MEHUCO

AI and Future Warfare:
Exploring the Hidden Challenges

With funding from the:

Federal Ministry
of Research, Technology
and Space

MEHUCO

Contents

AI and Future Warfare: Exploring the Hidden Challenges

Artificial intelligence (AI) is having a major impact on warfare: It is transforming and challenging legal frameworks, policy-making and knowledge systems that determine how war is conducted and how violence is inflicted. The integration of AI into military decision-making and autonomous weapon systems (AWS), for example, expands operational capabilities while reshaping how responsibility, control and the legitimacy of military action are assessed.

These developments are particularly evident in the tension between technological innovation and existing norms, especially those of international humanitarian law (IHL), which assumes that human actors possess sufficient judgement and control. AI systems increasingly analyse data autonomously, generate courses of action and preconfigure human decisions. As a result, new forms of cooperative decision-making are emerging in which human judgement becomes closely intertwined with algorithmic recommendations, which challenges the attribution of individual responsibility.

The military use of AI must also be understood as part of broader transformations in the organisation of military power. New constellations of actors – including start-ups, technology companies, venture capital investors and state institutions – are becoming closely interconnected. These developments draw on patterns of the military-industrial complex while reshaping them through digital platform logics and data-driven innovation economies, with AI-based military technologies being developed outside traditional defence industries.

At the same time, the platformisation of military structures is gaining relevance. Digital platforms aggregate data, standardise interfaces and automate decision-making, linking sensors, weapon systems, communication networks and human operators into complex socio-technical assemblages. Within such environments, knowledge production, perception and action become closely intertwined, generating unprecedented forms of knowledge and power alongside new operational risks.

The development of autonomous weapons systems further illustrates that military AI relies on diverse knowledge systems extending beyond technical disciplines, including philosophical concepts of autonomy, cybernetic systems theory, biological models of collective intelligence

and regulatory frameworks of responsible AI. Meanwhile, challenges in standardisation and regulation arise because autonomous and semi-autonomous weapons systems often defy existing legal and technical categories.

This dossier examines these hidden challenges of military AI from an interdisciplinary perspective. It highlights interdependencies between technological development, legal norms, economic and political power structures and knowledge practices. It demonstrates that military AI is not merely an innovative tool, but a driver of much broader and much more consequential transformations.

1. How AI challenges traditional legal frameworks and categories

Law, University of Hannover

The use of AI in weapons challenges international law, as machines struggle to reliably distinguish between combatants and civilians and attributing responsibility for war crimes to a specific human becomes difficult. This necessitates a debate on whether traditional legal frameworks must be adapted to address the use of AI in warfare.

Info Box: Cooperative decision making

In the context of AI, cooperative decision-making refers to a process where a human and an AI system work together to reach a conclusion. AI becomes part of the "thinking process". For example: Predictions made by a system can significantly influence a human's final decision by suggesting possible targets for attack or specific courses of action. There can be a risk that interacting humans will not have all the information at their disposal, which can cause uncertainty and make it difficult to decide against a system's suggestions. Traditional criminal law structures struggle to attribute the result to a responsible actor because even though a human technically makes the final choice, their decision is often a product of the AI's logic.

The question of how the use of AI affects existing legal frameworks has long been part of the national and international debate, particularly in relation to the military use of AI-assisted weapon systems. One of the most relevant legal frameworks for regulating warfare is IHL. Although it is not specifically tailored to AI systems, there is agreement that it also applies to their use in armed conflicts. In order to comply with the IHL principle of distinction, an AI system would have to be able to reliably distinguish between permissible targets and protected persons. This requires AI systems to be able to make an appropriate classification based on individual characteristics of the targeted person. Even without AI it can be difficult to determine with certainty what constitutes a protected person and dynamic situations intensify this issue. For example: Civilians are protected persons and must not be attacked, but if they are taking active part in the hostilities, they are a permissible target. Combatants are permissible targets, but if they lay down their arms and give up, they must not be attacked. Similar difficulties exist with regard to the IHL principle of proportionality. This means that in military operations, care must be taken to ensure that unintended damage to civilians is not excessive in relation to the military advantage. The decision as to how many civilian casualties are

excessive must be made on a case-by-case basis. It is doubtful whether a system can and should reliably make such a decision.

