European Parliament

Defence and artificial intelligence

SUMMARY

Artificial intelligence (AI) is rapidly transforming modern warfare. Russia's war on Ukraine has demonstrated AI's critical role in intelligence gathering, autonomous systems, and cyber operations. A global AI arms race is therefore gathering speed, with China and the United States vying for leadership and Russia investing heavily in AI capabilities. The EU Strategic Compass for security and defence underscores the growing importance of defence innovation, recognising its strategic value and emphasising the need to strengthen the EU's emerging military technologies, including AI.

The EU and its Member States have increasingly acknowledged AI's significance for security and defence, leading to expanded investment in AI-driven military technologies over the past decade. AI-powered defence innovation is progressing, with multiple European Defence Fund and Permanent Structured Cooperation (PESCO) projects dedicated to integrating AI into future military capabilities. Efforts are also underway to create synergies between the civilian, defence, and AI industries. In addition, the EU is cooperating with the North Atlantic Treaty Organization (NATO).

AI in warfare raises key ethical concerns, including accountability, compliance with international humanitarian law, and the risk of conflict escalation due to reduced human oversight. Global debate over military AI regulation has intensified amid the absence of a unified international framework, with contrasting approaches emerging – such as the US promoting flexible, innovation-friendly standards, and the EU adopting a human-centric, risk-based model through its AI Act, which excludes military use but may – according to some experts – shape future debate on military AI regulation. While organisations like the United Nations are pushing for responsible use and oversight, geopolitical tensions and differing strategic interests continue to hinder consensus on global rules.

The European Parliament recognises the strategic importance of AI in defence, but calls for regulation and a prohibition on lethal autonomous weapons (LAWS). The Parliament's Special Committee on Artificial Intelligence in a Digital Age (AIDA) stresses the need for ethical guidelines in defence AI, and has warned of the EU's potential lag in AI and called for international regulation of LAWS, robust cybersecurity measures, and global cooperation in military AI regulation.

IN THIS BRIEFING

EPRS | European Parliamentary Research Service

Author: Sebastian Clapp
Members' Research Service
PE 569.580 – April 2025

Introduction

New technologies have transformed Russia's war on Ukraine into an 'AI war lab'; the first international conflict where both sides have actively developed and deployed artificial intelligence (AI) for military purposes. AI technologies in geospatial intelligence, unmanned systems operations, military training, and cyber warfare have played a crucial role in battlefield success. However, AI is just one of many historical disruptive technologies, where the introduction of new military innovations has transformed warfare, reshaping how battles are fought, how militaries are structured, and how strategies are devised. Innovations like the crossbow, gunpowder, tanks, and nuclear weapons have led to 'revolutions in military affairs', and AI is seen as potentially leading to another such transformation. Discussions around AI frequently focus on lethal autonomous weapons or 'killer robots', but its applications are much broader. AI can enhance logistics, autonomous systems, cyber warfare, disinformation campaigns, and more. For instance, autonomous vehicles, like drones and unmanned systems, assist with reconnaissance and logistics. AI also helps analyse intelligence by processing data to identify threats and support decision-making. These systems span both offensive and defensive roles, supporting frontline operations and broader strategic efforts.

Defence experts agree on AI's growing role in defence, although opinions differ on its implications. One expert argues that AI will fundamentally alter the nature of warfare, while others focus on more specific, incremental changes in weapons technology. Some experts even speak of an existential threat to humanity or a 'race to extinction'. However, predicting AI's impact on military systems and operations is challenging. The effectiveness of any new military technology depends not just on its capabilities but also on innovative ways to use it. For instance, while tanks were introduced in World War I, their full potential was only realised with the blitzkrieg strategies of World War II. Similarly, military AI's transformative potential will depend on the development of new doctrines, organisational adjustment and training regimes. AI is a rapidly evolving field, with advances often driven by the civilian sector. This complicates predictions of when and how its military applications will mature. This interconnected progress also makes it difficult to predict the trajectory of military AI, although its transformative potential is undeniable.

Global AI arms race: China, Russia and the United States

In 2017, Russian President Vladimir Putin declared 'whoever becomes the leader in this sphere [AI] will become the ruler of the world'. A global arms race has emerged, driven by both the potential and dangers of AI-powered weapons. Major powers such as the United States, Russia, and China are actively advancing a suite of emerging military technologies to maintain or enhance their strategic capabilities.

The **US military** has long relied on technological superiority for national security. The 2018 and 2022 US National Defense Strategies highlight AI as critical for maintaining military superiority. The 2018 strategy emphasises AI's role in enhancing defence operations, while the 2022 strategy stresses the importance of swiftly adopting commercial AI technologies to stay ahead of competitors. Both strategies recognise AI as essential for modernising defence capabilities and ensuring the US retains its technological edge. The US military is investing heavily in AI to enhance national defence. Analysis finds that defence innovation funding (part of which is spent on AI projects) represented US$34 billion of the US national security budget for 2022, about 4 % of the total. The US Department of Defense's unclassified AI investments have increased, from slightly over US$600 million in 2016 to about US$1.8 billion in 2024, with more than 685 active AI projects currently underway.

