignity", 21 *Ethics and Information Technology* 75–87 (2019).
[33] Universal Declaration of Human Rights, 1948, art. 3.
[34] *Ibid*, art. 7.

DOI NO. - 10.5958/2582-7529.2025.00001.8

rivalries like the US-China AI arms race exacerbate them. For instance, US export bans on advanced chips, intensified in 2025, aim to curb China's "intelligentized warfare" doctrine, Beijing's strategy to fuse AI with military command for dominance but have inadvertently accelerated China's domestic innovation.[35]Furthermore, the US-China AI race highlights how these bans fuel proliferation risks, yet few studies integrate this with IHL gaps.[36] Similarly, Russia's AI tactics in Ukraine and Iran's drone exports receive scant comparative attention, overlooking how sanctions and alliances hinder global regulation.[37]This geopolitical myopia limits understanding of how power asymmetries impede treaties, such as stalled UN LAWS negotiations.

These gaps inform the subsequent analysis by framing AI vulnerabilities as not merely technical but geopolitically amplified. The literature's ethical and legal insights reveal how distinction and proportionality falter in AI systems, while human rights theories highlight dignity erosions issues intensified by escalations like export wars and doctrinal rivalries. Moving forward, this paper dissects these dynamics in contemporary conflicts, proposing pathways for resilient frameworks amid global tensions.

TECHNOLOGIES AND TRENDS IN GLOBAL INTEGRATION OF AI IN MODERN WARFARE

The integration of AI into modern warfare represents a seismic shift in military strategy, transforming battlefields from human centric arenas into data-driven ecosystems where algorithms dictate outcomes. As of mid-2025, AI's proliferation across global militaries has accelerated, driven by advancements in machine learning, neural networks and real time processing. This trend is not merely technological, as it is also conceptual, redefining warfare as a hybrid of kinetic force and computational intelligence. According to the AI Index Report from Stanford's *Human Centered Artificial Intelligence* (HAI), of 2025, the global legislative mentions of AI have surged 21.3% since 2023, reflecting heightened awareness of its dual-use potential in defense.[38] Similarly, a *StartUs Insights* analysis identifies AI as a core driver of military innovation, with investments in autonomous systems and connectivity fueling a projected market growth to $29 billion by 2030.[39]

Autonomous 'drones' epitomize AI's frontline role, evolving from remote-operated tools to self-governing swarms that navigate, target and strike with minimal human input. In modern conflicts, these systems leverage computer vision and AI algorithms to process sensor data in real-time, enabling coordinated attacks that overwhelm defenses. Ukraine's drone warfare against Russia exemplifies this, as by mid-2025, over 2.5 million AI-enhanced drones are projected for deployment, accounting for 60-70% of damage to Russian equipment.[40] These

[35] Chris Miller, "How US Export Controls Have (and Haven't) Curbed Chinese AI",*AI Frontiers*, Jul. 8, 2025, *available at:* https://ai-frontiers.org/articles/us-chip-export-controls-china-ai (last visited on July 23, 2025).
[36] Brandon Kirk Williams, "Winning the Defining Contest: The US-China Artificial Intelligence Race", 48 *The Washington Quarterly* 153–71 (2025).
[37] Anton Leitch, "In the Race for AI Supremacy, Can Countries Stay Neutral?,*AI Frontiers*, Jul. 23, 2025, *available at:* https://ai-frontiers.org/articles/in-the-race-for-ai-supremacy-can-countries-stay-neutral (last visited on July 24, 2025).
[38] Nestor Maslej*et. al,Artificial Intelligence Index Report 2025* (Stanford Institute for Human-Centered AI, 2025).
[39] Susi Wallner, "Top 10 Military Technology Trends in 2025",*StartUs Insights*, Mar. 7, 2025, *available at:* https://www.startus-insights.com/innovators-guide/military-technology-trends/ (last visited on July 24, 2025).
[40] SubimalBhattacharjee, "The Evolution of Modern Warfare: How Technology is Transforming the Rules of War", *Natstrat*, Jun. 23, 2025,*available at:* https://www.natstrat.org/articledetail/publications/the-evolution-of-modern-warfare-how-technology-is-transforming-the-rules-of-war-212.html (last visited on July 24, 2025).

