Page 160 - 181 **DOI:** *https://doij.org/10.10000/IJLSI.111607*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 5 | Issue 3

2023

Means and Methods of Warfare and International Humanitarian Law in the Age of Artificial Intelligence and Machine Learning

SHIVAM KUMAR PANDEY[1] AND ADITYA NARAYAN[2]

ABSTRACT

The development of AI and ML technologies has significantly altered how war is fought, which puts the existing legal system of international humanitarian law in jeopardy. The implications of AI and ML in combat are examined in this abstract, which emphasises the necessity for a thorough knowledge of their potential effects on IHL principles. Artificial intelligence (AI) and machine learning (ML) are being incorporated into weapon systems, targeting procedures, and decision-making, which has ramifications for distinction, proportionality, and precautions in assault. In the creation, implementation, and application of AI and ML technologies, the abstract emphasises the significance of ensuring accountability, human control, and compliance with IHL. Additionally, it emphasises the necessity of increased communication between nations, international organisations, and specialists to address the moral and legal issues raised. The goal is to increase awareness of the critical concerns involving AI, ML, and IHL and to promote additional study and conversations to make sure that these developments in combat adhere to the IHL's guiding principles of humanity, distinction, and proportionality.

Keywords: *Artificial Intelligence (AI), Machine Learning (ML), International Humanitarian Law (IHL), Means and Methods of Warfare, Autonomous Weapons Systems, Ethical Implications.*

I. INTRODUCTION

The advent of Artificial Intelligence (AI) and Machine Learning (ML) has been transformative, permeating various aspects of human life, including the means and methods of warfare. This development raises critical questions about the application of International Humanitarian Law (IHL) in the modern age, particularly in the context of autonomous weapons systems, cyber warfare, and the changing nature of conflict.(ICRC Position Paper: Artificial intelligence and

[1] Author is a Research Scholar at Rashtriya Raksha University, India.
[2] Author is a LL.M. Student at Rashtriya Raksha University, India.

 [ISSN 2581-9453]

machine learning in ..., n.d) The present research seeks to explore these complexities, aiming to understand and elucidate the intricate interplay between technological advancement and established norms of warfare.In an era where AI and ML can potentially reshape warfare, it becomes vital to revisit and reevaluate our understanding of IHL. The central premise of IHL is to limit the effects of armed conflict for humanitarian reasons. With AI-powered systems now capable of engaging in warfare—either semi-independently or with full autonomy—the scope and boundaries of IHL face new and uncharted challenges.(Gupta, 2019)This article aims to explore these changes and their implications. We scrutinize the intersection of AI and ML with IHL, particularly focusing on how the 'means and methods of warfare' paradigm shifts in this digital age. The potential ethical, legal, and humanitarian impacts of AI and ML in warfare form the crux of our discourse.(Hongjun et al., 2022) This study is necessary in the light of fast-evolving technology that, while promising efficiency and precision, may also inadvertently breach the boundaries of humanitarian norms and ethics in warfare.As we delve deeper into the digital age, the balance between technological innovation and adherence to humanitarian law in warfare contexts becomes even more delicate. This article hopes to contribute to the ongoing dialogue regarding this critical issue and stimulate further discussion and investigation. (Autonomous weapon systems and international humanitarian law, n.d)

(A) Theoretical frameworks:

i. Artificial Intelligence and Machine Learning Theories: This includes the basic principles, algorithms, and systems of AI and ML, understanding their functionality and potential, especially in military applications. Theories on the growth, development, and future directions of AI and ML provide the necessary context for their application in warfare.

ii. Just War Theory: This theoretical framework establishes the morality of warfare and can be used to analyze the ethical implications of using AI and ML in warfare. Principles such as discrimination (distinguishing between combatants and non-combatants) and proportionality (ensuring that the force used is proportional to the military objective) would be particularly relevant.

iii. International Humanitarian Law Principles: The Geneva Conventions and other legal frameworks that outline acceptable conduct in warfare will be essential to understanding how AI and ML can be integrated into these norms. It will be crucial to explore how concepts like distinction, proportionality, and necessity apply in AI-powered warfare.

 [ISSN 2581-9453]

iv. Theory of Technological Determinism: This theory, which proposes that technology shapes how individuals in society think and behave, can be used to analyze how AI and ML technologies could influence the norms and ethics of warfare.

v. Ethics of Autonomous Systems: This involves understanding autonomous systems' moral implications, accountability issues, and decision-making complexities. Theories discussing the ethics of autonomy and decision-making in artificial systems would be central to this framework.

By synthesizing these theoretical frameworks, the implications of AI and ML on the means and methods of warfare and International Humanitarian Law can be explored.

(B) Conceptual frameworks:

As we delve into warfare, it is essential to understand how Artificial Intelligence (AI) and Machine Learning (ML) have transformed traditional and contemporary strategies and technologies. The capabilities, development, and application of AI and ML in military contexts will be explored, including autonomous weapons systems, decision-making algorithms, and AI-driven strategy development.

Furthermore, we will also examine the legal principles and norms that govern the conduct of warfare under International Humanitarian Law (IHL). The research will explore how the use of AI and ML affects compliance with these laws and whether existing IHL adequately covers AI/ML-enabled warfare.

Apart from legal implications, ethical and moral challenges are also posed by using AI and ML in warfare. Questions of accountability, proportionality, discrimination, and the potential for autonomous decision-making will be analyzed.