The US Department of Defense has focused on integrating AI across intelligence, surveillance, reconnaissance (ISR), logistics, cyber operations, and autonomous systems. One of the most significant initiatives is the Joint Artificial Intelligence Center (JAIC), established in 2018 to coordinate AI efforts and develop applications for military use. In 2021, the JAIC was integrated into the newly created Chief Digital and Artificial Intelligence Office (CDAO), which now oversees AI strategy across the Pentagon. The Department also released a Data, Analytics, and Artificial

Intelligence Adoption Strategy in 2023, aiming to accelerate the integration of advanced AI capabilities to maintain decision superiority for US forces. The Defence Advanced Research Projects Agency (DARPA) is another major player, running multiple AI-driven programmes, such as the Air Combat Evolution (ACE) project, which aims to enhance autonomous air-to-air combat capabilities. Concrete examples of AI-enabled weapons systems include the MQ-9 Reaper drone, which uses AI for target identification and tracking, and the Sea Hunter, an autonomous naval vessel designed for anti-submarine warfare. AI is also being incorporated in Project Maven, which uses machine learning to analyse vast amounts of intelligence, surveillance, target acquisition and reconnaissance (ISR) data. Looking forward, US Secretary of Defense Pete Hegseth emphasised that defence AI investments will be prioritised by the Pentagon.

China is widely regarded as the primary competitor to the US in the global AI industry. Finding comparable spending data for Chinese defence AI spending is difficult, owing to limited public transparency – China's research and technology (R&T) budget has been called a 'black box' and 'murky'. However, analyses suggest that the People's Liberation Army (PLA) is investing significantly in AI, potentially matching or even exceeding US Defense Department expenditure. Analyses of China's defence budget suggest that actual defence spending is 40 % to 90 % higher than publicly announced figures, bringing the total estimated defence expenditure for 2024 to approximately US$330 billion to US$450 billion, part of which would be spent on R&T. China's 2017 'Next Generation AI Development Plan' identifies AI as a strategic priority and a focal point of global competition. Advances in language processing and facial recognition support its ambitions, particularly through integration with domestic surveillance. China is also developing autonomous military vehicles and swarm technology to overwhelm missile defences. AI is central to President Xi Jinping's goal of making the PLA a 'world-class' military by mid-century.

Russia lags well behind the US and China in AI development but has outlined a national strategy to bridge this gap. This strategy sets five- and ten-year goals focused on enhancing AI expertise, education, datasets, infrastructure, and regulations. Russia has also unveiled a ten-year military AI plan focused on fielding autonomous weapons. As part of its ongoing military modernisation efforts, Russia aims to automate 30 % of its military equipment by 2025. Russia sees AI as crucial for maintaining military superiority in an evolving battlefield. The Russian government, particularly the Ministry of Defence, has prioritised AI research, development, testing, and evaluation (RDT&E) to enhance combat capabilities. AI is viewed as a force multiplier that can improve command and control, intelligence gathering, decision-making, and autonomous weapons systems. While Russia's military AI ambitions are clear, the operational success of these technologies in the field remains difficult to determine due to their highly sensitive nature. The ongoing war in Ukraine has significantly shaped Russia's military AI strategy, underscoring the importance of AI-enabled systems in modern warfare. Russian forces actively seek to leverage AI for surveillance, targeting, electronic warfare, and unmanned systems. Similar to China, Russia's defence budget is also unknown.

Some experts warn that there can be no winners in an AI arms race and underline that the world's superpowers must work together to make sure that AI benefits humanity rather than destroying it. They underline that the US and China must move beyond a military-first approach to AI and prioritise its use for healthcare, education, and climate solutions. International cooperation is essential to AI governance, with shared ethical and safety standards to prevent misuse, such as misinformation and cyberattacks.

Role of civilian AI companies in the AI arms race

A significant number of ground-breaking innovations originated in the defence industry. Radar was invented in the UK in 1935, and in the 1960s and 1970s the US developed the internet, computer chips, and global positioning system for military purposes, all of which were later adapted for civilian use. In recent decades, much of this innovation has originated in the civilian AI sector. For instance, the costly development of the most advanced computer chips is possible primarily thanks to their

initial **commercial application**, ranging from computer games to AI. A recent example of civilian AI transfer to the defence sector is the collaboration between OpenAI and defence start-up Anduril. This partnership aims to enhance air defence and improve drone threat assessment.