The legal framework that regulates the criminal responsibility of participating individuals is International Criminal Law. If, for example, the principle of distinction is not complied with during the deployment of an AI-supported system and a protected person is killed, this could constitute a war crime. This raises the question as to who can be held responsible. Since AI systems are not recognized as legal entities themselves and therefore cannot be held responsible, the responsibility of other actors involved must be clarified. However, attributing responsibility in this way poses challenges, as AI systems are becoming increasingly integrated into human decision-making processes (see Infobox). In addition, some types of AI, including ML processes, promote a lack of predictability and transparency. Compared to conventional technology, it is therefore more difficult to predict how a particular system will behave. At the same time, it is rarely possible to understand in hindsight why a system acted in a certain way. In the context of the contributions made by AI systems, as well as their technical characteristics, it is questionable whether the resulting harm is still the work of the human being. Consequently, existing legal frameworks are being put to the test by the integration of AI systems, and it is doubtful whether traditional concepts of individual responsibility can be applied without hesitation, or whether the developments in the context of weapons systems could be taken as an opportunity to scrutinise and adapt the existing regulations and concepts.

Further Readings:

Acquaviva, Guido (2023). Crimes *without* Humanity? Artificial Intelligence, Meaningful Human Control, and International Criminal Law, *Journal of International Criminal Justice*, Volume 21/5, 981–1004.
This article explores how autonomous weapons systems challenge traditional criminal law by making it difficult to assign individual responsibility through standard legal concepts like intent and causation. The author examines whether the principle of "meaningful human control" can be linked to established legal theories to ensure accountability.

Amoroso, Daniele & Tamburrini, Guglielmo (2020). Autonomous Weapons Systems and Meaningful Human Control: Ethical and Legal Issues. Current Robotics Reports, Volume 1, 187–194.

The authors provide a comprehensive overview of the ethical and legal debates surrounding autonomous weapons systems.

Beck, Susanne & Barlag Schirin (2024). Humanity in War? The Importance of Meaningful Human Control of Autonomous Weapon Systems, Ethics and Armed Forces, Issue 1, 60-67.
The authors analyse the growing disconnect between traditional international criminal law and the technical reality of autonomous weapons, arguing that, to preserve the principle of individual criminal responsibility, legal frameworks must evolve to require "meaningful human control".

Sterz et al. (2024). On the Quest for Effectiveness in Human Oversight: Interdisciplinary Perspectives, FAccT '24: The 2024 ACM Conference on Fairness, Accountability, and Transparency, 2495 - 2507. https://doi.org/10.1093/jicj/mqad024
The article critically examines human oversight in high-risk AI systems and defines essential conditions that must be met for this oversight to effectively contribute to risk mitigation. Building on this, the paper analyses the EU AI Act and demonstrates the extent to which this regulatory framework aligns with scientific findings on moral responsibility.

Winter, Eric (2022). The Compatibility of Autonomous Weapons with the Principles of International Humanitarian Law, Journal of Conflict & Security Law, Volume 6/1, 1-20.
The author analyses the compatibility of autonomous weapons with the key principles of IHL. He argues that autonomous weapons are not currently able to comply with these principles, owing primarily to a lack of sufficiently advanced AI and context awareness but also highlights various ways in which future technological advances could enable autonomous weapons to comply with these legal standards.

2. AI for warfare and the organisation of military power

Sociology, University of Hamburg

AI-based warfare is reshaping military power. New defence start-ups, Big Tech, and venture capital challenge established arms industries while normalising AI-based warfare. In doing so, they transform not only military practices but also societal understandings of security and the future.

Info Box: ”Military-Industrial Complex”
The term military-industrial complex (MIC) refers to a concept primarily associated with the U.S. in the post–Second World War period. It describes a durable network of mutual interests linking the armed forces, the defence industry, and segments of the political apparatus – a phenomenon first critically articulated by U.S. President Dwight D. Eisenhower in his 1961 farewell address. The concept denotes a concentration of economic, political, and ideological power that permeates governmental institutions and society at large. This alliance – potentially including actors from science and research – promotes military expansion and armaments programs while limiting democratic oversight and public control. Although the concept originated in a specific historical context, it continues to provide a useful framework for understanding the dynamics of the modern military sector and has been revisited in light of the recent rise of start-ups.

The growing importance of AI in warfare (including in AWS) is contributing to the emergence of new economic actors and to significant transformations in the organization of military power. These developments reinforce the relevance of the military-industrial complex as an analytical lens, as military power increasingly arises from interdependent relations between the armed forces, political decisions, scientific research and industry. While the concept of the MIC originated in a specific U.S. historical context, similar patterns of interdependence can also be observed in Europe, albeit shaped by different trajectories and institutional arrangements.

