

RESEARCH ARTICLE

Artificial intelligence, semiconductors, and the new geopolitics of security: Why technology assessment must engage in emerging military technologies

Thomas Reinhold¹ 

28

Abstract • This conceptual research article examines the accelerating militarization of emerging technologies, particularly artificial intelligence (AI) and semiconductors, and its implications for technology assessment (TA). It highlights how quickly commercial innovation, especially in the field of AI, is integrated into military applications, thereby eluding traditional assessment methods. Drawing on examples from Russia's war against Ukraine and global semiconductor supply chains, the article argues for more agile, technically sound, and interdisciplinary TA approaches. It calls for assessment approaches that account for real-time deployment, dual-use dynamics, and geopolitical competition. Ultimately, it advocates further developing TA to remain relevant amid fast-moving security, technological, and strategic transformations.

Künstliche Intelligenz, Halbleiter und die neue Geopolitik der Sicherheit: Warum sich die Technikfolgenabschätzung mit neuen Militärtechnologien befassen muss

Zusammenfassung • Dieser konzeptionelle Forschungsartikel untersucht die zunehmende Militarisierung neuer Technologien, insbesondere von künstlicher Intelligenz (KI) und Halbleitern, und ihre Auswirkungen auf die Technikfolgenabschätzung (TA). Es wird aufgezeigt, wie schnell kommerzielle Innovationen, vor allem im Bereich der KI, in militärische Anwendungen integriert werden und sich dabei traditionellen Bewertungsmethoden entziehen können. Anhand von Beispielen aus dem russischen Angriffskrieg auf die Ukraine und den globalen Halbleiter-Lieferketten plädiert der Artikel für flexiblere, technisch fundierte und

interdisziplinäre TA-Ansätze. Er fordert Analyseansätze, die den Einsatz in Echtzeit, die Dynamik des doppelten Verwendungszwecks und den geopolitischen Wettbewerb berücksichtigen. Letztlich empfiehlt er eine Weiterentwicklung der TA, um inmitten der schnelllebigsten sicherheitspolitischen, technologischen und strategischen Umwälzungen relevant zu bleiben.

Keywords • artificial intelligence, semiconductors, technology assessment, emerging technologies

This article is part of the Special topic "Technology assessment and future warfare: The Good, the Bad, and the Ugly," edited by K. Weber, M. Bresinsky. <https://doi.org/10.14512/tatup.7286>

The challenge of the militarization of emerging technologies

The landscape of technological innovation is undergoing a profound transformation. So-called emerging technologies (Rotolo et al. 2015) are not just incrementally advancing; they are reshaping the tempo, scope, and unpredictability of change – for example, the advancements in robotic autonomy (Knuhtsen et al. 2025) – thus calling upon the field of technology assessment (TA) to explore how to analyze the impact of this development. This article approaches the issue not from the perspective of a traditional TA scholar but from a practitioner at the intersection of technological foresight and political consulting for the areas of military cyber and artificial intelligence (AI) capabilities and the development of arms control measures. This vantage point is based on monitoring defense contractors' demonstrations, strategic white papers, research and grant proposal tenders, or the technical specifications of chips, drones, and AI systems rather than an application of formal TA frameworks. And yet, the core question is comparable: What are the social and political implications

* Corresponding author: thomas.reinhold@prif.org

¹ Peace Research Institute Frankfurt (PRIF), Frankfurt am Main, DE



© 2026 by the author(s); licensee oekom. This Open Access article is published under a Creative Commons Attribution 4.0 International License (CC BY).

<https://doi.org/10.14512/tatup.7248>

Received: 23. 07. 2025; revised version accepted: 09. 10. 2025; published online: 23. 03. 2026 (peer review)

of specific technologies, and what are policy recommendations for their responsible management?