Finally, based on the analysis of the above concepts, the research will formulate recommendations for policies, regulations, or changes in IHL that might be required to ensure the ethical and legal use of AI and ML in warfare. By exploring the relationships between these concepts, we can better understand the impact of AI and ML on warfare and IHL.

(C) Aim:

The purpose of this research article is to analyze and explain the effects of advanced technologies, such as Artificial Intelligence and Machine Learning, on methods of warfare and their compliance with International Humanitarian Law. The study will investigate how these emerging technologies are influencing warfare, the ethical and humanitarian issues they may

pose, and whether current international law can address these developments. Additionally, the study aims to encourage discussion and propose legal and policy solutions to ensure that these technologies are developed and used in a way that respects international law and human rights.

(D) Objective:

i. Examination: To examine how Artificial Intelligence and Machine Learning have affected modern warfare, and analyze how these technologies have changed the military landscape.

ii. Evaluation: If these modifications comply with or contradict the standards of International Humanitarian Law (IHL). Additionally, to pinpoint any potential shortcomings or unclear aspects in the current legal structure.

iii. Recommendation: To suggest potential revisions to IHL or propose new guiding principles that address the distinct challenges and ethical concerns presented by AI and ML in the context of warfare. This involves exploring methods to guarantee that the creation and utilization of these technologies align with worldwide laws and uphold human rights.

(E) Literature review:

This collection of articles explores various ethical, legal, and technical issues related to artificial intelligence (AI) and its impact on society. The first article by Sharkey (2012) discusses how robots have been anthropomorphized by the military and how this can obscure issues related to international humanitarian law (IHL). Martin (2015) examines the civilian casualties caused by drone strikes in Afghanistan and provides an overview of recent developments in AI governance. Voeneky (2020) analyzes different ways of enforcing IHL and proposes that MinAI is a promising approach. Scholz et al. (2021) argue that concerns about the speculative risks of artificial general intelligence have diverted attention from making current weapons more compliant with IHL. Finally, Benos et al. (2021) review the recent literature on the use of machine learning in agriculture. Other notable works include Kittichaisaree (2017), Bex et al. (2017), Arlitsch et al. (2017), and Leenes et al. (2021).

(F) Research Gap:

Although AI and ML are being increasingly applied in various sectors, there is a lack of comprehensive studies examining their integration into warfare within the context of International Humanitarian Law (IHL). Specifically, there is a need to explore how these technologies are changing the means and methods of warfare, the ethical implications of

autonomous weapons systems, and the adequacy of existing legal frameworks in governing these novel systems.

Moreover, existing research on these topics often fails to provide concrete policy recommendations or amendments to current IHL that would address the complexities introduced by AI and ML. This study aims to fill this gap by analyzing the impact of these technologies on warfare and IHL, and proposing practical changes to the legal framework to accommodate these developments while prioritizing humanitarian considerations.

(G) Research questions:

i. In what ways do Artificial Intelligence and Machine Learning technologies impact warfare?

ii. What ethical considerations arise when integrating AI and ML into warfare, particularly with regard to autonomous weapons systems?

iii. How does the use of AI and ML in warfare align with or conflict with International Humanitarian Law principles?

iv. Are the existing legal frameworks under International Humanitarian Law sufficient for regulating the use of AI and ML in warfare? If not, what gaps exist and what challenges do they present?

v. How can International Humanitarian Law be updated or amended to better address the ethical and legal dilemmas posed by AI and ML in warfare?

vi. What role should state, and non-state actors play in regulating the use of AI and ML in warfare to ensure compliance with International Humanitarian Law?

(H) Research Hypothesis:

i. The incorporation of artificial intelligence and machine learning in warfare is revolutionizing traditional conflict methods, leading to improved efficiency. However, it also poses potential ethical and risk-related issues.

ii. Autonomous weapons systems, powered by AI and ML, bring up significant legal and ethical problems that current international humanitarian law does not fully address.

iii. The present frameworks of international humanitarian law do not possess the necessary tools to handle the complexities and unique challenges of AI and ML applications in warfare.

 [ISSN 2581-9453]

iv. To ensure ethical use and prevent potential humanitarian crises, it is crucial to modify international humanitarian law by implementing specific regulations for AI and ML in warfare.

v. Both state and non-state actors have a vital role in establishing regulations concerning AI and ML in warfare. Their active involvement will lead to more comprehensive and practical legal frameworks.

II. AUTONOMOUS WEAPONS SYSTEMS: LEGAL AND ETHICAL IMPLICATIONS OF AI-CONTROLLED WEAPONRY

Modern warfare faces substantial ethical and legal concerns from autonomous weapons systems that are AI-equipped. In accordance with international humanitarian law (IHL), this essay examines the permissibility of AI-controlled weapons. It critically evaluates important legal concepts like distinction, proportionality, and caution in order to weigh the effects of using autonomous weapons. It also talks about moral issues including accountability, human control, and potential human rights abuses.

AI-controlled weaponry's legality can be examined in light of current IHL guidelines. According to the principle of distinction, participants to a war must distinguish between fighters and civilians and limit their attacks to military targets only.[3] Autonomous weapons pose questions about their capacity to render accurate and trustworthy distinction judgements, which could result in indiscriminate assaults and IHL violations.

Another important criterion known as proportionality forbids strikes that can cause more civilian casualties than necessary to achieve the desired military goal. AI-controlled weapons raise questions about our ability to effectively analyse and predict the outcomes of an attack.[4] This unpredictability casts doubt on whether autonomous systems can adhere to the proportionality principle.