The increasing importance of AI for military applications is a key driver of current changes in this area of power. This is because the AI underlying algorithmic warfare is often not developed within the military itself. It comes predominantly from external actors in industry. The rise of AI, coupled with the war in Ukraine, has accelerated the emergence of new technology-oriented

defence start-ups in Europe. These companies challenge the dominance of established manufacturers and reflect a broader turn of Big Tech and capital-rich IT and AI industries toward military applications. Their focus is particularly on drones, software, and AI systems. Leading the way are internationally active start-ups with million-dollar valuations, such as Palantir, Anduril, Helsing, Open AI, and Space X. Ukraine serves as a testing ground and incubator for them, where training data is collected and technologies are not only refined, but also legitimised as necessary and helpful for modern warfare.

Against the backdrop of shifting international geopolitical power structures, various start-ups in Europe present themselves as contributors to European strategic autonomy, aiming to reduce dependence on U.S. and Chinese technologies. Their symbolic positioning contrasts sharply with that of established companies, which remain largely transatlantic in orientation. Their growth is driven primarily by venture capital, although there are also collaborations and investments by established players. The management cultures, strategies and public communication practices of these start-ups differ fundamentally from those of traditional defence firms. They participate actively in political and public debates, portraying themselves as modern, agile and innovative. They even openly criticise established defence companies for allegedly being outdated and institutionally rigid. They call for far-reaching structural reforms, streamlined procurement procedures, greater flexibility, and a stronger focus on digital and algorithmic warfare.

The growing discursive influence of this so-called “New Defense” contributes to the normalization of algorithmic and automated forms of warfare. They promote and visualize digital spectacles of dystopian war futures that only their AI-based systems can effectively counter. In doing so, they present themselves as extremely knowledgeable and familiar with the role of AI and claim interpretative authority over the future of warfare. Their close ties to former soldiers bolster their credibility as practical and user-oriented innovators.

These techno-optimistic ways of thinking have far-reaching political, legal, ethical, and social implications. Dystopian visions of war are intertwined with security policy narratives that portray technological progress – especially AI – as a prerequisite for securing democratic societies. This interpretive regime is increasingly shaping political, military, and civil debates about protection, threats, and responsibility. In the context of “total society defense,” the defense sector is therefore closely intertwined with internal actors, such as police, disaster control, and emergency services. Examples such as Anduril's border surveillance systems or

Palantir's data analysis platforms illustrate the global interdependence of military, police, and migration policy control technologies.

Together, these developments stabilize a dense network of AI-based military force, venture capital, technological visions of the future, and security policy narratives. This network not only transforms the organization of military power, but also shapes societal ideas of security, responsibility, and the future.

Further Readings:

Nadibaidze, Anna (2025): Startups Envisioning Algorithmic Warfare: The Discourses of US Tech Companies in Defense AI, in: Global Policy 16, 487-493.
The article shows how U.S. start-ups in the field of defense AI have become influential players whose public discourse normalizes certain visions of algorithmic warfare.

Hoijtink, Marijn/Van der Kist, Jasper (2025): Platforms on the Frontline: The Rise of the Platform Model in Defense Tech, in: https://opiniojuris.org/2025/02/11/platforms-on-the-frontline-the-rise-of-the-platform-model-in-defense-tech/, 11.02.2025.
The text shows how the increasing implementation of platform-based business and software models in the defense sector is restructuring military practice, knowledge, and decision-making, and creating new dependencies, monopolies, and risks to democracy and international law.

Vanderborght, Robin/ Nadibaidze, Anna (2025): Military demonstrations as digital spectacles: How virtual presentations of AI decision-support systems shape perceptions of war and security. *European Journal of International Security*. 1-20.
The article examines how developers of AI- and ML-based military decision support systems visually market their products, thereby asserting their authority over the future of warfare.

Schwarz, Elke (2025): From blitzkrieg to blitzscaling: Assessing the impact of venture capital dynamics on military norms. *Finance and Society*, doi:10.1017/fas.2024.18
The text argues that the VC sector has a significant influence on military procurement processes and thus also on the orientation of military operations and practices.

Daub, Adrian (2020): What Tech Calls Thinking. An Inquiry into the Intellectual Bedrock of Silicon Valley. FSG Adult.