Nowhere are the challenges posed by emerging technologies more apparent than in military applications, where a qualitative content analysis and comparison of strategic and national security doctrines (Schörning et al. 2024) reveal, that military realities have partially already overtaken theoretical considerations. Examples are the deployment of small (autonomous) drones or the real-time development and battlefield testing of AI enabled weapon systems. This dynamic of ‘on-the-fly’ militarization innovations underscores a critical shift. Emerging technologies are no longer being gradually integrated into military systems after long periods of assessment, prototyping, and strategic debate. Instead, they are often pushed into deployment amid ongoing conflicts (Slusher 2025), with a pace that outstrips existing methods for evaluating their broader implications. Meanwhile, normative debates like the discussion on meaningful human control of autonomous weapon systems (Sauer 2020) or the responsible use of military artificial intelligence (Afina and Persi Paoli 2024) are evolving alongside these innovations with the idea of keeping a ‘human in the loop’ as a guiding normative principle. Yet, especially as such systems grow more capable, these discussions are increasingly outpaced by developments on the ground, where semi- or fully autonomous systems are already being deployed in ways that blur the line between human judgment and machine execution (Watts and Bode 2023).

This pace of contemporary technological change compresses the window of reaction time, which raises fundamental questions for the future of TA: If the goal is to inform decision-making and shape governance before technologies become entrenched, what does this mean when those technologies are already fielded before assessment begins? What kind of methodologies can remain relevant when the frontier of innovation is constantly shifting? And how can TA assess the impact of this development in a way that includes and considers parallel technological progress and inter-technological dependencies and influence?

The following chapters use AI and semiconductor technologies as case studies to conceptually highlight the role of emerging technologies in shaping contemporary geopolitics and security. AI raises questions of autonomy, agency, and algorithmic opacity, while semiconductors underpin modern infrastructure and are increasingly central to global power competition. Together, these cases prompt us to consider whether new forms of anticipatory or adaptive assessment are needed to keep pace with technologies that evolve faster than our understanding.

The impact of commercial artificial intelligence on military transformation

AI has rapidly become one of the central pillars of contemporary military innovation as it plays a foundational role in areas such as surveillance and threat detection (King 2024), real-time support for battlefield decision-making (Nadibaidze et al. 2024)

and especially autonomous military systems with or without weapons (Mozur and Satariano 2024). This acceleration of AI into operational relevance is doing more than enhancing military capabilities. It is altering the tempo of warfare itself (Zeff 2025) and pushing decision-making toward real-time responsiveness, often supported or even initiated by machines. A key factor in this rapid integration is the dominant role of large, global technology companies in AI development. These firms – spanning the U.S., China, and, to some extent, Europe (Merle 2024) – drive progress in AI research. Although primarily aimed at consumer markets, their pace in funding and release cycles outpaces military research and development (Maslej 2025), making them natural feeders into defense applications. The dual pressure of return on investment and high demand from military and security organizations leads to the rapid embedding of successful AI models into security-relevant systems. Military planners are increasingly turning to commercial off-the-shelf solutions (Reuters 2025) and adapting them rather than building from scratch.

The war in Ukraine offers vivid examples of this transformation. Both Ukrainian (Matlack et al. 2025) and Russian forces (Stepanenko 2025) have employed swarms of small drones for reconnaissance, targeting, and direct strikes. Many are equipped with autonomous navigation systems and, in some cases, rudimentary target identification or loitering behavior. Ukraine has launched successful drone attacks deep into Russian territory using modified commercial technologies, targeting strategic assets such as long-range bombers, airfields, and logistical hubs. These innovations are not developed through traditional procurement pipelines but are improvised, deployed, and iteratively improved on the battlefield (Bondar 2025). This cycle is measured in weeks, not years, with companies gathering hands-on experience directly in conflict zones (Loh 2025).

One of the key drivers of this evolution is autonomous functionality (Suckau 2024), which – even when limited or semi-supervised – lets machines operate without direct human control. These autonomous vehicles, like unmanned/uncrewed aerial vehicles, unmanned/uncrewed ground vehicles or unmanned/uncrewed underwater vehicles are often introduced for pragmatic reasons, such as reducing response time, resisting electronic warfare, or extending the operation radius beyond reliable accessibility via traditional radio connections. Such capabilities rely heavily on AI and machine learning (Garikapati and Shetiya 2024) to provide the necessary degree of flexibility and adaptability of the vehicle’s operation in order to avoid obstacles, react to situational conditions, select and track targets, or engage them. Both Ukrainian and Russian forces have incorporated AI-driven systems in agile and adaptive ways. Ukraine has retrofitted commercial drones with AI (Collett-White et al. 2024), sometimes based on publicly available tools (Rudra 2025) whereas Russia is experimenting with AI-enhanced Shahed drones to improve target selection and tracking. A second major driver is the use of AI for decision-making and support (Bovet 2025). AI systems aggregate and process intelligence data at a scale and speed far beyond human capabilities. In Eastern Ukraine, trench warfare

is increasingly complemented by AI-powered surveillance tools that scan enemy movements, simulate courses of action, and manage logistics (Ministry of Defence of Ukraine 2025). Algorithms coordinate drone patrols, optimize supply chains, and assist with casualty evacuation. AI is now embedded at every level of combat – from tactical ground operations to strategic command centers.