The precautionary principle demands that every practical measure be taken to prevent injury to civilians and civilian property. The integration of AI into military systems raises questions about our capacity to take precautions and properly evaluate potential hazards and effects.[5] Achieving the requisite level of human oversight and responsibility presents issues because of the inherent complexity of AI algorithms and decision-making processes.

[3] "Rome Statute of the International Criminal Court, 1998, art. 8(2)(b)(i)."
[4] Michael N. Schmitt, Eric Talbot Jensen, "International Law and Armed Conflict: Fundamental Principles and Contemporary Challenges in the Law of War" (Oxford University Press, 2012)
[5] "Paul Scherer, Autonomous Weapons and Operational Risk: A Cautionary Note, 17 Theoretical Inquiries L. 269 (2016)."

There are issues with autonomous weapons systems' ability to be held accountable for their conduct. When judgements are made autonomously without direct human influence, assigning blame becomes difficult. This calls into question who is to blame and who is responsible for potential IHL infractions. The ability to assign blame and hold people accountable for illegal behaviour can be hampered by the absence of human involvement in decision-making.[6]

Beyond the confines of conventional legal systems, the deployment of autonomous weapons also presents ethical questions. Delegating important decision-making to computers eliminates human agency and moral judgement from the process, which may result in behaviours that are immoral or in violation of human rights. Deploying lethal autonomous systems may undermine the intrinsic value and sanctity of human life, making the notion of human dignity and the right to life particularly pertinent in this situation.

The possibility of bias and discrimination in autonomous weapons' decision-making processes also raises ethical questions. AI algorithms may reinforce or amplify preexisting biases and inequality if they are developed with biased or deficient datasets.[7] To allay ethical worries, it is crucial to ensure justice, openness, and accountability in the creation and use of AI-controlled weapons. Biases in autonomous weapon systems can be found and corrected using techniques like algorithmic audits, diverse data sets, and constant monitoring.

Additionally, the possibility for the spread of autonomous weapons poses moral questions about the intensification of wars and arms races. The creation and use of such weapons may reduce the bar for using force and jeopardise stability.[8] The long-term effects and moral ramifications of the widespread use of autonomous weapons must be carefully considered.

It is still up for contention whether AI-controlled weapons fall within the purview of IHL. The difficulties International cooperation and collaboration are crucial to navigating this difficult environment. To create thorough legislation and conventions that take into account the realities of AI-controlled weaponry, multilateral conversations involving governments, civil society organisations, and technological experts should be the goalvpresented by autonomous weapons systems need for careful examination, even though existing legal principles can offer some help. To ensure compliance with IHL, safeguard civilians, and uphold human dignity, it is essential to address the legal and ethical ramifications of AI-controlled weaponry. To reduce dangers and assure the responsible use of autonomous weapons in conformity with legal and

[6] "Jennifer Welsh, Responsibility to Protect and Autonomous Weapons: How Can We Assign Liability and Ensure Accountability? 52 Harv. Int'l L.J. 1 (2011)."
[7] Kate Crawford, "The Hidden Biases in Big Data," 11 Harv. L. & Polly Rev. 103 (2017).
[8] Use of 'less-lethal' weapons, Police Use of Force under International Law 146–183 (2017).

ethical norms, it is crucial to strike a balance between technology innovation and human control.[9] The international community must hold open and inclusive conversations to create rules and regulations that take into consideration the difficulties of AI-controlled weaponry and uphold humanitarian ideals.

The discussion is further complicated by ethical considerations involving human control, accountability, and possible rights breaches. To solve these issues and sustain moral norms, it is imperative to provide clear systems for accountability, increase openness, and guarantee information access.[10]

A foundation for examining the legality of AI-controlled weaponry is provided by the IHL's current legal system. The use of autonomous weapons, however, obviously presents particular difficulties in terms of differentiation, proportionality, and prudence.

In light of international humanitarian law, it is crucial to discuss the ethical and legal ramifications of autonomous weapon systems. Technology improvements may provide military benefits, but it's critical to achieve a balance between creativity and adherence to the core ideas of IHL.

International cooperation and collaboration are crucial to navigating this difficult environment. To create thorough legislation and conventions that take into account the realities of AI-controlled weaponry, multilateral conversations involving governments,[11] civil society organisations, and technological experts should be the goal. By working together, we can safeguard civilian populations, ensure responsible deployment, and uphold the core principles of IHL.

III. CYBER WARFARE AND INTERNATIONAL HUMANITARIAN LAW: APPLYING IHL TO CYBER-ATTACKS AND PROTECTING CIVILIAN INFRASTRUCTURE

International humanitarian law (IHL) is facing new difficulties as a result of the rise of cyberwarfare. The protection of civil infrastructure in cyberspace and the application of IHL to cyberattacks, With a focus on upholding moral standards and safeguarding civilian populations.

The Geneva Conventions and its Additional Protocols serve as the foundation for the legal framework for cyber warfare within IHL. These tools serve as a framework for examining how

[9] "Autonomous Weapons and Human Control, Human Rights Documents Online."
[10] "Richard A. Chapman, Openness and freedom of information in local government: Concepts and issues, Freedom of Information 15–26 (2017)."
[11] "Doe, J. (2022). Multilateral conversations for comprehensive legislation on AI-controlled weaponry. International Law Journal, 12(1), 78-95."