Indeed, **major global technology companies** play an essential role in the 'global AI arms race', emerging as pivotal geopolitical actors, and wielding influence that rivals or even surpasses that of nation states. The CEOs of major tech companies featured prominently at President Donald Trump's inauguration. One of the president's first actions was to launch the US$500 billion 'Stargate Project' to build AI infrastructure in the US. Shortly thereafter, a little-known Chinese AI start-up, DeepSeek, triggered a US$1 trillion stock market loss after releasing its advanced AI model, R1, which rivals top US models at a fraction of the cost. Firms such as Alphabet (Google), Amazon, Apple, Meta, Microsoft, Palantir and China's Alibaba, ByteDance and Tencent possess resources and capabilities that significantly impact international stability and the dynamics of war and peace. Their decisions can alter the course of conflicts, as evidenced by Elon Musk's Starlink satellites providing critical communication support during the war in Ukraine. Today's tech giants operate with a level of autonomy unprecedented in history. They often outpace governmental agencies in innovation, particularly in AI. The influence of private tech companies extends beyond economic and technological domains into the realm of international security. Their control over critical infrastructure, data, and communication networks grants them a strategic position that can affect national security decisions. One academic recommends that governments and private tech companies adopt stronger, more collaborative relationships to ensure security, innovation, and effective regulation, while recognising the increasing role of these companies in global power competition.

European Union and AI in defence

The geopolitical significance of AI systems has gained increasing attention at EU level, where they are viewed as a key instrument of economic, political, and military influence. This aspect has been particularly relevant in recent debates on enhancing Europe's 'strategic autonomy' and 'technological sovereignty', aligning with initiatives led by the current European Commission, which positions itself as 'geopolitical'. This focus is unsurprising, given the complexities of integrating critical technologies such as military AI into European security and defence frameworks. In recent years, the Commission has expanded its role in defence through market-driven and industrial initiatives aimed at enhancing the competitiveness and innovation of the European defence technological and industrial base (EDTIB). Additionally, it has increasingly integrated civilian science, technology, and innovation programmes with the EU's security and defence R&D policies, particularly in advancing critical dual-use technologies.

At Versailles in March 2022, EU leaders committed to substantially increasing defence expenditure, investing in critical and emerging technologies and innovation for security and defence, and fostering synergies between space, civilian and defence innovation and research. These commitments were later reiterated in the Strategic Compass. The March 2024 European defence industrial strategy also calls for increased defence innovation. Andrius Kubilius, the European Commissioner for Defence and Space, has emphasised the critical need for Europe to develop its own capacity in key technologies, including AI, to enhance its defence capabilities. In doing so, he will build on several recently launched defence innovation initiatives.

According to the March 2025 white paper on 'European Defence Readiness 2030', geopolitical rivalries have sparked both an arms and technology race, with AI, quantum, biotech, robotics, and hypersonics driving economic growth and military dominance. To stay competitive, innovation must be balanced with tighter controls on tech diffusion to protect national security, as strategic rivals ramp up investment. 'AI, Quantum, Cyber & Electronic Warfare' is one of seven priority areas critical to building robust European defence. The white paper also emphasises the urgent need for Europe to enhance its defence capabilities by embracing disruptive technologies. To strengthen defence readiness, EU Member States should enable the European defence industry to design, develop, and

deliver technologies faster and at scale. This requires greater investment in defence R&D, particularly through common European projects and innovative industrial processes such as AI, additive manufacturing, and distributed design. Given the blurred line between civilian and military tech, leveraging Europe's broader innovation ecosystem (especially in deep tech) is critical. The EU will launch a European armament technological roadmap, initially prioritising AI and quantum, to boost strategic autonomy and avoid technological dependence. Additionally, The ReArm Europe Plan/Readiness 2030, announced by President von der Leyen, aims at rapidly strengthening EU defence investment and capabilities by mobilising up to €800 billion. It focuses on unlocking national public defence spending, launching a SAFE (security action for Europe) instrument for urgent joint procurement (up to €150 billion in loans backed by the EU budget), and leveraging the European Investment Bank Group alongside the accelerated Savings and Investments Union to attract private capital. A substantial part of these increased funds could potentially be dedicated to defence innovation, with AI specifically being mentioned for the SAFE instrument in the white paper. AI could also potentially improve efficiency in defence, which is important, as European defence spending has been criticised for inefficiencies stemming from fragmentation, duplication, and underinvestment. An EPRS study estimates that the 'cost of non-Europe' in defence spending ranges from €18 billion to €57 billion annually.