of data at high speed and low latency – something only possible through cutting-edge semiconductor technologies. In this sense, any discussion about the development of autonomous systems, AI, and its implications is also a discussion about semiconductors. From an analytical standpoint, semiconductors could serve as a prime focus area for TA. It offers the advantage of a specific technology with measurable and quantifiable parameters whose

The convergence of commercial innovation and military application presents a challenge for technology assessment.

Similar dynamics can be observed in Western defense initiatives like Germany's 'Zeitenwende.' Start-ups such as Helsing have partnered to integrate AI in real-time combat systems, including drone coordination and jet dogfights (Sprenger 2025). U.S.-based Anduril builds autonomous drones, surveillance platforms, and intelligent sensors powered by AI to automate threat responses (O'Donnell 2024). These companies, structured like start-ups with flat hierarchies and agile processes, can rapidly meet military needs and often embrace the concept of 'software defined defense' (BMVg 2023), using off-the-shelf hardware with updatable software, which accelerates innovation.

This convergence of commercial innovation and military application presents a challenge for TA. Traditional approaches – relying on long-term forecasting and stakeholder dialogue – struggle under the compressed timelines of AI development and deployment. TA must now function amid real-time testing and iteration and must address military AI not as a derivative of civilian tech but as co-developed through civilian market dynamics and military urgency.

Semiconductors: the backbone of artificial intelligence and subject of geopolitical competition

While much of the public debate around artificial intelligence focuses on software, algorithms, and data, this explosive growth of AI would not have been possible without the underlying hardware: semiconductors. These microelectronic components are the backbone of AI, especially for current generation AI systems like large language models (LLM), as their training as well as their application requires huge quantities of computer chips. ChatGPT 5, for instance, the current state-of-the-art LLM from OpenAI, has – according to estimates – needed 200.000 processing chips just for training the system (Moss 2025) and uses even more for providing the system to end users and business applications over the coming years (Caswell 2025). Regardless of the exact amount, these numbers point to a clear direction, as nearly every advancement in machine learning, computer vision, autonomous navigation, or military IT applications like battlefield decision-support systems depends on processing vast volumes

technical progress is relatively visible and public due to the intense competition among companies for market dominance in this domain.

Semiconductors are among the most technically complex artifacts ever produced. The latest chips feature billions of transistors etched onto nanometer-scale silicon wafers using extreme ultraviolet (EUV) lithography – a process requiring a level of precision and purity that only a handful of actors worldwide can achieve. These chips enable AI computation, whether in the form of general-purpose graphics processing units designed for parallel computation, specialized tensor processing units optimized for AI workloads, application-specific integrated circuits custom-built for particular tasks, high-bandwidth memory chips, or ultra-fast networking semiconductors. Advances in these types of hardware – alongside breakthroughs in cooling systems, networking, and energy optimization – are occurring on ever-shorter cycles. A powerful illustration of this acceleration can be found in the evolution of AI models themselves. In late 2022, ChatGPT 1.0 demonstrated the potential of LLM for general-purpose dialogue and reasoning. Since then, the landscape has advanced dramatically: OpenAI's Veo-3 brings AI-generated video closer to photorealism; Meta's Llama 3 and other frontier models now approach multi-modal understanding; and reasoning agents have started to move beyond static responses toward complex situational decision-making (Delovski 2024). Sam Altman, CEO of OpenAI, and others now openly discuss pathways toward artificial general intelligence – a form of AI capable of performing any intellectual task a human can, reflecting a generalized, human-like understanding and cognitive flexibility (Frazier et al. 2024). This step, although controversial in terms of technical feasibility, would redefine the boundaries between human and machine cognition. These leaps result in qualitative transformations – 'capability jumps' that redefine what is technologically possible.