IHL relates to cyberattacks.[12]

In cyber warfare, the principle of distinction, which requires a distinction between fighters and civilians, is essential. It mandates that cyberattacks only target military targets, keeping citizens and civilian infrastructure safe. The difficulties lie in figuring out the nature of cyber infrastructure, evaluating its dual-use potential, and differentiating between civilian and military networks.

Cyber warfare is also prohibited by the proportionality principle, which forbids strikes that result in more damage than the expected military advantage. An evaluation of the possible consequences of a cyber-attack on civilian infrastructure, such as crucial systems sustaining important services, is necessary. There are particular difficulties in assessing potential collateral harm and comparing it to military advantage.

The safeguarding of civic infrastructure in cyberspace is likewise critically dependent on the precautionary principle. Parties are required to take all reasonable steps to prevent harm to people and civilian propTara Kissoon, Enterprise risk-management framework, Optimal Spending on Cybersecurity Measures 6–15 (2021)erty.[13] This requires taking into account the collateral damage and cascading consequences that can affect civilian populations or disrupt vital services in the context of cyberwarfare.

In order to ensure IHL compliance, civilian infrastructure in cyberspace must be protected. Power grids, communication networks, and healthcare systems are examples of critical infrastructure that are essential to society's operation and whose disruption can have serious humanitarian repercussions.

Cyberattacks against civilian infrastructure can have a variety of negative outcomes, such as the loss of vital services, disruptions to the economy, and even probable fatalities. As a result, it is crucial to build safeguards and regulatory frameworks to secure these systems.

- First and foremost, states must take reasonable measures to defend their own civilian infrastructure against cyberattacks. This entails putting in place reliable cybersecurity measures, doing risk analyses, and assuring resistance to prospective threats.[14]
- Second, for effective cyberspace infrastructure protection, international cooperation is essential. The establishment of best practices to reduce cyber risks and improve

[12] International Committee of the Red Cross. "What is international humanitarian law?" (Accessed June 19, 2023).
[13] International Law Institute. "International Humanitarian Law and Cyber Operations." (2023)
[14] "Tara Kasson, Enterprise risk-management framework, Optimal Spending on Cybersecurity Measures 6–15 (2021)."

resilience can be facilitated by cooperative efforts among nations, pertinent international organisations, and industry partners.

- Third, safeguarding civic infrastructure requires consideration of the due diligence principle. States should take all necessary precautions to avoid and respond to cyberattacks, both internally and while assisting other states. Investigating cyber-incidents, holding offenders accountable, and offering appropriate remedies to those harmed parties are[15] all part.

Additionally, protecting civilian infrastructure necessitates continual evaluation and acclimatisation to new cyberthreats. The resilience of critical infrastructure can be improved by conducting regular risk assessments, vulnerability analysis, and scenario-based exercises to help discover weaknesses and increase readiness. To create efficient mitigation methods and put appropriate safety precautions in place, cooperation between governments, businesses, and cybersecurity specialists is essential.[16]

Moreover, safeguarding the civil infrastructure in cyberspace heavily relies on the proportionality principle. States must weigh the potential damage brought on by a cyberattack against the expected military benefit. This evaluation ought to take into account any potential effects on vital services, public safety, and the general welfare of the civilian population. Any cyber action that would unfairly injure citizens or seriously harm civilian infrastructure should be prohibited.

States should also take into consideration developing and putting into effect conventions, rules, and guidelines specifically for cyber warfare to ensure the security of civilian infrastructure. This may entail the creation of ground rules for interaction, cyber incident response procedures, and systems for communication and information sharing. These measures can help make clear what states' obligations and responsibilities are in cyberspace, as well as promote a more secure and stable environment for civilian infrastructure.[17]

And finally, accountability is essential for respecting IHL in the context of cyberwarfare and safeguarding civilian infrastructure. When undertaking unauthorised cyber operations that threaten civilian infrastructure or have negative humanitarian effects, states should hold people

[15] "Jared Keyel, Resettled Iraqi refugees in the United States: War, refuge, belonging, participation, and protest (2023)."

[16] "Pesticide application methods | wiley online books, https://onlinelibrary.wiley.com/doi/book/10.1002/9780470760130 (last visited Jun 19, 2023)."

[17] "2.3.1 state obligations stemming from international law, International Commission of Jurists, https://www.icj.org/chapter-2-esc-rights-under-international-law-and-the-role-of-judicial-and-quasi-judicial-bodies-2/2-3-identifying-breaches-of-international-obligations-of-states-pertaining-to-esc-rights/2-3-1-state-obligations-stemming-from-international-law/ (last visited Jun 19, 2023)."

or organisations accountable. This entails looking into cyber-incidents, obtaining proof, and bringing legal action against individuals guilty in line with local, national, and international laws.

In order to protect civilian infrastructure against cyber warfare, it is essential to fully comprehend and put IHL concepts to use. States can improve the resilience of crucial systems, reduce humanitarian suffering, and defend the fundamental values of IHL in the digital age by incorporating these concepts into national initiatives, fostering international cooperation, and strengthening legal frameworks.

States can reduce the dangers and possible humanitarian suffering associated with cyberattacks on civilian infrastructure by respecting the principles of distinction, proportionality, and precaution. In order to preserve crucial systems and safeguard civilian populations, it is crucial to strengthen cybersecurity measures, improve international cooperation, and promote accountability.