The book examines the rhetoric of Silicon Valley by tracing its slogans and assertions back to older philosophical and cultural origins and showing how they function as self-justifications for technological and economic power.

3. Standards: Regulation meets Technology

Computer Science, Ostfalia University of Applied Sciences

Standards are one of the most influential mechanisms for regulating products, processes, and technological development. They are typically created by national or international standards bodies or industry consortia and refined through iterative, agreement-based processes.

Info Box: Standards

Standards are formal technical documents that define shared requirements for products, services, or processes. They are developed by national and international standards bodies, industry consortia, or multi-stakeholder groups. Typical content includes performance criteria, safety rules, testing methods, and interoperability guidelines. Standards support consistency, quality, and compatibility across industries and markets. Although voluntary by default, governments can make them mandatory by referencing them in laws or regulations. They also influence procurement, certification, and market-access conditions. Developing a standard is a multi-stage process involving expert drafting, public review, and consensus-building. Standards are regularly updated to reflect technological, regulatory, or societal changes. Some begin as industry best practices, open specifications, or NGO initiatives before being formalised.

Standards are technical documents that define requirements for products, production processes, or methods of use. They support regulation but do not function as regulations unless formally adopted into law or contractual frameworks. AWS span a wide range of platforms and levels of autonomy, and different technical or military standards may apply depending on their design, classification, and manufacturer. For example, some loitering munitions—semi-autonomous drones—may fall under existing ammunition or explosive ordnance standards, even though those standards were not originally designed with autonomous decisionmaking in mind. When international standards use broad terms like “munition” without explicitly addressing autonomy, important issues such as responsibility, oversight, and operational constraints may be insufficiently addressed. This shows why the broader context matters. Standards are not just technical instructions—they also reflect underlying assumptions and values. These need to be made visible and openly discussed when people from different fields work together.

Standards are usually developed by expert groups within a specific discipline, which means the terminology they use often reflects the assumptions and language of that field. Because different disciplines assign different meanings to the same terms, this can lead to semantic and contextual misunderstandings during communication or development processes. In this sense, each discipline functions like a sub-language with its own culture and conventions. To reduce these misunderstandings, interdisciplinary work benefits from shared definitions or a common reference vocabulary—a kind of "lingua franca" that clarifies how key terms are used. While this cannot eliminate all differences, it helps address many of the semantic challenges that arise when standards intersect across fields. Furthermore, it could help to understand the viewpoints of other disciplines to enhance cooperative working and understanding across all the different disciplines.

A general problem concerns both the accessibility and the legal status of technical standards. Even when a standard is widely recognized as important, obtaining access to it can be costly, creating disproportionate barriers for smaller organizations and limiting broader participation in standard-conformant development. If a standard is not incorporated into law or required through regulation, certification, or contractual obligations, companies retain considerable discretion in adopting alternative approaches or interpreting requirements in flexible ways, as illustrated in certain cases involving loitering munitions, where they are counted as ammunition instead of an AWS. When standards pertain to safety-critical or ethically sensitive technologies, relying only on voluntary guidelines is often insufficient. Some form of formal adoption, regulatory oversight, or independent conformity assessment is typically necessary to ensure consistent implementation and accountability.

Further Readings:

Bode, I. & Watts, T. (2023, June 29). Loitering munitions and legally binding rules on autonomy in weapon systems. ICRC Humanitarian Law & Policy Blog. https://blogs.icrc.org/law-and-policy/2023/06/29/loitering-munitions-legally-binding-rules-autonomy-weapon-systems/

The article highlights that loitering munitions occupy an ambiguous space between traditional ammunition and AWS. It is argued that existing AWS definitions are too narrow and leave these increasingly autonomous munitions outside meaningful regulation.

Breiner, J., & Ferran, M. (2024, February). L-297 loitering munitions. Munitions Safety Information Analysis Center (MSIAC). https://www.msiac.nato.int/publication/l-297-loitering-munitions/
This publication shows that loitering munitions are formally treated as ammunition even though they incorporate autonomous target-seeking functions. It is emphasized that this places them outside existing AWS-specific regulatory frameworks and that this gray zone creates technical and legal challenges.

Kaiser, S. (2025). Terminology Used in Standardisation: An International (and Culture-Specific) Perspective. In Standardization Strategies in China and India: Industrial Policy and Geopolitics and Implications for Europe (pp. 79-91). Wiesbaden: Springer Fachmedien Wiesbaden.
The chapter provides an interdisciplinary problem description of standards and focuses on the contextual problem of background knowledge and understandability under given terms.