But these technological capabilities and their underlying complexity come with strategic fragility. The production of advanced semiconductors relies on highly globalized supply chains (Sullivan 2025), involving the design capabilities of U.S.-based firms like NVIDIA, AMD, and Intel; fabrication facilities concentrated in Taiwan, like Taiwan Semiconductor Manufacturing Com-

pany Limited; EU-based suppliers like the advanced semiconductor materials lithography (ASML) Holding, which produces the world's only EUV lithography machines; and raw materials sourced from politically unstable regions, including rare earths from Africa and noble gases from Ukraine. This fragmented yet tightly interdependent supply chain means that geopolitical tensions can quickly disrupt the production and distribution of critical hardware. At the forefront of this competition are the United States and China (Frazier 2025), locked in a rapidly escalating technological rivalry. Both countries view dominance in AI and semiconductors not merely as a pathway to economic growth but as a national security imperative (Allen 2025). The U.S. has introduced sweeping export controls on high-end chips, chip

due to their irreplaceable technologies (European Court of Auditors 2025). As the U.S. restricts exports to China, these European firms are drawn into compliance regimes reflecting U.S. interests over EU sovereignty, while simultaneously gaining leverage to strengthen Europe's strategic position.

For Taiwan, the main site of advanced chip manufacturing, these dependencies are not just economic – they are central to national security, forming what is known as the 'Silicon Shield' (Wu 2024). This concept, which highlights Taiwan's centrality to global chipmaking, illustrates the interplay between technology and security policy, where the island's semiconductor role acts as a deterrent to aggression, given that disruptions could trigger global crises and geopolitical escalation.

These technological capabilities and their underlying complexity come with strategic fragility.

design software, and semiconductor manufacturing equipment and pressured key equipment suppliers such as the Dutch company ASML to restrict maintenance and support for advanced lithography machines previously sold to China (Allen and Goldston 2025). These measures aim to limit China's access to the technologies essential for training large AI models and building advanced military systems. In response, China has poured billions into developing a domestic semiconductor ecosystem and launched numerous state-supported AI labs and companies (Chang et al. 2025).

An example of this high-stakes contest is DeepSeek, a Chinese AI company that frequently draws attention for publishing models claimed to rival Western competitors (Baptista 2025). While the technical success behind such models remains debated (Rubstov 2025), this underscores the aggressiveness and volatility of the AI race, as models emerge rapidly – often backed by massive state or private investment – only to fragment, pivot, or vanish under geopolitical pressure, hardware constraints, or commercial hurdles. A particularly notable case occurred when DeepSeek announced its R1 model in early 2025, claiming competitive performance at significantly lower hardware costs. Nvidia's stock price dropped approximately 17–18% in a single day (Mortimer and Page 2025), as investors feared DeepSeek's breakthroughs might reduce demand for Nvidia's expensive hardware. Even though the loss was quickly offset, it illustrates the financial pressure created by high development costs and the influence of technical disruption in the AI ecosystem.

Between the U.S. and China, Europe faces a complex challenge. It is deeply dependent on technologies across the global AI and semiconductor stack, from fabrication to cloud infrastructure. However, it also hosts some of the most critical chokepoints in global chip production. Companies like ASML in the Netherlands and Carl Zeiss SMT in Germany (key optical suppliers for ASML's chipmaking machines) have become geopolitical actors

Layered on top of these dynamics is the issue of rare earths and critical materials, which form the invisible substrate of both AI systems and chip production. China dominates the extraction and processing of many key inputs, including neodymium (used in magnets), gallium, and germanium – vital for semiconductors and sensors (Teer et al. 2024). The U.S. and Europe have responded with strategies to diversify supply chains, build processing capacity, and invest in recycling technologies. However, these efforts trail behind the scale and integration of China's supply chains. Even with design and fab capacity in place, a material bottleneck could paralyze production.

In sum, the AI-semiconductor-nexus is a geopolitical pressure point where technological evolution, economic rivalry, and military strategy converge. The 'chip war' is not only about industrial competition – it is about strategic autonomy, resilience, and first-mover advantage in future security architectures.

