About the Article

Main question: How does AI impact modern warfare and IHL compliance? Argument: AI weapons and cyber tools boost military power but risk civilian harm and legal accountability. Conclusion: Human oversight and regulation are crucial to ensure AI respects IHL principles

About the Author

Giulia Convertini is pursuing a M.A. in International Relations with a focus on International Politics and Regional Dynamics at the Università degli Studi di Milano (IT). Her research focuses on EU affairs and digital/tech policies, as well as regional dynamics in Asia and the Middle East, with a particular focus on the US's role in global affairs.

1. Introduction – The Role of AI and Cyber Technologies in Warfare

The integration of artificial intelligence (AI) and cyber technologies into modern warfare represents one of the most consequential shifts in military strategy since the advent of nuclear weapons. AI is now actively shaping battlefield decisions, powering autonomous systems and enabling new forms of digital warfare that transcend physical borders. At the same time, cyberspace has emerged as a contested domain in its own right—where states and non-state actors conduct operations ranging from espionage to infrastructure sabotage, often below the threshold of conventional war and sliding more towards the realm of hybrid warfare. This convergence of AI and cyber capabilities has already begun to transform the character of armed conflict. Russia's war in Ukraine has illustrated the real-time use of AI-enhanced targeting, autonomous drone swarms and coordinated cyberattacks on critical infrastructure, such as energy grids and communications networks. These developments raise urgent questions about the adequacy of existing legal frameworks and the international community's ability to prevent destabilising consequences. The current applications of military AI are very diverse. They range from support in the targeting cycle and the conduct of hostilities in general, use for hostile activities in cyberspace and for intelligence, surveillance, and reconnaissance purposes. AI is also deployed within the context of so-called 'information warfare', launching cyberattacks on communication systems or civilian infrastructures. Another concrete example of 'information warfare' is the use of deep fake videos in the Russia-Ukraine conflict, with the aim of influencing or spreading disinformation to the general public. Research and development into AI for defence is now broad, well-funded and moving fast. Work ranges from blue-sky algorithms to near-term operational integration — with emphasis on trustworthiness, human-machine teaming, and robustness against adversarial attacks. Major defence research agencies and alliances are accelerating programmes while policymakers race to put governance and legal guardrails. An example of that is NATO's revised Artificial Intelligence Strategy, released in July 2024, which stresses both opportunities and risks, reaffirming principles of responsible use such as lawfulness, accountability, explainability, reliability, human oversight, and bias mitigation. Importantly, the strategy acknowledges challenges such as adversarial use and misuse of AI, disinformation, and unintended consequences, positioning NATO to balance innovation with safeguards while shaping global norms for responsible defence applications. The pace of technological advancement far exceeds that of legal reform. International humanitarian law (IHL), while rooted in principles of humanity and military necessity, was not designed to account for self-learning algorithms or invisible cyber operations. Key challenges such as attributing attacks, assigning accountability for autonomous decisions and regulating dual-use technologies, underscore the need for legal reviews. This article explores the legal implications of AI-driven and cyber-enabled conflict. It examines how current International Humanitarian Law engages with these technologies, where significant gaps remain and what emerging risks may demand urgent attention.

LAWS:
AI weapons that autonomously select and engage targets

2. Legal Frameworks: Current landscape and gaps

Autonomous weapons are set to revolutionise warfare. They have the potential to scale up armed conflict to such a fast pace that humans might lose control over it. According to the United Nations Secretary General, Antonio Guterres (2018): "Our challenge is to maximize the benefits of the technological revolution while mitigating and preventing the dangers. The impact of new technologies on warfare is a direct threat to our common responsibility to guarantee peace and security." The development of AI weapon systems would lead to a global arms race, which,

without oversight, could increase risks to global stability. Given the unpredictable behaviour of machine-learning AI systems, which are controlled by algorithms that dictate weapon engagement systems, humans may lose their ability to intervene promptly in case of faulty behaviour, as Jurgen and Altman (2017) argued. Warfare has already integrated AI, mostly to assist physical military hardware with specific functions and tasks such as flight, surveillance and navigation. Autonomous systems are increasingly being deployed both in wars and in law enforcement situations like police operations and cyberspace. Cyberattacks do not directly cause killings but can significantly harm critical infrastructures like electricity grids and hospitals. Autonomous systems can also be hacked. Stuart Russell (2019) warned about how autonomous weapons threaten human security on the national, international, local and personal levels. International Humanitarian Law (IHL), which consists of the four Geneva Conventions of 1949, their additional protocols and customary law, was established to explicitly recognise the need for striking a balance between military necessity and humanity in a situation of armed conflict. This means that there are certain limits as to which actions can be taken, even during wars. A fundamental principle of International Humanitarian Law is that States are constrained in their selection of weapons and methods of warfare by established norms of international law. Specifically, Article 36 of Additional Protocol I to the Geneva Conventions (AP I) requires states parties to assess, during the development, acquisition, or adoption of any new weapon or method of warfare, whether its use would be prohibited under international law. This obligation becomes even more significant and challenging when applied to emerging technologies whose effects on civilians and civilian infrastructure remain uncertain. Article 36 calls on states to evaluate new weapons and methods of warfare through the lens of IHL and all other relevant international legal obligations applicable to them. With the growing recognition of the concurrent application of IHL and International Human Rights Law (IHRL) in armed conflicts, such legal reviews, should ideally assess compliance with both legal frameworks. While many IHL rules apply only in times of armed conflict, Article 36 reviews often occur during peacetime. For states that are party to AP I, this constitutes a procedural obligation. However, it can be argued that even non-party states—if bound by substantive legal limits on the use of certain weapons or methods—should undertake similar pre-emptive legal reviews to ensure they do not violate those substantive rules. For example, regarding the co-application of IHL and international human rights law, the Human Rights Committee's General Comment 36 interprets the obligation to protect the right to life under Article 6 of the International Covenant on Civil and Political Rights (ICCPR) as including preventive measures, such as legal reviews of new weapons. Cyberspace has emerged as a critical domain in modern military operations, with cyberattacks increasingly forming a regular component of armed conflict. The development of new cyber capabilities and tools, whether they represent novel means of warfare or introduce new methods, undoubtedly requires legal scrutiny under Article 36. When cyber operations directly support conventional attacks – for instance, by disabling air-defence systems to enable airstrikes – they function as means of warfare that complement kinetic operations and as such, must be subject to an Article 36 legal review.