Robinson, R. C. (2022). The Linguistic Challenge for Standards. Standards, 2(4), 449-459.
The article examines both linguistic and broader conceptual challenges associated with standards.

ISO (International Standard Organization). (2026, 19. January). Stages and resources for standards development. ISO. https://www.iso.org/stages-and-resources-for-standards-development.html
An in depth explanation of the development process for standards and their stages.

4. Military AI and the Platformisation of Warfare

Media Studies, University of Bonn

Platforms are an increasingly relevant factor in the military use of AI. They shape diverse processes, such as data collection, automation, decision-making or control. Conceptualising platforms as an analytical approach, accounts for this diversity, shedding light on infrastructural and technical conditions, knowledge production and human/machine relations, which will play a major part in defining the future of warfare.

Info Box: Platformisation

The concept of platformisation describes a far-reaching transformation of society that is tied to the power and effects of digital platforms. This transformation concerns technical and infrastructural aspects, including the universal computation of social life, software applications or networked communication and data-processing. Platformisation enforces particular organising principles, structuring content, access or socioeconomic and political hierarchies. The economic power of a few corporations that offer server and cloud infrastructures raises questions on (national and individual) digital sovereignty or effective governance. Platforms also set formal, technical and aesthetic norms, rules and patterns. This includes, for example, application programming interfaces (APIs), user interfaces (UIs), software standards, database architectures or layout options for websites. Platforms control access to information, organise and monetise data and use it to develop new technologies and applications (e.g. AI), which further accelerates the centralisation of power.

The use of autonomous weapons and military AI heavily relies on social and technical conditions. The assessment of weapon systems cannot be reduced to their kinetic capabilities, degrees of automation or algorithmic foundations. Rather, their use must be understood in a much broader context, which can be analytically captured via the media theory concept of platformisation. This concept describes a far-reaching transformation that encompasses technical, infrastructural, economic, political and cultural aspects (see info box). Contemporary forms of warfare are no exception.

The current developments with regard to platformisation in the military can be traced back to the doctrine of network-centric warfare (NCW) that emerged in the 1990s. NCW was conceived as a centralised "system of systems" aimed at achieving shared situational awareness

and more effective decision-making by connecting human and non-human elements. These historical roots point towards contemporary platforms that orchestrate sensors, ML and human operators across infrastructures, edge processing and communication networks. Data-centric and algorithmic command-and-control systems reconfigure the unresolved NCW promises and tensions between decentralisation and recentralisation, between the chaos of war and its imagined antidote of technologically enabled control.

Current examples of how platforms shape military realities in this regard are AIP (Artificial Intelligence Platform) by the US software company Palantir, Brave1 by the government of Ukraine or GhostPlay, which is co-developed by the German Bundeswehr Armed Forces. They combine platform logics of capitalism, automation and gamification. These developments shed light on how the platformisation approach allows one to distinguish several analytical layers.

1. *Infrastructure*: The infrastructural conditions of military AI and autonomous weapons are of particular relevance, such as electricity, connectivity or physical data storage capacity. The dependencies on network providers or cloud computing services are strongly tied to economic questions (Which major companies gain political clout through market power?) as well as subsequent questions of governance (How can these infrastructures be adequately regulated in light of global dynamics and competing legal systems?).

2. *Interfaces and interfacing processes*. Both APIs that mediate between software systems and UIs, which shape human-machine relations, are constitutive for the platformisation tendencies in the military. They enable universal datafication and data interoperability, while also shaping claims of autonomy as interface effects (for example in manned-unmanned teaming).

3. *Knowledge*: Platformisation promotes certain forms of knowledge that shape ideas of current and future warfare. This means, they favour particular ways of producing and structuring knowledge, which is called an “epistemic practice”. Targeting in platform environments, for example, combines and conflates meaning-making with decision-making. Meaning is created by automated data analysis and profiling techniques; decisions are made by tying a particular label (for example target,

enemy or terrorist) to an ensuing action (such as attack or surveillance). Gamification and simulation tendencies also have epistemic repercussions: battle management UIs used for swarm control or virtual twin training environments steer human attention, normalise playbook reasoning and amplify automation bias. Most recently, the underlying structures of AI models (LLMs) have begun to play a major role in creating and defining highly consequential forms of knowledge: What battle scenarios, for example, seem likely? What will the enemy's next steps be? What if the AI system is wrong?