Recommendations for an effective and relevant technology assessment

Being not a classic TA scholar, I rather approach technologies as a technician and analyst: focusing on what they can do now, where they're headed, and how quickly these developments proceed. My analysis is based on qualitative content analysis of relevant national doctrines (Schörnig et al. 2024) and grounded in capability tracking, the assessment of technical limits, deployment timelines, and the identification of starting points for regulatory measures rather than an application of formal TA frameworks. That said, my vantage point reinforces the growing importance of TA as we are living through rapid technological shifts. AI, once seen as speculative, is starting to inform military decisions, and chip development outpaces procurement cycles. Conflicts like Ukraine's are not only exposing these tools – they

are actively shaping them. The key issue isn't just capability, but speed of change and emerging strategic turning points.

The problem I observe is the current mismatch between this pace and nature of innovation and the methodological tools used to assess them. Many analytical frameworks remain too slow, too linear, and too disconnected from the systems they aim to evaluate. They often rely on models of risk anticipation and societal deliberation that presuppose a certain amount of time, stability, and clarity of trajectory – all of which are increasingly absent in the domains of AI and semiconductors. What kind of assessment, then, might be better suited to this reality?

First, analytical frameworks must be agile and more technologically grounded. This can be achieved for AI, for instance, by including the analysis of the technological architectures, the source code of systems, hardware constraints, and data dependencies. Taking these aspects into account could help to keep track of swift innovations that can shift the development direc-

ingness to cooperate on the part of the engineering and natural sciences. This includes finding a common language, understanding and accepting the concepts and constraints of politics, and the willingness to evaluate one's own scientific achievements in a social and security-related context. Within this context, TA has a unique opportunity to help classify and prioritize emerging technologies by providing structured analysis that highlights critical chokepoints, infrastructure bottlenecks, or design vulnerabilities – insights that are urgently needed for political decision-making.

Finally, this means that TA should adapt its principles to a new landscape. Participatory and normative approaches still matter, especially in defining acceptable use conditions and governance frameworks. But these approaches must be integrated with real-time capability tracking, technical scenario modeling, and system-level diagnostics, thus becoming more iterative, more exploratory, and more strategically aware.

The key issue isn't just capability, but speed of change and emerging strategic turning points.

tions or a change in the meaning of individual components of a technical system as a whole. For example, a currently cutting-edge AI system may become quickly obsolete through changes in chip efficiency, bandwidth limitations, or model advancements of competitors. These are deeply technical issues, but their consequences can have a strong impact in terms of geopolitical power and the necessary policy adjustments.

Second, assessments must actively engage with security policy and defense strategy, taking into account the dual-use nature of emerging technologies. As discussed earlier, technologies developed for consumer purposes – such as image recognition or predictive analytics – are getting adapted by military companies, weaponized, or integrated into military decision-making systems. The current AI ecosystem underlines, that commercial companies are no longer just a part of a bigger picture, but the core innovator, driver, and provider of security-relevant technologies, thus becoming the rule-setter of what capabilities and limitations exist.

Third, analytical assessments need to draw on interdisciplinary expertise. This includes fields that are often underrepresented in such contexts: computer science and semiconductor engineering. Only the collaboration between these disciplines can track the full lifecycle of a technology, from initial development to deployment and adaptation in scenarios – including their impact analysis. This also enables the identification of critical supply-chain dependencies, such as those discussed in the context of chip manufacturing or rare earth supplies – dependencies that may be invisible to purely social or ethical assessments but decisive in times of crisis. Of course, interdisciplinary work is no one-way responsibility but requires an equal will-

I do not claim to have the methodological blueprint for this transformation, nor come these recommendations from an empirical study. What I can offer are insights from my fieldwork and technical analysis, hoping that these fragments might help to point out where TA might need to stretch, collaborate, and evolve in a world where emerging technological changes are no longer incremental but exponential – and where their consequences are being written in real time on the battlefield, in code, and in silicon.

Funding · This article received no funding.

Competing interests · The author declares no competing interests.

Ethical oversight · The author confirms that all procedures were performed in compliance with relevant laws and institutional guidelines.

References

- Afina, Yasmin; Persi Paoli, Giacomo (2024): Governance of artificial intelligence in the military domain. A multi-stakeholder perspective on priority areas. Geneva: UNIDIR. Available online at <https://unidir.org/publication/governance-of-artificial-intelligence-in-the-military-domain-a-multi-stakeholder-perspective-on-priority-areas/>, last accessed on 24.11.2025.
- Allen, Gregory (2025): DeepSeek, Huawei, export controls, and the future of the U.S.-China AI Race. Washington, DC: CSIS. Available online at <https://www.csis.org/analysis/deepseek-huawei-export-controls-and-future-us-china-ai-race>, last accessed on 24.11.2025.
- Allen, Gregory; Goldston, Isaac (2025): Understanding U.S. allies' current legal authority to implement AI and semiconductor export controls. Washington, DC: CSIS. Available online at <https://www.csis.org/analysis/understanding-us-allies-current-legal-authority-implement-ai-and-semiconductor-export>, last accessed on 24.11.2025.