"loitering munitions" hybrids of drones and missiles circle battle zones, using onboard AI to identify and engage targets autonomously, as seen in Iran's AI-equipped drones downed by Ukrainian forces in May 2025.[41]Conceptually, this shifts warfare toward "swarm intelligence", where decentralized AI mimics biological flocking to achieve emergent behaviors, outpacing human reaction times. A *Vision of Humanity* report notes that such technologies are transforming conflicts into high-tech testbeds, with 59 state-based wars in 2025, the highest since World War II, amplifying their use.[42]

Predictive analytics further embeds AI in operational planning, using big data and machine learning to forecast enemy movements, logistical needs, and battle outcomes. This application turns vast datasets, from satellite imagery to social media signals, into actionable insights, enabling preemptive strikes and resource optimization. The U.S. Army's *Predictive Analytics Suite*, employs AI to anticipate equipment failures and supply shortages in contested environments, drawing lessons from Ukraine's attrition warfare.[43] In conceptual terms, predictive AI embodies the "OODA loop" (observe, orient, decide, act) on 'steroids', compressing decision cycles from hours to seconds and its integration into theater-scale command, automating planning to enhance adaptability amid electronic jamming.[44]Globally, this trend is evident in the Pacific Air Forces strategic use of data analytics for resiliency.[45]

Cyber-AI hybrids represent the stealthier frontier, blending AI with cyber security to orchestrate digital assaults that complement physical operations. These systems automate threat detection, intrusion countermeasures and disinformation campaigns, creating a seamless "hybrid warfare" paradigm. *Radware's* June 2025 report on the Israel-Iran conflict details how AI-driven cyber attacks, paired with propaganda escalate *psychological warfare*, with Iran responding to Israeli strikes via AI-fueled misinformation.[46] Conceptually, this fusion elevates cyber operations to "cognitive warfare", where AI manipulates information flows to erode enemy morale and public support. A recent U.S. Army study from March-April explores AI-enhanced cyber-information integration, noting its potential to drive national policies without kinetic action.[47] Whereas, cyber security challenges highlight AI's role in sophisticated threats, including state-sponsored attacks.[48]

These applications unfold against a backdrop of intensifying geopolitical rivalries, where AI becomes both a tool and a flashpoint. The US-China AI arms race exemplifies this escalation with U.S. export bans on AI chips, tightened in 2025, aim to curb China's "intelligentized

[41] Ryan Gity, "Artificial intelligence on the battlefield in 2025", *The Jerusalem Post,* Jul. 20, 2025, *available at*: https://www.jpost.com/defense-and-tech/article-861611 (last visited on July 24, 2025).

[42] *Supra* note 28.

[43] Anthony Grajales, "The Predictive Turn: Preparing to Outthink Adversaries Through Predictive Analytics" (*U.S. Army*, Jan. 22, 2025), *available at:* https://www.army.mil/article/282476/the_predictive_turn_preparing_to_outthink_adversaries_through_predictive_analytics (last visited on July 24, 2025).

[44] John Keller, "Home stretch eyed in project to develop large-scale military planning software with predictive analytics",*Military Aerospace*, Jan. 22, 2025, *available at:* https://www.militaryaerospace.com/computers/article/55262215/military-planning-software-using-predictive-analytics(last visited on July 24, 2025).

[45] Wren Fiontar, Data Driving PACAF Strategic Planning", *PACAF Public Affairs*, May 8, 2025,*available at:*https://www.pacaf.af.mil/News/Article-Display/Article/4179176/data-driving-pacaf-strategic-planning/(last visited on July 24, 2025).