When comparing the EU with major global powers in terms of **defence innovation spending** (particularly AI), it becomes evident that the EU has a long way to go. The EU and its Member States allocate **€14.4 billion annually to military research and development** (which includes research and technology spending), a fraction of the **€130 billion spent by the United States – ten times more**. While it is of course not strictly comparable, Google spends almost ten times more than the combined research and technology budget of the 27 EU Member States. To make matters worse, this limited funding is spread thinly across fragmented efforts, with each Member State pursuing its own priorities and working in isolation. The fact that Europe is absent from the top 15 global tech companies is also concerning. In 2023, private investment in US AI reached €62.5 billion, while Europe (the EU and the United Kingdom) attracted only about €9 billion, and China €7.3 billion. Positively, however, the most recent European Defence Agency data show that R&T spending has been on an upward trend in recent years. After a period of underspending between 2008 and 2016, R&T expenditure has significantly increased (since 2016, Member States have nearly tripled their R&T investments), highlighting a growing emphasis on this sector. In 2023, total defence R&T spending reached €4 billion, marking an 8 % real-term increase from 2022. However, R&T spending as a share of total defence expenditure only stood at 1.4 %, which still falls short of the 2 % benchmark established in 2007 within the framework of the European Defence Agency. Furthermore, R&T spending remains highly concentrated, with two Member States accounting for over 80 % of the EU's total expenditure. More positively, projections for 2024 suggest that defence R&T spending could potentially reach €5 billion. Venture capital investment in European defence and security start-ups also surged by 24 % in 2024 to US$5.2 billion.

The **European Defence Fund** allocates 4 % to 8 % of its annual budget to emerging disruptive technologies (EDTs), including AI technologies. For instance, in the first round of selected proposals (2021 call), over 5 % of the budget was allocated to EDTs. Several successful project proposals, awarded funds under the 2021 EDF call, incorporate AI elements. These include applications in cyber defence operations, intelligent automation, knowledge extraction, frugal learning (developing high-performing machine learning algorithms with minimal data and energy efficiency) for quick AI system adaptation, intelligent and cooperative manned and unmanned land systems, AI-based language solutions, and innovative automated video detection algorithms. The Strategic Technologies for Europe Platform (STEP) is providing a €1.5 billion boost for 2024-2027, further enhancing investment in digital technologies and deep-tech innovation. Under the existing EDF Regulation (and the European Defence Industry Reinforcement through Common Procurement Act (EDIRPA) and Act in Support of Ammunition Production (ASAP)), even LAWS could in theory already qualify for EU funding. However, according to the EDF Regulation, any research project involving autonomous weapons must involve meaningful human control. The EDF Regulation specifies that

the eligibility of projects related to new defence technologies should align with developments in international law. As such, the development of LAWS that lack meaningful human control over selection and engagement decisions for strikes against individuals should not qualify for funding. This is without prejudice to the potential funding for actions aimed at developing early-warning systems and countermeasures for defensive purposes. However, the precise definition of meaningful human control and the concept of military AI have sparked significant international political and academic debate and remain contentious.

European Defence Agency (EDA)

The **EDA** has been involved in defence innovation since its inception in 2004. EDTs (including AI) are one of its core research and technology activities. The EDA has recognised the critical need to incorporate cutting-edge civilian technology into EU defence research and development, as these technologies have advanced rapidly. The EDA emphasises the importance of integrating 'innovative resilience' into military systems, ensuring that armed forces can adapt and incorporate new technologies throughout their lifecycle to avoid obsolescence. This includes AI, which is identified as a key enabler for military capabilities, improving decision-making, real-time situational awareness, operational efficiency, and predictive battlefield assessments. The EDA has also established initiatives like the AI in defence action plan and strategic research agenda to create a clearer understanding of AI within the defence sector. These efforts address varying interpretations of AI among EU Member States, aiming to develop a common vocabulary. Three key initiatives led by the EDA stand out. The first is a project focused on creating an EU-wide pool of defence data, based on principles such as data sovereignty, security, trust, interoperability, and the portability of data and services. The second project aims to examine the requirements for AI systems trusted in defence, including technical robustness, safety, traceability, accountability, and data governance rules. The third initiative involves mapping out the requirements for a unified EU framework to validate and certify military AI systems, considered a crucial step towards a more cohesive approach.

In 2022, a **European Defence Innovation Hub (HEDI)** was launched within the EDA to enhance the agency's innovation activities, and catalyse new activities jointly with Member States and stakeholders. It was one of the first concrete Strategic Compass deliverables. Although HEDI's primary role in defence innovation is identifying ideas, connecting innovators, and promoting innovative solutions, it also has a practical component. It provides funding for defence innovation prizes, proof-of-concept development, European defence innovation shows, and innovation challenges – an R&T methodology designed to rapidly transition from proof-of-principle to a minimum viable product. The EDA Defence Innovation Prize stimulates the engagement of mainly non-traditional defence R&T communities in generating innovative ideas; the 2020 Defence Innovation Prize was awarded to the SWADAR project, which focuses on AI-enabled drone swarm tracking. This technology provides military commanders with an operational view of swarm attacks by recognising and learning new swarm behaviours, highlighting the role of AI in modernising defence capabilities.