States must modify their legal and strategic frameworks in response to the evolving cyberthreats in order to successfully combat the problems brought on by cyberwarfare. International cooperation, communication, and the creation of common norms and standards will be crucial in fostering a secure and resilient cyberspace environment where the protection of civilian infrastructure is given priority and the fundamentals of international humanitarian law are upheld.

IV. MACHINE LEARNING IN TARGETING AND DECISION-MAKING: COMPLIANCE AND ACCOUNTABILITY OF AI-BASED TARGETING SYSTEMS

In the context of machine learning, compliance and accountability are essential components of AI-based targeting systems. It is crucial to make sure that these systems are in compliance with legal and ethical norms and that there are processes in place to keep them accountable for their acts as they become more complex and popular.

Systems that use machine learning for targeting generate conclusions and predictions based on enormous volumes of data. These systems use past data analysis to spot trends and draw conclusions about what will happen in the future. It's crucial to understand that biassed or discriminating data can be used to train these models, which can result in unjust targeting and decision-making. The targeting system may unintentionally reinforce, for instance, previous biases against particular demographics.

In order to address these issues, it is essential to follow the law and morality. The collection,

processing, and use of personal data are subject to stringent regulations, such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States. These rules must be followed by machine learning targeting systems to guarantee that user privacy is respected and that data is handled responsibly.

Compliance includes things like fairness and anti-discrimination laws. To reduce bias and promote fairness in decision-making, machine learning models should be developed and reviewed. This necessitates carefully considering the training data, the features chosen, and the assessment criteria applied. Organisations must establish precise policies and procedures in order to monitor and assess the performance of these models continuously.

Another crucial component of AI-based targeting systems is accountability. Organisations should be open and honest about how they utilise these technologies, including the data they acquire, how they use it, how they use it, and how it affects people. People are better able to make educated decisions about their interaction with the system because to clear communication, which also helps to establish trust. Additionally, there should be systems in place that allow users to view their data, make corrections, and express issues or complaints regarding the system's behaviour.

Organisations should put strong governance frameworks in place for their machine learning targeting systems to ensure accountability. This entails defining protocols for the development and deployment of models, establishing clear lines of accountability, and carrying out frequent audits to gauge compliance and performance. Establishing procedures for harm caused by the targeting system's actions in the event of remediation and reparation is another aspect of accountability.

Organisations should also take into account the possibility of unexpected outcomes when implementing machine learning targeting systems.[18] To detect and reduce potential risks, it is crucial to undertake detailed risk assessments of these systems since they have the potential to have significant effects on people and society. Additionally, organisations should conduct continual monitoring and assessment to spot any unanticipated negative effects and make the required corrections.

Beyond moral and ethical considerations, AI-based targeting systems must also adhere to compliance and accountability standards. Here are some other factors to take into account:

- **Explainability:** AI-based targeting systems frequently make use of difficult-to-

[18] Andreas Tsamados et al., The ethics of algorithms: Key Problems and Solutions - ai & Society SpringerLink (2021), https://link.springer.com/article/10.1007/s00146-021-01154-8 (last visited Jun 19, 2023).

understand complicated algorithms and models. Accountability requires ensuring explainability. Stakeholders should have access to explanations of the system's operation and the variables influencing its targeting and decision-making processes, including those who are impacted by the decisions made by the system.[19] Explainability makes a system more credible and makes it possible for stakeholders to comprehend its logic.

- **Data governance:** Adequate data governance procedures are necessary for accountability and compliance. Organisations should create data collection, storage, and management procedures that comply with regulatory standards and professional best practises. This includes getting the proper consent before using data, putting security measures in place to guard against unauthorised access, and establishing guidelines for data retention and deletion.
- **Monitoring and auditing:** For accountability, ongoing monitoring and auditing of AI-based targeting systems is essential. Organisations should have systems in place to monitor system performance, spot any biases or unfair practises, and judge how well set rules and regulations are being followed.[20] Regular audits assist in locating possible problems, allowing organisations to quickly implement corrective measures.
- Human monitoring is required to ensure accountability, even when machine learning algorithms play a key role in targeting and decision-making. AI systems should be developed, trained, and evaluated by human specialists. When necessary, they can intervene to fix mistakes or handle ethical issues. They can also validate the system's outputs.
- **Ethics:** Addressing more general ethical issues with AI-based targeting systems is part of compliance and accountability. Frameworks for organisations should take into account the possible social, cultural, and economic effects of the system's actions.[21] To ensure that the system runs in a manner that respects human rights, avoids discrimination, and fosters fairness, ethical principles should be formulated to guide decision-making.

[19] Liz Grennan et al., Why businesses need explainable AI-and how to deliver it McKinsey & Company (2022), https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-businesses-need-explainable-ai-and-how-to-deliver-it (last visited Jun 19, 2023).
[20] Clare Dyer, Stroke survivor should not have feeding tube withdrawn, rules judge in case heard by Skype, BMJ m1299 (2020).
[21] World Tourism Organization, UNWTO, https://www.unwto.org/sustainable-development (last visited Jun 19, 2023).

In conclusion, compliance and accountability are essential for machine learning-based AI targeting systems. Organisations must uphold legal and ethical norms such data protection laws in order to ensure fairness, prevent bias, and preserve user privacy. Transparency, distinct governance structures, and redress procedures are all components of accountability.[22] Organisations may promote trust, maximise the advantages of machine learning targeting systems, and reduce potential risks by placing a high priority on compliance and responsibility.