[46] Anna Ribeiro, "Radware reports hybrid warfare as cyberattacks, disinformation escalate in 2025 Israel-Iran conflict",*Industrial Cyber*, 2025, *available at:* https://industrialcyber.co/threats-attacks/radware-reports-hybrid-warfare-as-cyberattacks-disinformation-escalate-in-2025-israel-iran-conflict/ (last visited on July 24, 2025).

[47]Russell E. McGuire, Andre Slonopas and Edward Olbrych, "Exploring Artificial Intelligence-Enhanced Cyber and Information Operations Integration" in *Military Review* (U.S. Army University Press, 2025).

[48]WasyihunSema Admass, YirgaYayehMunaye and AbebeAbeshuDiro, "Cyber security: State of the art, challenges and future directions", 2 *Cyber Security and Applications* 100031 (2024).

DOI NO. - 10.5958/2582-7529.2025.00001.8

warfare" doctrine, which integrates AI into command structures for dominance.[49] *Fox News* reports detail how both nations weaponize drones and biotech, with China's projected 1,000-drone divisions per combat unit by 2026.[50] Russia's AI deployment in Ukraine adds another layerof machine-vision drones and autonomous loitering munitions like the 'V2U' have scaled up, navigating jammed environments to strike targets.[51]Similarly, Israel's Lavender system, an AI database for Gaza targeting, processes 37,000 targets hourly with minimal oversight, raising ethical alarms about automated kill lists.[52]These contexts underscore AI as a multiplier of geopolitical tensions, fueling proliferation to non-state actors.

Data from international bodies reinforces this narrative. The UN General Assembly's Resolution 79/62 held in December, 2024 and subsequent informal consultations in May, 2025 urge regulation of LAWS, adopted by 166 votes amid fears of uncontrolled escalation.[53] SIPRI's 2025 Yearbook warns of a new arms race, with AI integration into nuclear and conventional systems exacerbating proliferation risks, estimating 12,241 nuclear warheads globally and highlighting AI's role in dual-use technologies.[54]These reports conceptualize AI as a destabilizer, eroding arms control amid weakened regimes.

However, the benefits of AI integration are compelling, as enhanced precision reduces collateral damage in theory, as AI targets with *superhuman accuracy*; predictive tools optimize logistics, saving lives through foresight and cyber hybrids *bolster defenses* against asymmetric threats.[55] Yet, risks loom large as unintended civilian harms from biased algorithms, as in Gaza's AI strikes causing disproportionate casualties, or escalation via autonomous miscalculations in Ukraine.[56]Thus, AI's potential to alter nuclear escalation, introducing "doomsday scenarios" through an opaque decisions, while balancing these demands urgent governance, as geopolitical rivalries accelerate adoption without safeguards.[57]

LEGAL FRAMEWORKS AND IMPACT ON HUMAN RIGHTS

The advent of AI in warfare has thrust existing legal frameworks into uncharted territory, where traditional principles of international law strain against the opacity and autonomy of algorithmic systems. As of mid-2025, the integration of AI into military operations from AWS to predictive targeting, demands a reevaluation of how these technologies align with established norms. IHL also known as the law of armed conflict, forms the cornerstone of this oversight, primarily through the Geneva Conventions of 1949 and their Additional Protocols

[49] Marina Yue Zhang, "The China-US AI Race Enters a New (and More Dangerous) Phase", *The Diplomat*, May, 16, 2025, *available at:*https://thediplomat.com/2025/05/the-china-us-ai-race-enters-a-new-and-more-dangerous-phase/ (last visited on July 22, 2025).

[50] Morgan Phillips, "AI arms race: US and China weaponize drones, code and biotech for the next great war",*Fox News*, Jul. 23, 2025, *available at:* https://www.foxnews.com/politics/ai-arms-race-us-china-weaponize-drones-code-biotech-next-great-war (last visited on July 20, 2025).

[51] John Hardie, "Ukrainian intelligence details Russia's new V2U autonomous loitering munition",*FDD's Long War Journal* (2025).