The EU is **promoting synergies between civilian and defence research and innovation**. Unlike many revolutionary innovations such as the internet, initially developed by the military, innovation in AI is mostly civilian sector-driven. A European Commission action plan seeks to increase complementarity between EU programmes such as Horizon Europe and the EDF to leverage the disruptive potential of technologies at the intersection between space, defence and civil use. A roadmap on critical technologies for security and defence outlines how the EU can enhance research, technology development and innovation in critical technologies and reduce strategic dependencies. The roadmap aims to strengthen synergies between civilian and defence R&D, enhancing the EU's security and defence sectors' competitiveness and resilience. Civilian AI factories, collaborative hubs designed to accelerate AI innovation across Europe by bringing together computing power, data, and skilled talent connect universities, supercomputing centres, industry, and financial actors to drive AI advances in health, manufacturing, climate, and finance.

As part of a broader effort to establish Europe as a global leader in AI, the Commission has prioritised the rollout of AI factories, with the first wave (seven sites in 15 Member States and two EuroHPC

(High-Performance Computing Joint Undertaking) partners) set to launch in April 2025, with €1.5 billion in funding. In March 2025, six additional AI factories were announced in Austria, Bulgaria, France, Germany, Poland, and Slovenia, supported by a further €485 million. While the AI factories are for civilian AI applications, the technological advances and infrastructure they create could indirectly support defence-related innovation, as in deep tech the line between civilian and military applications is increasingly blurred. This means civilian start-ups and research outcomes can make vital contributions to advanced solutions that boost military effectiveness and readiness. However, despite Europe's strong technological base, it has yet to fully harness this potential for defence advantage.

An **Observatory on Critical Technologies** was created within the European Commission to identify critical technologies for space, security, defence, and public order. In February 2023, the Observatory announced it had identified risks related to autonomous systems and electronic components. Specific technology roadmaps were created to reduce these risks and find remedies in 2023. According to the European External Action Service (EEAS), there are still more initiatives underway in the defence sector to identify strategic dependencies. A first classified report by the Observatory on critical technologies for civil-defence-space industries contains detailed findings on electronic components. A second report is currently being finalised.

The EU has also launched an **EU defence innovation scheme (EUDIS)**. With a financial envelope of €2 billion (€1.46 billion from the EDF, €90 million in co-funding from the Member States, and €400 million to €500 million from other public and private sources), the scheme supports innovation and entrepreneurship on essential technologies for the European defence industry. The EUDIS funds initiatives such as defence hackathons across Europe, supports the establishment of innovation test hubs, and promotes the application of civil research for military use; it aligns with the EU's 2021 action plan on synergies between civil, defence, and space industries. Technologies used in defence applications, such as microelectronics, high-performance computing, quantum and cloud computing, artificial intelligence, cybersecurity, robotics, 5G, and advanced connectivity, are also expected to be eligible for funding under STEP. Additionally, EUDIS fosters business coaching and partnership matchmaking to enhance collaboration and innovation. The EDF's National Focal Points (NFPs) in EU Member States and Norway play a key role in implementing EUDIS by engaging with stakeholders and providing guidance to potential applicants and beneficiaries of the EDF programme. In 2024, the scheme awarded €225 million to about 400 companies.

EU-NATO cooperation

Both the Strategic Compass and the new NATO Strategic Concept mention EDTs, which includes AI, as an area where deeper cooperation will be pursued, with experts deeming it to be an opportunity for EU-NATO cooperation. It is also included as a new area of cooperation in the third EU-NATO joint declaration. NATO has made large efforts in this area by launching the Defence Innovation Accelerator for the North Atlantic (DIANA), and endorsing an EDT strategy. Operating as a distinct NATO entity, DIANA has its own legal and financial framework, overseen by a board comprising representatives from academia, the private sector, and the governments of NATO member states. This board determines annual focus areas, such as the 2023 pilot challenge programmes, which targeted energy resilience, secure information sharing, and sensing and surveillance. Similar to EUDIS, DIANA provides both financial and technical support, including mentoring and access to specialised test centres and accelerators across NATO countries. Additionally, it is linked to a separate venture capital initiative, the NATO Innovation Fund, which allows governments to invest flexibly through their foreign or defence ministries. This governmental initiative aims to raise €1 billion over a 15-year period to drive innovation. In July 2024, the EIF partnered with the NATO Innovation Fund following the signing of a Memorandum of Understanding in Brussels. It outlines a framework for enhanced collaboration, aiming to boost funding for start-ups, SMEs, and midcaps in the defence, security, and resilience sectors. In 2021, NATO also released an AI strategy, which was revised in 2024. NATO's revised AI strategy emphasises the rapid integration of emerging AI technologies, such as generative AI, to enhance defence capabilities. The strategy outlines four primary aims: promoting responsible AI use for defence, accelerating AI adoption to improve interoperability, safeguarding AI technologies and managing associated risks and countering threats from adversarial AI.