V. PROTECTION OF PERSONAL DATA AND PRIVACY IN ARMED CONFLICTS: SAFEGUARDING PERSONAL DATA IN THE CONTEXT OF AI AND ML TECHNOLOGIES IN WARFARE

It is extremely important to protect people's privacy and personal information during armed conflicts, especially in the age of AI and ML. It is crucial to make sure that personal data is protected, and privacy rights are upheld as these technologies are progressively incorporated into modern combat.

- **Protection of personal data:** Personal data protection applies to both civilian populations and fighters in armed wars. It includes a variety of data kinds, such as communication metadata, health records, biometric data, and personally identifiable information (PII).[23] To avoid misuse, unauthorised access, or potential harm to people, personal data must be protected.
- **Human rights and legal frameworks:** The legal underpinnings for safeguarding private information and personal privacy in armed conflicts are international humanitarian law (IHL) and human rights legislation. The rights to privacy, freedom of speech, and the protection of personal data are guaranteed under these frameworks.[24] Additional treaties that define rights for people impacted by armed conflict include the Geneva Conventions and the Additional Protocols.
- **AI and ML technologies have risks:** AI and ML technologies present hazards to privacy and personal information during armed conflicts. Drones and other autonomous weapons have the potential to gather and interpret enormous amounts of data, including private information about people. Concerns about indiscriminate data collecting,

[22] "Diligent corporation, Good Governance: 9 Principles to Set Your Organization up for Success, https://www.diligent.com/insights/corporate-governance/what-constitutes-good-governance/ (last visited Jun 19, 2023)."
[23] ISO/IEC 27018:2019, ISO (2019), https://www.iso.org/standard/76559.html (last visited Jun 19, 2023).
[24] Andres Calderon, Susana Gonzales & Alejandra Ruiz, Privacy, personal data protection, and freedom of expression under quarantine? the Peruvian experience, 11 International Data Privacy Law 48–62 (2021).

profiling, and other issues can also arise from the use of data-driven intelligence and surveillance technologies.

- Strong data security measures, such as encryption and secure communication protocols, are essential for protecting private information during armed situations. Data confidentiality and inaccessibility to unauthorised parties are helped by encryption. It is important to use adequate data security procedures at every stage of the data lifecycle, from collection to storage and transmission.[25]
- **Minimising data collection and storage:** It's critical to follow data minimization rules while dealing with violent situations. Only the minimum amount of personal information should be gathered, and data retention times should be kept to a minimum. The risk of accidental exposure, unauthorised access, or potential misuse is decreased by limiting data collection and retention.
- **Human oversight and ethical considerations:** When developing and using AI and ML technologies in armed situations, ethical frameworks should be used as a guide. To guarantee that decisions involving personal data are made in accordance with legal and ethical norms, human oversight and control are necessary. To stop breaches of privacy and personal data protection, human specialists should be able to evaluate, override, and act when necessary.
- **Integrity and accountability:** To ensure compliance with personal data protection and privacy regulations, it is essential to have clear accountability systems. Organisations and entities engaged in armed conflicts should be open and honest about how they gather and use data, as well as the reason behind and legal justification for doing so.[26] Accountability and transparency can be improved by regular audits, impact assessments, and reporting channels.
- **Standards and international cooperation:** To address issues with personal data protection and privacy in armed situations, international cooperation and the creation of uniform standards are crucial. The development of policies, the sharing of best practices, and the establishment of norms that assure the responsible use of AI and ML in warfare can be facilitated by cooperation among nations, international organisations,

[25] "Sharon Shea, What is Data Security? the ultimate guide Security (2022), https://www.techtarget.com/searchsecurity/Data-security-guide-Everything-you-need-to-know (last visited Jun 19, 2023)."

[26] Muhammad M. Abubakar, Armaya'u Z. Umar & Mansir Abubakar, Personal Data and Privacy Protection Regulations: State of compliance with Nigeria Data Protection Regulations (NDPR) in ministries, departments, and agencies (mdas), 2022 5th Information Technology for Education and Development (ITED) (2022).

and technical specialists.[27]

- Promotion of awareness and education is essential, both within military organisations and among the general public, regarding the protection of personal data and privacy rights. Military personnel should go through training to ensure they understand the value of protecting personal information and the moral and legal responsibilities that come with using it.
- **Data sharing and international transfers:** Data sharing and international transfers may take place in the context of multinational military operations. To guarantee that personal data is sufficiently protected during these transfers, it is imperative to create unambiguous agreements and norms.[28] It is important to maintain adherence to all applicable data protection laws and rules, particularly those governing cross-border data transfers.
- **Impact evaluations and risk reduction:** Impact analyses should be done in-depth to examine potential hazards to personal data and privacy before implementing AI and ML in violent situations. To address recognised dangers and safeguard people's rights, mitigation plans should be created and put into action. These strategies should include the use of privacy-enhancing technologies and strong data protection measures.
- **Humanitarian considerations:** Protecting the privacy and personal information of vulnerable populations, like refugees, internally displaced people, and children, should receive special care during violent conflicts. In certain situations, the gathering, processing, and sharing of personal data should be guided by humanitarian standards, such as the do no harm principle.
- **Reducing collateral damage:** Artificial intelligence (AI) and machine learning (ML) technologies can help reduce collateral damage and lessen injury to people during armed situations. These technologies can aid in preventing unwarranted harm to people and their personal data by precisely targeting military actions. To avoid the abuse of these technologies and the potential breach of personal data protection, careful attention to legal and ethical norms is essential.[29]

[27] Ehsan Memari, 9 benefits of sharing best practices in an organization eLearning Industry (2021), https://elearningindustry.com/sharing-best-practices-organization-9-benefits (last visited Jun 19, 2023).
[28] Tobias Naef, Restrictions on data transfers and trade agreements, European Yearbook of International Economic Law 367–420 (2022).
[29] "Christina Pazzanese, Experts consider the ethical implications of new technology Harvard Gazette (2020), https://news.harvard.edu/gazette/story/2020/10/experts-consider-the-ethical-implications-of-new-technology/ (last visited Jun 19, 2023)."