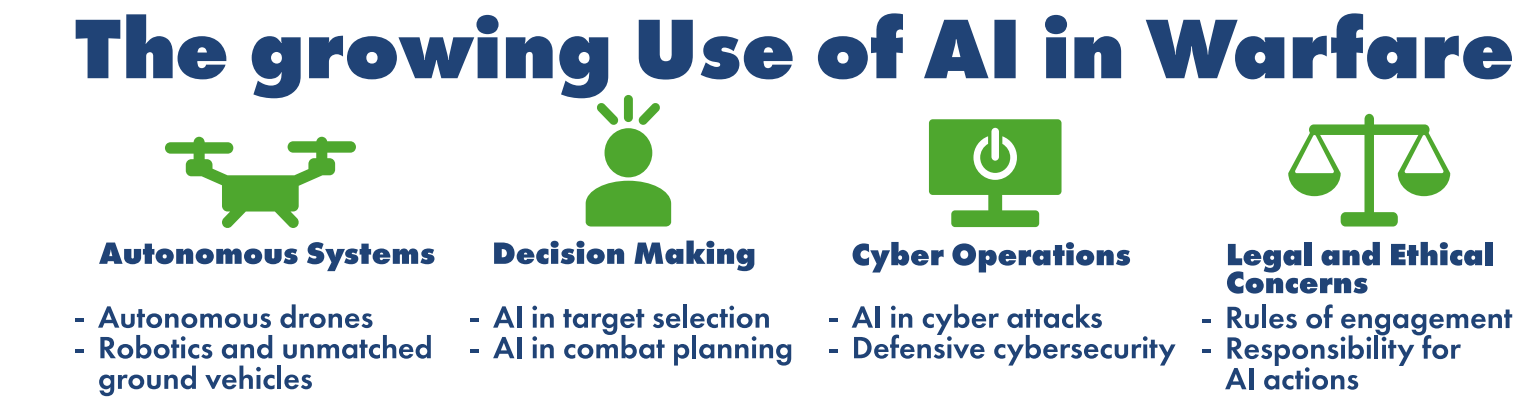

Figure 1: Summary of the growing Use of AI in Warfare

3. The Intersection of Lethal Autonomous Weapons (LAWS), AI and machine learning in conflict within the International Humanitarian Law framework

The most prominent and imaginative use case of AI for military purposes involves the deployment of AI in unmanned physical robotic systems, including lethal autonomous weapon systems (LAWS). The International Committee of the Red Cross (ICRC) defines LAWS as weapons that select targets and attack them without human intervention. According to the ICRC, this means that a human merely activates an autonomous weapon, but at that point does not know specifically who or what it will target, nor where or when it will do so. LAWS will make this decision autonomously based on the observations from sensors and software in the deployment environment, which link this input to a specific 'target profile'. Not all LAWS have machine learning (ML) features, as some of these weapons are rule-based and operate within human-designed scenarios, making their functionalities limited to humans' commands. ML allows LAWS to have a much higher level of autonomy in decision-making, in ways that range from the ability to move through enemy territory to identifying, selecting, locating and attacking particular targets. Within the framework of International Humanitarian Law, the integration of AI in warfare would bring in the opportunity to enhance the respect of IHL, as machine learning processes complex information in a faster way and can take informed decisions while taking into account IHL principles. Ideally, AI-driven LAWS have the potential to take a clear picture of complex scenarios and play an effective part in conflicts. In practice, as the ICRC argues in its publication on Artificial intelligence and machine learning in armed conflict: A human-centred approach (2019), autonomous weapons have no human perception of emotions like fear or anger and preserving this more emotional side of armed conflicts also would allow for the preservation of humanity in this realm. If we look at the case of IHL's proportionality principle, which calls for a balance between the potential civilian harm and military necessity, it indeed requires human, subjective participation in defining military advantage and the level of harm caused to civilians. The core of International Humanitarian Law is to protect people who are not involved in conflicts, so humans cannot feed AI-driven weapons with a way to precisely and objectively evaluate the level of civilian casualties compared to military gains. This puts AI-driven LAWS against IHL, unless human involvement remains a key part of armed conflicts. The application of AI systems in warfare also raises concerns regarding their unpredictability and the issue of explainability. Machine learning can get to a point where humans can't trace how and why an AI-driven system has made a specific decision and acted in a specific way. Not knowing in advance how autonomous weapons might act also raises questions regarding their ability to respect the IHL principle of distinction, which requires parties to the conflict to distinguish at all times between combatants and civilians. Another cause for concern is the fact that AI systems are subject to biases, putting once again at risk the IHL principle of protecting people and places that should not be targeted in armed conflict.