Furthermore, in January 2024 the €175 million **Defence Equity Facility (DEF)** was created under InvestEU. It is managed by the European Investment Fund (EIF) on behalf of the European Commission's Directorate-General for Defence Industry and Space (DEFIS). The DEF is designed to support venture capital and private equity funds investing in European companies developing innovative defence technologies with dual-use potential. All investments must comply with the EIF's exclusion and restriction policies. Funding for the DEF includes a €100 million contribution from the EDF and an additional €75 million from the EIF, with a four-year investment period running until 2027. The facility aims to generate up to €500 million in investment, including private sector contributions.

Permanent Structured Cooperation (PESCO) – a legal framework to deepen defence cooperation between its 26 Member States – is also being leveraged to coordinate AI development. Several PESCO projects are integrating artificial intelligence (AI) to enhance defence capabilities. For example, the 'automated modelling, identification, and damage assessment of urban terrain' (AMIDA-UT) project is developing an automated system for rapid mapping and identification of target structures, which supports decision-making and training activities.

Defence AI in the Member States

There is also an increase in defence AI activities in EU Member States. For instance, in **France** AI is a 'priority for national defence'. In April 2019, the French Ministry of Armed Forces introduced a strategy for AI in defence, emphasising responsible and controlled use of AI technologies to enhance military capabilities. In 2022, it approved the final phase of the Artemis big-data processing platform, designed to enable autonomous operations in the intelligence, command, and digital domains. In March 2024, France revealed plans to redirect €2 billion from the 2024-2030 defence budget towards AI. France plans to build Europe's most powerful classified supercomputer to take the lead in AI for defence purposes. Armed Forces Minister Sébastien Lecornu has argued that France must become a global leader in military AI. In May 2024, France established the Ministerial Agency for Artificial Intelligence in Defence (MAAID), with a budget of €300 million. In the private sector, major defence contractor Thales files the most AI-related patents for critical systems in Europe. Its in-house AI accelerator, cortAIx, integrates AI into sensors and complex systems, enhancing data analysis, decision-making, and object detection while ensuring cybersecurity and operational efficiency. French defence start-up Mistral has recently teamed up with German defence tech start-up Helsing to developed advanced military AI systems.

Another example is **Germany**, where the government has also pledged to increase AI research and development in defence. Germany's Ministry of Defence outlined its approach to defence AI in a 2019 concept paper, viewing AI as a tool to enhance decision-making, streamline processes, and improve mission readiness. According to an expert, Germany's defence AI initiatives prioritise augmenting the survivability of the Bundeswehr (German military) rather than increasing its lethality. The Defence AI Observatory (DAIO), based at Helmut Schmidt University, plays a crucial role in analysing AI applications within the Bundeswehr, helping guide strategic planning. The Bundeswehr Cyber Innovation Hub (CIHBw) drives digital transformation in the armed forces by developing software-driven defence technologies to enhance resilience. In the private sector, companies like Helsing are developing AI software to enhance weapons systems and improve battlefield decision-making. Founded in 2021, Helsing has partnered with defence firms such as Rheinmetall and Saab to integrate AI into existing military platforms. The company made international headlines when it raised €450 million in venture capital funding in 2024.

Ethics of AI in warfare

The integration of AI into warfare raises several important ethical concerns. One significant issue is accountability and responsibility. Determining who is responsible when AI systems make autonomous decisions is complex. If an AI system causes unintended harm, assigning liability becomes challenging, leading to concerns about accountability in military operations.

Another key consideration is compliance with international law. This relates to AI systems' adherence to principles such as distinction (ensuring combatants and civilians are properly differentiated) and proportionality (ensuring military actions are proportionate to the threat). Ensuring that AI systems can effectively follow these principles is essential to ensure compliance with international law. Human oversight therefore remains critical in the use of AI in warfare. While AI can enhance decision-making speed and accuracy, maintaining human judgement in the decision-making process is essential to ensure that ethical standards are upheld. AI also has the potential to escalate conflicts. By lowering the risks to a state's own troops, such systems may also lower the political barrier to deploying or using force. While they offer the advantage of rapid operational response, this often comes at the cost of substantive human oversight. These characteristics can increase the likelihood of conflict escalation due to swift, machine-led interactions.

Lastly, ethical concerns around the developers of AI technologies also arise. Companies creating AI for military applications face dilemmas regarding the potential misuse of their products. Human Rights Watch recently expressed deep concern when Google's parent company, Alphabet, lifted its long-standing ban on using AI for developing weapons and surveillance tools. The company has revised its AI usage guidelines, removing a section that previously excluded applications deemed 'likely to cause harm'. The human rights group criticised the move, noting it could 'complicate accountability' in military decisions that have life-or-death implications. In response, Google defended the decision, stating that businesses and democratic governments must collaborate on AI that 'supports national security.'