4. *Human/machine relations*: With their specific interfaces and structuring effects on knowledge, perception and decision-making, platform logics also shape human/machine relations. In this way, platform logics extend into bodies, cognition or social collaboration. At the same time, the human is modelled as deficient, in need of augmentation, and ultimately as an optimised element of the platform.

Platformisation necessitates a research agenda that encompasses this range of its effects. It combines an analysis of infrastructural conditions and their economic and political repercussions with the study of interfacing effects across human–machine and machine–machine relations, with a particular focus on epistemic phenomena. Platform autonomy emerges as a hidden locus of power in contemporary warfare.

Further Readings:

Bächle, Thomas Christian: The AI-augmented super soldier: Enhancement, interfaces and the extended cognition of human-machines, in: Bérénice Boutin, Taylor Woodcock, Sadjad Soltanzadeh (eds.): Decision at the edge: Interdisciplinary Dilemmas in military artificial intelligence, Den Haag 2026.
This study focuses on human-machine relations in the military, paying particular attention to augmentation and the idea of "the human as a platform".

Helmond, Anne: The Platformization of the Web: Making Web Data Platform Ready, in: Social Media + Society, 1(2), 2015, 1–11, doi.org/10.1177/2056305115603080.
This analysis shows the implicit effects of platform logics on the organisational structure of the internet as a whole.

Hoijtink Marijn/Planqué-van Hardeveld, Anneros: Machine Learning and the Platformization of the Military: A Study of Google's Machine Learning Platform TensorFlow, in: International Political Sociology, 16, 2022, 1–19, doi.org/10.1093/ips/olab036.
A compelling analysis of platformisation effects that shows the importance of the concept.

van Dijck, José/Poell, Thomas/De Waal, Martijn: The Platforms Society. Public Values in a Connective World, New York 2018.
This foundational work makes a clear case for a critical assessment of powerful platforms.

5. When Knowledge Becomes a Weapon / The Weaponization of Knowledge

Science & Technology Studies, Paderborn University

An appropriate understanding of AWS needs to take into account non-technical knowledge such as philosophical understandings of human autonomy, biologically inspired concepts of distributed intelligence and regulatory concepts of an ethical and responsible AI. These knowledge systems do not only provide a background to reflect on or negotiate the meaning of AWS. Rather, they can have a decisive influence on their development.

Info Box: Knowledge Systems

Knowledge Systems are organized bodies of knowledge that form patterns of interpretation and action. While knowledge systems may encompass traditional or religious beliefs and local wisdom, modern "knowledge societies" are increasingly shaped by and depend on scientific systems of knowledge. However, knowledge systems are neither objective nor neutral. On the one hand, their validity rests on their institutionalisation in social structures and material practices within specific socio-historic contexts. On the other hand, they determine which perspectives, aims and decisions are valued and legitimized and which are not.

The process of developing AWS is not a purely technical endeavour. It is influenced, shaped and guided by cultural, social and political factors. Among these factors, knowledge systems that do not originate from the military context or robotics play a central role.

To start with, the perceived autonomy of weapon systems points to bodies of knowledge that far exceed the military one. Our modern understanding of autonomy, which informs AI research and its practical applications, originates from the philosophy of the Enlightenment. There, autonomy was grounded in the idea of self-determination and the free will of individual subjects. Enlightenment thinkers such as Immanuel Kant attributed this characteristic exclusively to humans. However, in the scientific discipline of cybernetics (ancient Greek κυβερνήτης / *kybernḗtēs* refers to the person who steers a ship), which emerged in the wake of World War II, the concept of autonomous systems was coined, where "system" referred particularly to technical systems, such as a rocket with a target-seeking mechanism. While the goal is pre-determined, there is a degree of flexibility in how to achieve this goal. In the case

of the rocket that is: how to adjust its course according to the movement of the target. From the perspective of cybernetics, the autonomy of a human (its voluntary action and free will) and the dynamic, goal-oriented behaviour of an autonomous system are more or less synonymous. This equation forms the basis of most of the AI research, including its military applications. Here, the autonomy of machines is modeled after the modern understanding of human autonomy.