- Baptista, Eduardo (2025): Explainer. What is DeepSeek and why is it disrupting the AI sector? In: Reuters, 28.01.2025. Available online at <https://www.reuters.com/technology/artificial-intelligence/what-is-deepseek-why-is-it-disrupting-ai-sector-2025-01-27/>, last accessed on 17.10.2025.
- BMVg – Bundesministerium der Verteidigung (2023): Software defined defence. Positionspapier des BDSV, BDLI, Bitkom und BMVg. Berlin: Bundesministerium der Verteidigung. Available online at <https://www.bmvg.de/resource/blob/5711942/6fb70a45412601fdf03f63aeebf72451/cyber-defined-defence-papier-data.pdf>, last accessed on 24.11.2025.
- Bondar, Kateryna (2025): Ukraine's future vision and current capabilities for waging AI-enabled autonomous warfare. Washington, DC: CSIS. Available online at <https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare>, last accessed on 24.11.2025.
- Bovet, Peter (2025): Exploring decision advantages. Improving speed, precision and efficiency in military targeting by applying artificial intelligence. Stockholm: Swedish Defence University. <https://doi.org/10.62061/leiy7136>
- Caswell, Amanda (2025): Why OpenAI wants 100 million GPUs – and how it could supercharge ChatGPT. In: Tom's Guide, 22.07.2025. Available online at <https://www.tomsguide.com/ai/sam-altmans-trillion-dollar-ai-vision-starts-with-100-million-gpus-heres-what-that-means-for-the-future-of-chatgpt-and-you>, last accessed on 17.10.2025.
- Chang, Wendy; Arcesati, Rebecca; Hmaid, Antonia (2025): China's drive toward self-reliance in artificial intelligence. Berlin: Mercator Institute for China Studies. Available online at <https://merics.org/en/report/chinas-drive-toward-self-reliance-artificial-intelligence-chips-large-language-models>, last accessed on 24.11.2025.
- Collett-White, Mike; Dutta, Prasanta; Zafra, Mariano (2024): How Ukraine pulled off an audacious drone attack deep inside Russia. Months of planning went into a covert operation that relied on cheap, short-range drones. In: Reuters, 05.06.2025. Available online at <https://www.reuters.com/graphics/UKRAINE-CRISIS/DRONES-RUSSIA/mypmjzayyvr/>, last accessed on 17.10.2025.
- Delovski, Boris (2024): A brief history of GPT models. Available online at <https://www.edlitera.com/blog/posts/gpt-models-history>, last accessed on 17.10.2025.
- European Court of Auditors (2025): The EU's strategy for microchips. Luxembourg: Publications Office of the European Union. <https://doi.org/10.2865/0902427>
- Frazier, Kevin (2025): What comes next in AI regulation? In: Lawfare, 28.07.2025. Available online at <https://www.lawfaremedia.org/article/what-comes-next-in-ai-regulation>, last accessed on 17.10.2025.
- Frazier, Kevin; Rozenshtein, Alan; Salib, Peter (2024): OpenAI's latest model shows AGI is inevitable. Now what? In: Lawfare, 23.12.2024. Available online at <https://www.lawfaremedia.org/article/openai-s-latest-model-shows-agi-is-inevitable.-now-what>, last accessed on 17.10.2025.
- Garikapati, Divya; Shetiya, Sneha (2024): Autonomous vehicles. Evolution of artificial intelligence and learning algorithms. In: arXiv. <https://doi.org/10.48550/arXiv.2402.17690>
- King, Anthony (2024): Digital targeting. Artificial intelligence, data, and military intelligence. In: Journal of Global Security Studies 9 (2), p. ogae009. <https://doi.org/10.1093/jogss/ogae009>
- Knuhtsen, Reyk; Patel, Dylan; Ciminelli, Niko; Ryu, Joe; Ghilduta, Robert; Ontiveros, Jeremie Eliahou (2025): Robotics Levels of Autonomy. SemiAnalysis, published on 30 July 2025. Available online at <https://newsletter.semianalysis.com/p/robotics-levels-of-autonomy>, last accessed on 04.02.2026