One ethicist argues that using robots in warfare is unethical for two reasons. First, robots reduce risks to such an extent that future wars may become more frequent, as human fatalities often serve as a deterrent by applying political pressure on governments. Second, robots cannot reliably distinguish between combatants and non-combatants, increasing the risk of civilian casualties. On the other hand, robotic soldiers could reduce human casualties by removing soldiers from the battlefield and adhering to military doctrines without emotional interference. However, the critical debate lies in whether robots should be allowed to make autonomous decisions about taking human lives or if humans should retain ultimate decision-making authority. While opinions remain divided, another ethicist notes the use of robots in combat is likely inevitable. Emphasising the importance of adhering to international humanitarian law in the deployment of AI in warfare, another expert argues that the use of AI must be regulated to ensure compliance with established legal frameworks that govern armed conflict. This includes upholding principles such as distinction, proportionality, and necessity to protect non-combatants and prevent excessive harm. The author calls for the development of comprehensive regulations to address the unique challenges posed by AI technologies in military contexts.

Defence AI regulation

The rapid advance of military AI has intensified global calls for regulation, with international debates highlighting the lack of a unified framework. At the February 2025 Paris AI summit, US Vice President JD Vance urged a more flexible, innovation-friendly approach to AI regulation and criticised the European approach. Indeed, the decision whether to regulate 'has become a hot geopolitical issue'.

During the Biden Administration, the US was proactive in establishing ethical principles for AI use in defence, emphasising key tenets such as responsibility, equitability, traceability, reliability, and governability. The US Department of Defense (DOD) issued a Responsible Artificial Intelligence (RAI) strategy and implementation pathway, which provides governance guidelines, training for the defence workforce, and lifecycle management protocols for AI systems. To ensure security and compliance with international law, the DOD has developed testing and evaluation frameworks that aim to safeguard AI systems from adversarial manipulation and assess their reliability in operational contexts. The US also proposed a non-binding Code of Conduct for Lethal Autonomous Weapon Systems to encourage responsible behaviour and adherence to legal standards, but opposed any pre-emptive ban on LAWS. In February 2023, during the Summit on Responsible Artificial

Intelligence in the Military Domain (REAIM) in The Hague, the US Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy provided a normative framework to guide the ethical and responsible development, deployment, and use of AI in military settings. It emphasises compliance with international law, particularly international humanitarian law, and underscores the importance of maintaining human accountability in AI-enabled military operations. As of November 2023, 45 countries have endorsed this declaration. However, as one expert puts it, 'President Trump torpedoed Biden-era approaches to regulating AI'. Upon re-election, Trump signed an Executive Order aimed at enhancing America's leadership in AI, revoking previous Biden-era AI policies, viewed as restrictive to innovation. The new directive mandates the creation of an AI action plan to bolster US dominance in the field, including in national security.

Regulation of defence-related AI technologies at the international level has been addressed by several organisations and frameworks. The United Nations (UN) Convention on Certain Conventional Weapons (CCW) has hosted discussions on LAWS since 2014. These discussions have seen advocacy from some member states and non-governmental organisations for a pre-emptive ban on such systems due to ethical concerns about their use. However, achieving consensus has been challenging, as some countries oppose outright bans, instead favouring regulation or codes of conduct. As noted above, the US opposes a pre-emptive ban, arguing that these systems could offer humanitarian benefits and that existing international humanitarian law (IHL) is sufficient to govern their development and use. Russia similarly rejects a ban, contending that LAWS might improve targeting accuracy and reduce civilian casualties while noting that there is no legal precedent for banning an entire class of weapons pre-emptively. Meanwhile, China supports a ban on the use (but not the development) of LAWS, defining them as fully autonomous, indiscriminate lethal systems without human oversight, a definition that many argue would make such weapons inherently illegal under IHL, with some analysts viewing China's stance as strategically ambiguous.

In December 2024, the UN Security Council debated the use of AI in conflict. UN Secretary-General António Guterres warned against misuse of AI in warfare. He noted that recent conflicts have essentially turned into proving grounds for military AI applications, with algorithms used in life-and-death decision-making. He warned that 'artificial intelligence without human oversight would leave the world blind – and perhaps nowhere more dangerously and recklessly than in global peace and security', and emphasised the urgent need for 'unprecedented global cooperation' to reduce AI governance fragmentation. The UN High-Level Advisory Body on AI has created a blueprint addressing both the significant risks and opportunities AI presents, including laying the groundwork for a framework that ties together existing initiatives and ensures all nations can contribute to shaping the digital future. Guterres urged member states to act quickly in forming an international scientific panel on AI and launching a global dialogue on AI governance within the UN, as outlined in the UN Global Digital Compact. Amid calls for a binding UN framework to regulate AI, some members, notably Russia, cautioned against imposing Western norms.