In some cases, however, AWS are not modeled after the individual human mind. Instead, they mimic swarming behaviour as it can be observed in nature. Here, knowledge systems from biology come into play. The military interest in robotic swarming developed around the turn of the millennium, parallel to the new scientific field of swarm robotics, which originates from the concept of swarm intelligence. In swarm robotics (including its military application), swarm intelligence serves as a guiding principle to develop robotic systems where emergent behavior and distributed intelligence replace direct human control (human in/on the loop) and pre-programming of specific behaviors. In contemporary military imaginaries, implementing this swarm intelligence into robotic units would bring greater mass, coordination, intelligence, and speed to the battlefield. This would enhance the ability of warfighters to gain a decisive advantage over their adversaries.

A third example of how non-military knowledge systems influence the development of AWS is regulation. Lately, there have been increasing efforts to transfer the concept of responsible and ethical AI to military contexts. In the EU AI Act that established a common regulatory and legal framework for civil AI applications as well as in numerous national AI regulations, it is required that only trustworthy, explainable, and transparent AI systems be used, thus enabling human operators of such systems to maintain a sufficient degree of control. However, transferring this approach to the military sphere not only changes how we evaluate, regulate or even ban AWS. It also alters the technological development itself as value-based design principles are implemented. Now, an AWS might be designed according to certain ethical standards from the outset, having consequences on the human-machine-interactions characterising their use in combat.

The ways AWS are developed and designed is neither straight forward nor a simple translation of military requirements into technological solutions. It is shaped by numerous non-military knowledge systems and can only be understood - both in terms of its alleged capabilities and problematic consequences - with regard to this wider background.

Further Readings:

Bousquet, Antoine (2009). *The Scientific Way of Warfare. Order and Chaos on the Battlefields of Modernity*. Columbia University Press.
This study analyses the relations between historically dominant scientific worldviews and changes in ways wars have been thought and waged since the 18th century.

Hälterlein, Jens (2025). The more-than-human biopolitics of swarming – complexity, emergence, and control in military robotics. *European Journal of International Security*. Published online:1-18. doi:10.1017/eis.2025.10023.
This paper gives a detailed account of how biological understandings of swarming have been implemented into military robotics.

Scharre, Paul (2014). *Robotics on the Battlefield: Part 2: The Coming Swarm*. Center for a new American Security. https://www.cnas.org/publications/reports/robotics-on-the-battlefield-part-ii-the-coming-swarm
This policy report outlines expectations towards the implementation of swarming into the (US) military, problems arising from it and options for controlling a robotic swarm.

Suchman, Lucy, & Weber, Jutta (2016). Human-Machine-Autonomies. In Nehal C. Bhuta, Susanne Beck, Robin Geiß, Hin-Yan Liu & Claus Kreß (Eds.), *Autonomous Weapons Systems. Law, Ethics, Policy*. Cambridge University Press, 75-102.
This paper provides a detailed reconstruction of how philosophical understandings of autonomy informed AWS.

Troath, Sian (2024). Trusting technology to wage war: the politics of trust and ethics in the development of robotics, autonomous systems, and artificial intelligence. *Critical Military Studies*, DOI: 10.1080/23337486.2024.2362074.
This paper investigates the ways by which the claim of being able to develop a trustworthy and ethical military AI is constructed.

Even in an age of autonomous weapons and military AI: Humans remain responsible for war

The military use of AI does not just introduce new weapons – it is transforming the logic of war itself. AWS blur human responsibility, platforms centralise control through data and code, and new actors – start-ups, tech firms, venture capital – reshape military power that potentially moves beyond democratic oversight. Legal frameworks, on the other hand, are becoming less effective: loitering munitions can evade regulation by being misclassified as ammunition, while standards remain fragmented and opaque. The prominent idea of a "meaningful human control" is undermined by systems that shape, not just support, decisions – especially when AI draws on non-military knowledge systems (like cybernetics or swarm biology) to redefine autonomy.

These are not hypothetical risks. They are already unfolding in global conflicts, in procurement processes, and in the rhetoric of self-styled "defence innovators". The result is a system where power is concentrated in private hands, accountability erodes, and war becomes a data-driven spectacle.

Consequently, there is only one reasonable position regarding so-called "fully autonomous weapons": they must be banned. Not because AI is inherently dangerous, but because its military use – unregulated, unaccountable, and driven by opaque platforms and profit – threatens the core principles of IHL and human responsibility. The future of war must not be decided by algorithms, investors, or tech narratives. It must be governed by law, transparency, and democratic control.