[52] Bethan McKernan and Harry Davies, "'The machine did it coldly': Israel used AI to identify 37,000 Hamas targets",*The Guardian*, Apr. 3, 2024, section World news.

[53] *Supra* note 17.

[54]Thomas Reinhold, Elisabeth Hofberger-Pippan and Alexander Blanchard (eds.), *Artificial Intelligence, Non-Proliferation and Disarmament: A Compendium on the State of the Art* (EU Non-Proliferation and Disarmament ConsortiumPaper No. 92, 2025).

[55] Mehmet AkifUzer, "The Integration of AI in Modern Warfare: Ethical, Legal and Practical Implications",*CYIS*, Sept. 24, 2024, *available at:* https://www.cyis.org/post/the-integration-of-ai-in-modern-warfare-ethical-legal-and-practical-implications (last visited on July 18, 2025).

[56] David Kirichenko, "How AI Is Eroding the Norms of War",*AI Frontiers*, May 27, 2025, *available at:* https://ai-frontiers.org/articles/how-ai-is-eroding-the-norms-of-war (last visited on July 21, 2025).

[57] Jeffrey M Kaplow and Ryan A Musto, "Artificial Intelligence and the Future of Nuclear Weapons" In P. Hacker (ed.), *Oxford Intersections: AI in Society* (Oxford University Press, 2025).

DOI NO. - 10.5958/2582-7529.2025.00001.8

of 1977 and 2005. These instruments mandate core principles such as distinction, proportionality and precautions during armed conflict. Yet, as a 2025 ICRC submission to the UN emphasizes, AI's role in decision-making complicates compliance, as systems must interpret these qualitative rules in dynamic environments.[58]*The Martens Clause*, embedded in IHL, invokes principles of humanity and public conscience to fill gaps, but its application to "black box" AI remains conceptually fraught, as machines lack the moral intuition humans possess.[59]

Complementing IHL is IHRL, which applies concurrently in armed conflicts and peacetime operations. Key treaties include the International ICCPR of 1966, safeguarding rights to life[60], privacy[61]and non-discrimination[62]and the *European Convention on Human Rights* (ECHR) of 1950, enforced by the *European Court of Human Rights* (ECtHR). These frameworks demand that AI deployments respect inherent human dignity, as articulated in the UDHR. A 2025 HRW report highlights how AWS erode these protections by dehumanizing targets, reducing individuals to data patterns susceptible to bias and error.[63]

Emerging AI-specific guidelines attempt to bridge these gaps, but they often fall short for military uses. The EU AI Act, effective from August, 2024, classifies AI by risk levels but explicitly excludes systems "exclusively for military, defence or national security purposes",as per article 2(3), regardless of the entity involved.[64] This carve-out, as analyzed in a CETaS explainer in 2025, reflects member states' sovereignty concerns but risks creating regulatory silos, potentially stifling innovation while leaving ethical voids.[65] Similarly, non-binding initiatives like the *U.S. Political Declaration on Responsible Military Use of AI, 2023* and UN General Assembly Resolution 79/62 of 2024 advocate for human oversight, but lack enforcement teeth.[66]

These frameworks, while robust in theory, reveal profound vulnerabilities when confronted with AI's inherent characteristics. Foremost among them are accountability gaps, exacerbated by the "black box" nature of AI algorithms opaque processes where inputs and outputs are visible, but internal reasoning remains inscrutable. Under the *Rome Statute of the International Criminal Court* of 1998, command responsibility[67]holds superiors liable for subordinate's crimes if they knew or should have known of them. However, anAWS disrupts this chain as, if an AI system errs in targeting, attributing intent or negligence becomes elusive, creating an "accountability gap" that shields human operators from scrutiny.[68] It draws parallels to Roman law's agency concepts, proposing oversight models to bridge this void, but warns that without transparency mandates, impunity prevails. On the same lines, the ICC's drafted a policy on cyber-enabled crimes of March, 2025, acknowledging AI's role but omits explicit *mens rea* considerations for autonomous acts, further muddling liability.[69]