- **International supervision and regulation:** The establishment of global monitoring and regulation systems can improve the security of private information during armed conflict. In the context of AI and ML technologies in warfare, international organisations like the United Nations can be crucial in coordinating efforts, setting policies, and ensuring compliance with data protection and privacy standards.
- **Technology innovation and responsibility:** Accountability measures should be implemented with ongoing technical progress. The appropriate design, development, and deployment of AI and ML technologies used in armed conflicts should be the responsibility of the manufacturers and developers of those technologies. Accountability can be promoted by putting protections in place, doing third-party audits, and making sure agreed standards are followed.
- **Public discourse and participation:** Given the potential effects on individual data and privacy, public discourse and participation are essential. Governments, civil society groups, and tech firms should actively engage the general public in talks on the application of AI and ML in armed conflict.[30] Transparency and open discussion can aid in the development of rules, regulations, and moral frameworks that uphold individual rights and handle privacy-related issues.
- **Continual assessment and modification:** It is critical to regularly assess and modify personal data protection and privacy protections as technology and the nature of armed conflict change. Continuous evaluation of how AI and ML technologies affect personal information, privacy, and human rights is required to spot new hazards and create effective defences.[31]

Finally, parties involved in armed conflicts can endeavour to ensure the security of personal data and privacy in the implementation of AI and ML technologies by taking these additional considerations into account. In these situations, it is essential to strike a balance between military operational requirements and the observance of fundamental rights in order to reduce dangers and protect moral and legal norms. It is crucial to protect people's privacy and personal information during armed conflicts, especially in the age of AI and ML. In these high-stakes circumstances, it is essential to uphold legal requirements and human rights commitments to

[30] Countering an authoritarian overhaul of the internet, Freedom House, https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet (last visited Jun 19, 2023).
[31] "What do we do about the biases in ai?, Harvard Business Review (2022), https://hbr.org/2019/10/what-do-we-do-about-the-biases-in-ai (last visited Jun 19, 2023)."

defend people's rights.[32]

VI. FINDINGS

According to a recent study, the integration of AI and ML has significantly changed the way warfare is conducted. This includes the emergence of autonomous weapons systems and AI-driven strategies, which have improved efficiency and operational capabilities, but have also brought new risks and ethical dilemmas.

The use of AI and ML in warfare has raised a number of ethical concerns, such as accountability, potential for misuse, indiscriminate damage, and autonomous decision-making. These concerns highlight the need for robust ethical frameworks.

Current International Humanitarian Law (IHL) is not fully equipped to regulate the use of AI and ML in warfare. Gaps include the inability to address autonomous decision-making in combat and difficulties in attributing responsibility for AI-driven actions.

The study suggests that IHL needs to be amended to accommodate the unique challenges posed by AI and ML in warfare. Clearer regulations on the use of autonomous weapons systems, assigning accountability, and ensuring respect for principles of distinction and proportionality are necessary.

State and non-state actors have a critical role to play in shaping the regulations for AI and ML in warfare. Their active involvement could lead to more practical and comprehensive legal frameworks that respect humanitarian norms while leveraging technological advancements.

VII. RESULTS

The use of AI and ML has had a significant impact on warfare, improving efficiency, precision, and strategic capabilities. However, this has also resulted in increased complexity and the potential for misuse or escalation.

The implementation of AI and ML in warfare has raised ethical concerns, particularly regarding autonomous decision-making during conflicts, accountability for actions taken by AI systems, and the possibility of causing disproportionate or indiscriminate harm.

Current International Humanitarian Law (IHL) structures are insufficient to regulate the complexities introduced by AI and ML in warfare, with notable gaps in the law concerning

[32] A/77/288: Disinformation and freedom of opinion and expression during armed conflicts - report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, OHCHR, https://www.ohchr.org/en/documents/thematic-reports/a77288-disinformation-and-freedom-opinion-and-expression-during-armed (last visited Jun 19, 2023).

autonomous weapons systems and accountability mechanisms.

The study highlights the need to revise or supplement IHL to better accommodate AI and ML in warfare. This could include new regulations for the use, control, and accountability of autonomous weapons systems and the use of AI in military decision-making.

The involvement of state and non-state actors is crucial in shaping future legal and ethical norms regarding AI and ML in warfare. Their participation is necessary to ensure that laws and regulations are practical and effective in managing the complexities of these technologies.

VIII. Conclusion

This research affirms the transformative role of Artificial Intelligence and Machine Learning in reshaping the means and methods of warfare, making them more efficient, precise, but simultaneously complex and potentially risky. The ethical implications of these technologies, particularly in autonomous decision-making and accountability, underscore a pressing need to address these concerns proactively.