- Loh, Matthew (2025): Western arms makers can now live-test their prototype weapons on the battlefield against Russia's forces. In: Business Insider, 18.07.2025. Available online at <https://www.businessinsider.com/ukraine-testing-western-weapon-prototypes-russian-forces-combat-2025-7>, last accessed on 17.10.2025.
- Maslej, Nestor (ed.) (2025): Artificial intelligence index report 2025. Stanford, CA: Stanford Institute for Human-Centered Artificial Intelligence (HAI). Available online at <https://hai.stanford.edu/ai-index/2025-ai-index-report>, last accessed on 24.11.2025.
- Matlack, Jon-Wyatt; Schwartz, Sebastian; Gill, Oliver (2025): Ukraine's drone ecosystem and the defence of Europe. Lessons lost can't be learned. London: LSE IDEAS. Available online at <https://www.lse.ac.uk/ideas/publications/Research-Reports/Ukraine-s-Drone-Ecosystem-and-the-Defence-of-Europe-Lessons-Lost-Can-t-be-Learned>, last accessed on 24.01.2025.
- Merle, Quentin (2024): Chips supply chain. Bifurcation and localization. In: CSS Analyses in Security Policy. <https://doi.org/10.3929/ETHZ-B-000680146>
- Ministry of Defence of Ukraine (2025): Enemy equipment detected in 2 seconds. The ministry of defence showcased delta and Avengers systems at the London defence conference. Available online at <https://mod.gov.ua/en/news/enemy-equipment-detected-in-2-seconds-the-ministry-of-defence-showcased-delta-and-avengers-systems-at-the-london-defence-conference>, last accessed on 17.10.2025.
- Mortimer, Ian; Page, Matthew (2025): How has DeepSeek affected the AI market for investors? In: Guinness Global Investors, 24.02.2025. Available online at <https://www.guinnessgi.com/insights/how-has-deepseek-affected-ai-market-investors>, last accessed on 17.10.2025.
- Moss, Sebastian (2025): OpenAI says its compute increased 15x since 2024, company used 200k GPUs for GPT-5. As company releases its latest generative AI model. In: Data Center Dynamics, 07.08.2025. Available online at <https://www.datacenterdynamics.com/en/news/openai-says-its-compute-increased-15x-since-2024-company-used-200k-gpus-for-gpt-5/>, last accessed on 17.10.2025.
- Mozur, Paul; Satariano, Adam (2024): A.I. begins ushering in an age of killer robots. In: The New York Times, 02.07.2024. Available online at <https://www.nytimes.com/2024/07/02/technology/ukraine-war-ai-weapons.html>, last accessed on 17.10.2025.
- Nadibaidze, Anna; Bode, Ingvild; Zhang, Qiaochu (2024): AI in military decision support systems. A review of developments and debates. Odense: Center for War Studies. Available online at <https://www.sdu.dk/en/forskning/forskningens-heder/samf/cws/cws-activities/2024/ai-gammel>, last accessed on 24.11.2025.
- O'Donnell, James (2024): We saw a demo of the new AI system powering Anduril's vision for war. In: MIT Technology Review. Available online at <https://www.technologyreview.com/2024/12/10/1108354/we-saw-a-demo-of-the-new-ai-system-powering-andurils-vision-for-war/>, last accessed on 17.10.2025.
- Reuters (2025): US defense department awards contracts to Google, Musk's xAI. In: Reuters, 14.07.2025. Available online at <https://www.reuters.com/business/autos-transportation/us-department-defense-awards-contracts-google-xai-2025-07-14/>, last accessed on 17.10.2025.
- Rotolo, Daniele; Hicks, Diana; Martin, Ben (2015): What is an emerging technology? In: Research Policy 44 (10), S. 1827–1843. <https://doi.org/10.1016/j.respol.2015.06.006>
- Rubstov, Alexey (2025): AI supply chain shocks. Insights from DeepSeek R1. Toronto: Global Risk Institute. Available online at <https://globalriskinstitute.org/publication/ai-supply-chain-shocks-insights-from-deepseek-r1/>, last accessed on 24.11.2025.
- Rudra, Sourav (2025): This open source software was used in Ukraine's drone attack on Russia. Is this a turning point for open source software in warfare? In:

Its FOSS, 04.06.2025. Available online at <https://news.itsfoss.com/open-source-drone-attack/>, last accessed on 17.10.2025.

Sauer, Frank (2020): Stepping back from the brink. Why multilateral regulation of autonomy in weapons systems is difficult, yet imperative and feasible. In: *International Review of the Red Cross* 102 (913), pp. 235–259. <https://doi.org/10.1017/S1816383120000466>

Schörnig, Niklas; Suckau, Liska; Korkusuz, Abdullah; Reinhold, Thomas (2024): Emerging disruptive technologies. *Neue Militärtechnologien in nationalen Sicherheitsstrategien – eine vergleichende Analyse*. In: *CNTR Monitor*. 2024. Perspektiven auf Dual Use. Frankfurt a. M.: Peace Research Institute, pp. 58–77. <https://doi.org/10.48809/cntr2024>

Slusher, Matthew (2025): Lessons from the Ukraine conflict. Modern warfare in the age of autonomy, information, and resilience. Washington, DC: CSIS. Available online at <https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age-autonomy-information-and-resilience>, last accessed on 24.11.2025.

Sprenger, Sebastian (2025): Saab, Helsing let Gripen fighter fly with AI in charge. In: *Defense News*, 11.06.2025. Available online at <https://www.defensenews.com/global/europe/2025/06/11/saab-helsing-let-gripen-fighter-fly-with-ai-in-charge/>, last accessed on 17.10.2025.

Stepanenko, Kateryna (2025): The battlefield AI revolution is not here yet. The status of current Russian and Ukrainian AI drone efforts. Washington, DC: Institute for the Study of War. Available online at <https://understandingwar.org/research/russia-ukraine/the-battlefield-ai-revolution-is-not-here-yet-the-status-of-current-russian-and-ukrainian-ai-drone-efforts/>, last accessed on 24.11.2025.

Suckau, Liska (2024): The limits of autonomy. Critically assessing factors limiting full autonomy of military uncrewed ground vehicles. Frankfurt a. M.: Peace Research Institute Frankfurt. <https://doi.org/10.48809/prifspot2406>

Sullivan, Helen (2025): A journey through the hyper-political world of microchips. In: *The Guardian*, 28.02.2025. Available online at <https://www.theguardian.com/technology/2025/feb/28/inside-the-mind-bending-tin-blasting-and-hyper-political-world-of-microchips>, last accessed on 10.11.2025.

Teer, Joris; Seaman, John; Caruso, Alessia (2024): EUISS intra-EU workshop outcomes. Starting with the end in mind. De-risked gallium, germanium, and rare earth value chains by 2030. Paris, France, 09.12.2024. Available online at <https://www.iss.europa.eu/sites/default/files/2025-03/EUISS%20workshop%20outcomes%3B%20De-risked%20Ga%20Ge%20and%20REE%20value%20chains%20-%20FINAL.pdf>, last accessed on 24.11.2025.

Watts, Tom; Bode, Ingvild (2023): Loitering munitions and unpredictability. *Autonomy in weapon systems and challenges to human control*. Odense: Center for War Studies. Available online at <https://www.sdu.dk/en/forskning/forskningsenheder/samf/cws/cws-activities/2023/loitering-munitions-unpredictability>, last accessed on 24.11.2025.

Wu, Emily (2024): 'Silicon Shield'. Looking beyond semiconductors. Washington, DC: United States Institute of Peace. Available online at <https://www.usip.org/publications/2024/01/silicon-shield-looking-beyond-semiconductors>, last accessed on 24.11.2025.

Zeff, Maxwell (2025): The Pentagon says AI is speeding up its 'kill chain'. In: *TechCrunch* 09.01.2025. Available online at <https://techcrunch.com/2025/01/19/the-pentagon-says-ai-is-speeding-up-its-kill-chain/>, last accessed on 17.10.2025.



DR. THOMAS REINHOLD

is a researcher at the Research Department International Security and the Cluster for Natural and Technical Science Arms Control Research (CNTR) at PRIF, the Peace Research Institute Frankfurt. He conducts research on the militarization of cyberspace, AI and possibilities for arms control and disarmament of these technologies.