[58] International Committee of the Red Cross, "Submission to the United Nations Secretary-General on Artificial Intelligence in the Military Domain and Its Implications for International Peace and Security" In *UN GA Resolution A/RES/79/239*(2025).
[59] Alexander Kmentt, "Geopolitics and the Regulation of Autonomous Weapons Systems", *Arms Control Association*, Jan. 2025, *available at:* https://www.armscontrol.org/act/2025-01/features/geopolitics-and-regulation-autonomous-weapons-systems (last visited on July 25, 2025).
[60] "The International Covenant on Civil and Political Rights," 1966, art. 6.
[61] *Ibid,* art. 17.
[62] *Ibid,* art. 26.
[63] *Supra* note 15.
[64] Artificial Intelligence Act, 2024 (Regulation (EU) 2024/1689).
[65] Rosamund Powell, *The EU AI Act: National Security Implications* (Alan Turing Institute, 2024).
[66] *Supra* note 17.
[67] The Rome Statute of the International Criminal Court, 1988, art. 28.
[68] Marta Bo, "Countering the 'Humans vs. AWS' Narrative and the Inevitable Accountability Gaps for Mistakes in Targeting: A Reply to Kevin Jon Heller", *Harvard National Security Journal Online* (2025).
[69] Office of the Prosecutor, International Criminal Court, "ICC Office of the Prosecutor Launches Public Consultation on Policy on Cyber-Enabled Crimes under the Rome Statute" (The Hague: ICC, Mar. 7, 2025).

DOI NO. - 10.5958/2582-7529.2025.00001.8

Compliance issues compound these gaps, particularly in upholding distinction and proportionality. Autonomous systems, reliant on machine learning, falter in contextual judgment, distinguishing a farmer with a tool from a combatant, or assessing if collateral damage is excessive relative to military gain. Thus, many are advocating for risk-benefit analyses tailored to AWS, categorizing threats to enforce proportionality, yet the current IHL's human-centric assumptions render it inadequate.[70] Further, arguing that AI's probabilistic outputs undermine precautionary obligations, as systems may not adapt to evolving battlefield data. UNIDIR's 2025 report on IHL interpretation for LAWS emphasizes regional divergences, with some states viewing autonomy as enhancing precision, while others decry its unpredictability.[71] These failures risk normalizing indiscriminate harm, violating IHL's foundational ethos.

Human rights assaults manifest vividly through privacy erosion and discrimination. Surveillance AI, integral to *targeting* pipelines, aggregates vast personal data, often non-consensually but *eroding* ICCPR privacy protections. HRW's 2025 analysis links this to 'digital dehumanization', where mass data collection for AWS training invades dignity and enables unchecked profiling.[72]*Discriminatory biases* in algorithms, inherited from skewed training datasets, disproportionately target marginalized groups, amplifying inequalities under IHRL's non-discrimination mandates.[73] Thus, the proposal for bias audits for national security AI, citing predictive policing's racial disparities as a cautionary parallel can be adopted, as justified by the U.S. State Department's 2025 AI risk profile warns of systemic harms, urging safeguards against discriminatory outcomes in military contexts from 2021-2025.[74]

Case Studies

In Gaza, Israel's "Lavender" AI system—processing 37,000 targets hourly with minimal oversight has been implicated in disproportionate civilian casualties, exceeding 55,000 Palestinian deaths by June 2025, per *Gaza Health Ministry* figures.[75] A July, 2025 National investigation reveals algorithmic flaws leading to "data-driven deaths," where biases in input data resulted in erroneous strikes on aid seekers, killing over 1,000 since May 2025 alone.[76] This contravenes distinction and proportionality, as UN experts in 2025 decried AI-enabled "domicide," destroying civilian infrastructure under purported precision claims.[77]

In Ukraine, drone swarms projected at 2.5 million units in 2025, employ AI for autonomous targeting, inflicting 60-70% of Russian losses but raising compliance concerns.[78] A June 2025, *Guardian* report details Russia's counter-AI efforts, where swarms overwhelm defenses but risk civilian misidentification in jammed environments, eroding IHL safeguards amid attrition warfare.[79]

---

[70]Steve Hammerton, "LAWS Need Laws: Distinction and Proportionality in the Age of Autonomy", 3(1) *Student Journal of Information Privacy Law* (2025).