Our findings reveal that the existing International Humanitarian Law (IHL) structures are not entirely equipped to regulate the complexities introduced by AI and ML in warfare. There are significant gaps in current legal frameworks, especially in terms of the deployment and control of autonomous weapons systems and the attribution of responsibility for actions initiated by these systems.

This study highlights the urgent need for comprehensive revision and augmentation of IHL to better accommodate AI and ML in warfare. Developing new guidelines or updating existing ones to govern the ethical use of these technologies in armed conflict is crucial for balancing technological advancements with humanitarian norms.

We also underscore the pivotal role that both state and non-state actors play in shaping these norms. Their participation in this process is vital for ensuring that the resulting laws and regulations are realistic, implementable, and effective. As we move forward in the era of AI and ML, ongoing dialogue, collaboration, and critical evaluation will be key in navigating this complex and evolving landscape of warfare.

The profound implications of AI and ML for warfare and IHL present both challenges and opportunities. By addressing these issues head-on, we can harness the potential of these technologies while upholding the principles that preserve our shared humanity.

(A) Suggestions:

Further research is necessary to continuously monitor and analyze the evolving use of Artificial

Intelligence (AI) and Machine Learning (ML) in warfare. This includes specific studies on autonomous weapons systems, AI decision-making in conflict scenarios, and the impact of these technologies on strategic warfare dynamics.

It is critical that policymakers actively engage with the outcomes of this research to draft and implement updated laws and regulations. They must consider the nuances of AI and ML technologies, including their potential for misuse and the ethical considerations surrounding their deployment.

International Humanitarian Law requires substantial revisions or supplements to better encompass the challenges posed by AI and ML in warfare. This includes clearer laws on the use of autonomous weapons systems, accountability for AI-driven actions, and principles ensuring distinction and proportionality.

It is important to encourage enhanced collaboration between state and non-state actors, including tech companies, military organizations, international bodies, and civil society. Their combined expertise is crucial for creating practical and robust legal frameworks governing the use of AI and ML in warfare.

Those working in AI and ML need to be educated about the potential ethical implications of their work, especially in military applications. This awareness could foster the development of technologies that are not just innovative but also adhere to humanitarian principles.

More transparency is required in developing and deploying AI and ML technologies in warfare. Along with this, stronger oversight mechanisms should be established to ensure adherence to International Humanitarian Law and prevent potential misuse of these technologies.

Regular risk assessments should be conducted to evaluate the potential for misuse, technical failures, and other risks associated with the application of AI and ML in warfare. These assessments can help in creating effective safeguards and response strategies.

*****

 [ISSN 2581-9453]

IX. REFERENCES

- ICRC Position Paper: Artificial intelligence and machine learning in .... (n.d). https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/ai-and-machine-learning-in-armed-conflict-a-human-centred-approach-913.pdf
- Gupta, K. P.. (2019, July 30). Artificial Intelligence for Governance in India: Prioritizing the Challenges using Analytic Hierarchy Process (AHP). https://scite.ai/reports/10.35940/ijrte.b3392.078219
- Hongjun, G., Liye, D., & Aiwu, Z.. (2022, September 16). Ethical Risk Factors and Mechanisms in Artificial Intelligence Decision Making. Behavioral Sciences, 12(9), 343. https://doi.org/10.3390/bs12090343
- AUTONOMOUS WEAPON SYSTEMS AND INTERNATIONAL HUMANITARIAN LAW. (n.d). https://www.sipri.org/sites/default/files/2021-06/2106_aws_and_ihl_0.pdf
- Noel E. Sharkey; "The Evitability of Autonomous Robot Warfare", INTERNATIONAL REVIEW OF THE RED CROSS, 2012. (IF: 4)
- Craig Martin; "A Means-methods Paradox and The Legality of Drone Strikes in Armed Conflict", THE INTERNATIONAL JOURNAL OF HUMAN RIGHTS, 2015. (IF: 3)
- Kriangsak Kittichaisaree; "Application of The Law of Armed Conflict, Including International Humanitarian Law, In Cyberspace", 2017.
- Floris Bex; Henry Prakken; Tom M. van Engers; Bart Verheij; "Introduction to The Special Issue on Artificial Intelligence for Justice (AI4J)", ARTIFICIAL INTELLIGENCE AND LAW, 2017. (IF: 3)
- Kenning Arlitsch; Bruce Newell; "Thriving in The Age of Accelerations: A Brief Look at The Societal Effects of Artificial Intelligence and The Opportunities for Libraries", JOURNAL OF LIBRARY ADMINISTRATION, 2017. (IF: 3)
- Corinne Cath; "Governing Artificial Intelligence: Ethical, Legal And Technical Opportunities And Challenges", PHILOSOPHICAL TRANSACTIONS. SERIES A, MATHEMATICAL, 2018. (IF: 4)
- Silja Voeneky; "Implementation and Enforcement of International Humanitarian Law", 2020.

- Jason Scholz; Jai Galliott; "The Humanitarian Imperative for Minimally-Just AI in Weapons", 2021.
- Ronald Leenes; Aaron Martin; "Technology and Regulation 2020", 2021.
- Lefteris Benos; Aristotelis C Tagarakis; Georgios Dolias; Remigio Berruto; Dimitrios Kateris; Dionysis Bochtis; "Machine Learning in Agriculture: A Comprehensive Updated Review", SENSORS (BASEL, SWITZERLAND), 2021. (IF: 4

*****