Human oversight: Essential to ensure AI weapons follow IHL

4. Conclusion

Prioritizing the human aspect of military operations calls for a reimagining of the human role within an evolving human–machine cognitive system. Militaries should be equipped to lead diverse, integrated teams across the military infrastructure, encompassing military personnel, government actors and civilian contributors. To do so effectively, they will need a sufficient understanding of their AI-driven tools, enabling meaningful collaboration as well as critical oversight. AI is already reshaping the character of warfare and disrupting long-established human practices. By fostering a human-centric approach to AI

and cyberwarfare, militaries would more effectively prepare for the inevitable transformations ahead without making the world more unsafe. Netta Goussac summarises here the need for legal reviews regarding the integration of AI in warfare: "Today's technological advances in how conflicts are fought mean that robust legal reviews are as critical now as they were when Article 36 was conceived, during the Cold War arms race. While Article 36 does not specify the process by which legality should be determined, in the view of the ICRC, the obligation clearly implies a mandatory standing procedure that assesses all weapons and their normal or expected method of use, against a State's international obligations, including IHL. According to the ICRC's Guide to legal reviews, this entails a multi-disciplinary examination of the technical description and actual performance of a weapon, at the earliest possible stages of its research, development or acquisition. Legal reviews can be a potent safeguard against the development and use of AI weapons that are incapable of being used in compliance with IHL rules regulating the conduct of hostilities, notably the rules of distinction, proportionality and precautions in attack. These rules are addressed to those who plan, decide upon and carry out attacks in armed conflict. It is humans that apply this law and are obliged to respect it. An AI weapon system that is beyond human control would be unlawful by its very nature—a conclusion that would become evident during a legal review." (Goussac, 2019) It is clear that there is an urgent need for global action not only to safely embark on the ongoing AI-driven technological revolution of warfare, but also to make sure that is effectively regulated. This research highlighted the current gaps between the IHL framework and the application of AI in warfare, shedding a spotlight on the need to harness AI responsibility in military contexts, especially with regards to the principles of proportionality and distinction, which are at the core of International Humanitarian Law. This paper ultimately calls for concerted international cooperation to adapt international law to the new challenges and opportunities arising from the development of autonomous weapons and cyber warfare.

Figure 2: Summary of Modern Warfare in the Digital Age: AI, Cyber Capabilities & Legal Gaps

References

Goussac, N. (2019, April 18). Safety net or tangled web: Legal reviews of AI in weapons and war-fighting. ICRC Humanitarian Law and Policy Blog. https://blogs.icrc.org/law-and-policy/2019/04/18/safety-net-tangled-web-legal-reviews-ai-weapons-war-fighting

International Committee of the Red Cross. (2019). Artificial intelligence and machine learning in armed conflict: A human-centred approach. https://www.icrc.org/en/document/artificial-intelligence-and-machine-learning-armed-conflict-human-centred-approach

Altmann, J., & Sauer, F. (2017). Autonomous weapon systems and strategic stability. Survival, 59(5), 117–142. https://doi.org/10.1080/00396338.2017.1375263

EURODEV. (2025, May 19). The future of defense: How AI is transforming the industry. https://www.eurodev.com/blog/defense-industry-ai-transformation

Leuven Centre for Public Law, International humanitarian law and new technologies. KU Leuven. https://www.law.kuleuven.be/ai-summer-school/blogpost/Blogposts/international-humanitarian-law

Lieber Institute. (2023, May 3). IDF introduces AI to the battlefield: A new frontier. West Point. https://lieber.westpoint.edu/idf-introduces-ai-battlefield-new-frontier/

Royal United Services Institute. (2023). Trust in AI: Rethinking future command. https://www.rusi.org/explore-our-research/publications/occasional-papers/trust-ai-rethinking-future-command

United Nations Human Rights Committee. (2018). General comment No. 36: Article 6 of the International Covenant on Civil and Political Rights, on the right to life (CCPR/C/GC/36). https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-36-article-6-right-life

UN Secretary-General Discusses Maximizing Security Benefits of Technology, Mitigating Dangers, (3 April 2018)

Russell, S. (2019). Human compatible: Artificial intelligence and the problem of control. Penguin Books.

Summary of NATO's revised Artificial Intelligence (AI) strategy, 10 July 2024. https://www.nato.int/cps/en/natohq/official_texts_227237.htm?utm