[71] *Supra* note 30.

[72]Leif Monnett, *Sending Up a Flare: Autonomous Weapons Systems Proliferation Risks to Human Rights and International Security* (Geneva Academy of International Humanitarian Law and Human Rights, 2024).

[73] Laurie N. Hobart, "AI, Bias, and National Security Profiling", 40(1) *Berkeley Technology Law Journal*165–232(2025).

[74] U.S. Department of State, *Risk Management Profile for Artificial Intelligence and Human Rights* (Washington, DC, Jul. 25, 2024).

[75]WafaaShurafa and Fatma Khaled, "More than 55,000 Palestinians have been killed in the Israel-Hamas war, Gaza health officials say",*The Associated Press*, Jun.11, 2025, *available at:* https://www.ap.org/news-highlights/spotlights/2025/more-than-55000-palestinians-have-been-killed-in-the-israel-hamas-war-gaza-health-officials-say/ (last visited July on 20, 2025).

[76]"Thomas Harding and NaghamMohanna, "Data-driven deaths: How Israel's AI war machine pinpoints Palestinian victims",*The National*, Jun. 9, 2025, *available at*: https://www.thenationalnews.com/news/mena/2025 /07/09/data-driven-deaths-how-israels-ai-war-machine-pinpoints-palestinian-victims/ (last visited on July 21, 2025)."

[77] Becky Sullivan, "What is 'domicide,' and why has war in Gaza brought new attention to the term?",*NPR*, Feb. 9, 2024, section Middle East crisis.

[78] Vikram Mittal, "Swarming Drones Will Be On The Russian-Ukrainian Battlefield In 2025",*Forbes* (Jan. 2, 2025).

[79] *Supra* note 2.

DOI NO. - 10.5958/2582-7529.2025.00001.8

Geopolitically, these vulnerabilities are amplified by tensions stalling treaties. *The Convention on Certain Conventional Weapons* (CCW) GGE on LAWS, ongoing since 2017, remains stagnant due to consensus-based vetoes from powers like Russia and the U.S., prioritizing military advantages over regulation.[80] A 2025 *Arms Control Association* feature attributes this to US-China rivalry, where export bans on AI chips fuel proliferation without shared norms. UNGA's 2024 resolution for LAWS consultations saw progress in 2025, but geopolitical fissures exacerbated by conflicts in Ukraine and Gaza hinder binding agreements with 'militarism' trumping diplomacy.[81]*Carnegie Endowment's* 2025 analysis urges EU leadership in inclusive frameworks, leveraging its AI Act to counter arms races and promote human-centric standards.[82]

CONCLUSION AND SUGGESTIONS

As the digital age propels AI deeper into the fabric of modern warfare, the findings of this study paint a sobering portrait of a world teetering on the brink of unprecedented ethical and legal upheaval. The global integration of AI, manifests in autonomous drones swarming Ukrainian skies, predictive analytics shaping U.S. military logistics and cyber-AI hybrids fueling disinformation campaigns amplifies vulnerabilities within IHL and IHRL, eroding fundamental protections in a geopolitically volatile landscape. Core principles like distinction and proportionality, enshrined in the Geneva Conventions, falter against AI's "black box" opacity, where algorithmic decisions lack the nuanced judgment humans provide.