NATO released a revised AI strategy in 2024, which establishes standards for responsible use, protection from adversarial exploitation, and the accelerated adoption of AI in military operations. This updated strategy builds on the 2021 version, incorporating recent advances in AI, such as generative AI and AI-driven information tools. Key priorities include implementing NATO's Principles of Responsible Use, enhancing interoperability of AI systems across the Alliance, integrating AI with other emerging disruptive technologies, and strengthening NATO's AI ecosystem.

The EU is also increasingly engaging in AI governance; the **Artificial Intelligence Act (AI Act)**, adopted in December 2023, is the first binding worldwide horizontal regulation on AI. It aims to foster AI development while mitigating risks, positioning the EU as a global leader in trustworthy and democratic AI governance. The act focuses solely on commercial AI, explicitly excluding military applications and national security services. Indeed, during the negotiations some Member States, notably France, pushed for exemptions to preserve Europe's strategic autonomy, ensuring minimal restrictions on AI in defence and security. The newly established EU AI Office plays a central role in implementing the AI Act. While the act does not directly regulate military AI, it may still influence

defence AI policy, particularly in dual-use technologies like drones. The regulation introduces a risk-based classification for AI applications, imposing compliance obligations on suppliers. The act's 'human-centric approach' could shape future debates on LAWS within EU defence policy.

According to one expert, 'the AI act clearly states that one of its objectives is to guarantee the Union's technological sovereignty and strategic autonomy, which implicitly means that the Europeans are not about to adopt a restrictive approach to this technology in the military sector'. According to another analyst, the EU should create a framework for responsible AI in defence, using the AI Act's risk tiering as a model. A unified framework would demonstrate the EU's leadership in AI governance, addressing risks and ensuring the responsible use of AI in both military and civilian contexts. One expert highlights the need for stronger EU regulation of military AI, despite the AI Act exempting it from oversight. While the exemption is justified by national security concerns, it raises the urgency of establishing governance frameworks, given AI's dual-use potential in both civilian and military applications. Additionally, the claim that military AI should be regulated solely at national level is weakening. Since these technologies have cross-border implications and EU countries already collaborate on defence initiatives, a coordinated regulatory approach is necessary. Analysts have criticised the AI Act for potentially stifling innovation due to over-regulation, leading to reduced global competitiveness.

European Parliament position

The European Parliament has been a key player in the military AI debate, addressing the issue early on. It has adopted two major resolutions: one in 2018 focused on lethal autonomous weapons systems (LAWS), and another in 2021 covering both military AI and autonomous lethal weapons. Overall, the Parliament is rather open to military AI use and recognises AI's strategic importance and potential to protect soldiers and civilians. Members emphasise three key principles for military AI: (1) maintaining human involvement in command and control, (2) ensuring legal accountability for individuals and states, and (3) advocating for international AI governance through the UN, including export regulations.

However, on LAWS, the Parliament has consistently urged the Council to prevent the development and use of LAWS that operate without meaningful human control and to push for their global prohibition. Specifically, it wants the Council to engage in UN negotiations under the Convention on Certain Conventional Weapons to regulate military AI and ban fully autonomous weapons. The 2021 resolution emphasises the need for the EU to develop a comprehensive framework to regulate AI technologies, ensuring they align with international law and uphold fundamental rights. It highlights the importance of ethical guidelines, transparency, and accountability in AI deployment, particularly in areas affecting public administration and military operations. The Parliament calls for Member State cooperation to establish common standards and practices for AI use, promoting innovation while safeguarding ethical principles and legal norms.

The Parliament endorsed the Artificial Intelligence Act in 2023. This legislation explicitly excludes national security, defence, and military purposes from its scope, reflecting a cautious approach to AI in defence sectors. The Parliament also set up a Special Committee on Artificial Intelligence in a Digital Age (AIDA), although military AI was not its focus. Its final report acknowledges that AI serves as a dual-use technology with both civilian and military applications. It emphasises the necessity for clear governance and ethical guidelines to ensure responsible AI use in the security and defence sectors. The report also highlights concern about the EU potentially lagging behind other global powers in AI development, including military applications, and stresses the importance of European technological sovereignty. Additionally, it raises concern regarding the development of LAWS without meaningful human control, advocating for international regulation to prevent their misuse. The report discusses AI's role in enhancing cybersecurity and addressing hybrid threats, urging the EU to develop robust AI-powered cybersecurity measures. Furthermore, it encourages collaboration with international partners, including NATO, to support multilateral efforts to regulation the military use of AI.

MAIN REFERENCES

Congressional Research Service, Emerging Military Technologies: Background and Issues for Congress, February 2024.

Franke, U., Artificial Intelligence Diplomacy: AI governance as a new EU external policy tool, European Parliament Study requested by the AIDA Committee, June 2021.

Csernatoni, R., Charting the Geopolitics and European Governance of AI, Carnegie Europe, March 2024.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

https://eprs.in.ep.europa.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)