Similarly, IHRL safeguards under the ICCPR like rights to life, dignity and non-discrimination, are assaulted by biases in training data and surveillance overreach, as evidenced in conflicts like Gaza, where AI-driven targeting has contributed to disproportionate civilian casualties exceeding 55,000 by mid-2025. These vulnerabilities are not abstract; they manifest in real-world harms, from arbitrary killings via misidentified targets to dehumanization that reduces individuals to probabilistic data points. Geopolitical escalations, particularly the US-China AI arms race and Russia's tactics in Ukraine, exacerbate these issues, fostering an environment where military innovation outpaces regulatory oversight, leading to proliferation risks that extend lethal autonomy to non-state actors.

Conceptually, this erosion represents a paradigm shift, where warfare evolves from human-directed endeavors to algorithm-mediated spectacles, where the volatility of global rivalries marked by export bans, doctrinal divergences like China's "intelligentized warfare" and stalled multilateral talks undermines the universality of human rights. The CSIS June 2025 report, "Artificial Intelligence and War," underscores how biases in sensitive military applications perpetuate discrimination, disproportionately affecting marginalized groups in asymmetric conflicts.[83] UNIDIR's 2025 analysis on AI in the military domain further highlights compliance challenges with IHL, noting that existing frameworks, while robust for conventional arms, struggle with AI's unpredictability, potentially normalizing indiscriminate harm in a world of 59 active state-based conflicts, the highest since World War II.[84] In

[80] *Supra* note 59.
[81] Leila Varella, "To Live Long and Prosper, We Must Ban Autonomous Weapons",2(1) *AWS Diplomacy Report* 7 (WILPF, 2025).
[82] RalucaCsernatoni, "Governing Military AI Amid a Geopolitical Minefield", *Carnegie Europe,* Jul. 17, 2024, *available at:*https://carnegieendowment.org/research/2024/07/governing-military-ai-amid-a-geopolitical-minefield?lang=en&center=europe (last visited on July 23, 2025).
[83] *Supra* note 25.
[84] Kristian Humble, "War, Artificial Intelligence, and the Future of Conflict", *Georgetown Journal of International Affairs* (2024).

DOI NO. - 10.5958/2582-7529.2025.00001.8

essence, AI integration does not merely amplify vulnerabilities; it reframes human rights as collateral in a high-stakes technological contest, demanding a conceptual realignment of law, ethics and strategy to preserve dignity amid chaos.

SUGGESTIONS

The urgency of reform cannot be overstated. Without decisive action, geopolitical escalations will propel unchecked harms, transforming AI from a precision tool into a catalyst for global instability. This study reveals a surge in AI-related incidents, with governance lagging far behind technological advancements, heightening risks in cybersecurity and military domains. While, analysts warn that military AI's accountability gaps could lead to cyber vulnerabilities and loss of human control, as seen in the rising deployment of autonomous systems without adequate legal reviews.[85]

Thus, in a volatile world where nuclear arsenals hover at 12,241 warheads and AI integrates into command structures, the absence of reforms risks doomsday scenarios, where algorithmic errors trigger escalations beyond human remediation. *The World Economic Forum's*, 2025 insights on AI and cybersecurity emphasize assessing vulnerabilities early, yet current trajectories suggest a perilous gap between innovation surges while ethical safeguards stagnate, potentially costing trillions in economic and human terms, as per the Global Peace Index.[86] Reiteration here serves as a clarion call that delay invites catastrophe, where human rights become footnotes in the annals of algorithmic warfare.

To mitigate these perils, concrete solutions must be pursued with vigor such as:

a. Binding International Treaty on Lethal Autonomous Weapons Systems (LAWS)

A cornerstone reform is the establishment of a binding UN treaty on LAWS by 2026, prohibiting systems that operate without *meaningful human control* (MHC). HRW's April 2025 report, "A Hazard to Human Rights," advocates for explicit bans on AWS that fail to uphold IHL principles, such as distinction and proportionality, to prevent digital dehumanization. The UN's 2025, *Governing AI for Humanity* report reinforces this, proposing verification mechanisms akin to nuclear treaties to curb escalation in rivalries like US-China dynamics. Conceptually, this treaty reframes AI as a regulated domain, mandating transparency in algorithmic decision-making to bridge accountability gaps under the Rome Statute and emphasizing risk assessments across the AI lifecycle by ensuring compliance with IHRL and mitigating arbitrary killings in conflicts like Gaza.

b. Mandatory Bias Audits for Military AI Systems

To combat discriminatory vulnerabilities, mandatory independent bias audits should be implemented for all military AI applications, focusing on training data to eliminate prejudices that target marginalized groups. As AI biases as amplifiers of conflict and inequality, recommending fairness metrics and dataset diversification, incorporating cross-border standards, drawing from GDPR-like regulations to enforce corrective measures in biased targeting scenarios has become essential. Conceptually, these audits position AI as a reflective tool of societal equity, requiring ongoing evaluations to align with ICCPR

[85] Davit Khachatryan, "Military AI Challenges Human Accountability", *Center for International Policy*, Jul. 21, 2025, *available at:*https://internationalpolicy.org/publications/military-ai-challenges-human-accountability/ (last visited on July 25, 2025).
[86] World Economic Forum, *Artificial Intelligence and Cybersecurity: Balancing Risks and Rewards* (White Paper Series, 2025).

non-discrimination mandates, enforcing stress integration of such audits to prevent rights erosions in surveillance and predictive analytics.

c. Strengthened Export Controls on Dual-Use AI Technologies

Export controls must be expanded to restrict the flow of dual-use AI such as chips and software, to prevent proliferation to non-state actors amid arms races. This is essential to disrupting technological blocs, extending U.S.-style bans internationally while advocating for WTO compliant mechanisms to reduce spillover into human rights abuses. Conceptually, this reform treats AI as a strategic global asset, fostering cooperation to mitigate risks in volatile regions like the Middle East, where drone repurposing threatens civilians, as without these controls, rivalries will accelerate unchecked harms.

d. Updating Domestic Laws and Directives

National reforms should prioritize updating domestic frameworks, such as revising *U.S. DoD Directive*(3000.09) to enforce MHC and regular legal reviews for AWS, urging "human-in-the-loop" mandates to preserve command responsibility. In the EU, extending AI Act principles to military exclusions could mandate risk assessments. Conceptually, these updates embed ethical oversight into national security, ensuring alignment with IHL and preventing dignity erosions in operations like Ukraine's drone warfare, recommends harmonization to address broader geopolitical strains.

e. Fostering Multi-stakeholder Coalitions

Multi-stakeholder coalitions, comprising governments, tech firms, NGOs and academia should be cultivated to develop shared standards and advocacy. The purpose of these alliances for ethical protocol drafting, as in Diplo's digital diplomacy insights envisions collaborative verification to bridge divides. Conceptually, this reform democratizes AI governance, leveraging diverse expertise to counter militarization and promote human-centric innovations, urgeing corporate disclosure of rights impacts in defense AI.

THE WAY FORWARD

Ultimately, AI emerges as a double-edged sword in global security, as a beacon of precision and efficiency, yet a harbinger of unchecked power and human erosion. The broader implications are profound without reforms, we risk a future where warfare's horrors are automated, rights are algorithmically arbitrated, and geopolitical volatility spirals into existential threats. Yet, with visionary action, AI can be harnessed for humane ends, reinforcing the pillars of international law and affirming our shared humanity in an increasingly digital domain.

Looking to the future, civil society's role in advocacy will be pivotal amid ongoing escalations. Organizations like HRW and Amnesty International must amplify calls for reform, leveraging public campaigns to pressure states into treaty adherence. Grassroots movements, on AI risk-benefit balances, can drive accountability, fostering a culture where citizens demand transparency in military tech. In a world of persistent rivalries, civil society's watchdog function could tip the scales toward ethical AI, conceptualizing advocacy as a counterforce to militarization.

DOI NO. - 10.5958/2582-7529.2025.00001.8