Research Paper

International Security Programme

April 2026

How a surge in defence and dual-use technology investment could reconfigure the global AI race

Katja Bego

CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is a world-leading policy institute based in London. Our mission is to help governments and societies to build a secure, sustainable, prosperous and just world.

Contents

	Summary	**2**
01	**Introduction**	**4**
02	**How current trends could lead to a more securitized, multipolar AI race**	**9**
	Trend 1: A ‘boom’ in dual-use and defence tech	10
	Trend 2: The rise of ‘patriotic tech’ and the blurring of boundaries between civil and military	16
	Trend 3: The pursuit of sovereign AI	21
	Trend 4: Growing concerns about a potential AI valuation bubble	28
03	**How can the private sector prepare? Likely outcomes and recommendations**	**33**
	About the author	**41**
	Acknowledgments	**41**

Summary

- While the US and China still dominate AI development, rising geopolitical tensions, a growth in dual-use AI and increasing concerns over technological dependencies are pushing more countries to develop their own AI capabilities and 'chokepoints'. Over time, a multipolar, but also securitized and fragmented, AI landscape may emerge as a result. This paper analyses four prominent trends from 2025 and early 2026 that are driving this dynamic, and argues that they have the potential to significantly reconfigure the AI race.
- Investment and deployment of dual-use defence AI are accelerating globally. High levels of defence spending and an investment boom in dual-use AI may provide an opportunity for smaller and middle powers to catch up with the dominant players, and could generate spillovers that could help smaller markets mature and develop competitive niches.
- Commercial AI firms are increasingly embedded in national security and defence ecosystems (a trend referred to in this paper and elsewhere as 'patriotic tech'). This deep integration can boost strategic capacity, but risks creating a powerful tech-military complex that could increase geopolitical distrust and accelerate decoupling.
- Concerns among governments over sovereignty and increasing alignment between state and tech industry interests are also reshaping the global AI ecosystem. Governments are beginning to prioritize 'sovereign AI' and deeper partnerships with domestic tech firms, leading to tighter integration between commercial and military sectors, growing distrust and – over time – the potential emergence of a greater number of competing, politically aligned AI blocs.
- High levels of AI infrastructure spending are increasingly questioned by investors, raising fears of a valuation bubble. A market correction could shift focus away from expensive frontier models towards open-source and other AI that are cheaper to deploy – enabling smaller companies and countries to compete through adoption and application, rather than chasing the frontier.
- While a more geographically diverse AI marketplace could bring new sources of innovation and funding, expand the range of solutions available to consumers and reduce dependence on a small number of dominant countries and firms, it may also lead to a scenario in which different regions or states develop incompatible 'sovereign' technology stacks in pursuit of national security and self-reliance.

- A more securitized and multipolar AI market also introduces new risks, including greater instability, reduced interoperability, and heightened exposure to geopolitical tensions or even bad actors.

Recommendations

- In this future scenario, companies would face a range of new risks. This paper presents a series of recommendations on how they can prepare. These recommendations include:
  - **Establishing dedicated geopolitical risk functions.**
    The aim would be to create permanent capabilities to monitor geopolitically motivated operational risks, including 'buy local' policies and government efforts to bolster tech sovereignty, and to assess how technology stacks can be made more resilient or diversified.
  - **Conducting regular 'tech decoupling' stress tests.**
    These tests would model the implications of a sudden loss of market access or forced supply-chain and infrastructure decoupling (e.g. moves towards sovereign AI clouds), and map technological and supply-chain dependencies to identify vulnerabilities.
  - **Developing infrastructure architectures compatible with sovereignty requirements.**
    Efforts should lead to systems that can be replicated across jurisdictions and comply with data-localization rules, ensuring compatibility with multiple infrastructure providers and AI solutions while identifying high-risk areas (e.g. the storage of sensitive data).
  - **Structuring operations to enable legal and operational separation across regions.**
    Companies must adapt their corporate structures and technology stacks to allow for genuine regional separation, diversify inputs and avoid reliance on single providers – while mitigating valid perceptions of 'sovereignty washing'.
  - **Investing in cybersecurity, resilience and crisis preparedness.**
    A more fragmented, contested and AI-enabled technology sphere will see the barriers for kinetic and cyberattacks lowered. Efforts should be targeted, in particular, at enhancing in-house cyber capabilities, building redundancy, 'airgapping' critical systems, and improving data security practices, while mapping vulnerabilities in physical infrastructure and developing crisis protocols in coordination with governments.

01 Introduction

The global AI race, long dominated by the US and China, may become more fragmented and multipolar if current trends continue. This development would enable a wider range of countries to develop competitive AI ecosystems.

The AI race is frequently presented as a race between the US and China, in which other countries may be able to build specific niches, but will ultimately remain reliant on the solutions and underpinning infrastructure provided by either of the two superpowers. At present, the US and China remain firmly in the lead when it comes to the development of frontier AI – with most research, investment, computing power, infrastructure availability, talent, patents and new product deployment centred around those two markets. Other countries are usually afforded little agency in this framing.

As the global security order deteriorates, countries worldwide are becoming increasingly concerned that, in a more hostile, transactional new world, overreliance on others for pivotal technologies like AI is a source of profound vulnerability.

However, geopolitical tensions and the rapid securitization of the AI sphere may start to challenge the status quo. As the global security order deteriorates, countries worldwide are becoming increasingly concerned that, in a more hostile, transactional new world, overreliance on others for pivotal technologies like AI has become a source of profound vulnerability. This fear has led to a growing number of countries seeking trusted technology alternatives with greater urgency, and encourage efforts to bolster their domestic AI industries. The increasing level of entanglement between private sector AI companies and governments and militaries has begun to prompt similar concerns over external dependencies.

This evolving security environment also provides a catalyst for this change. High defence spending (which has already reached a level not seen since the early Cold War)[1] – with growing shares allocated to AI development – could see smaller markets benefit from spillover effects into their wider AI ecosystems and help their domestic solutions to achieve scale. A rapidly growing global ecosystem of 'dual-use'[2] AI solutions may similarly enable smaller countries and developers to gain a larger market share.

This paper argues that the dynamics described above may result in a more securitized, multipolar – and likely also fragmented – global AI industry, in which it will become more difficult for one or two actors to substantially dominate the value chain or the technology's wider rollout. To understand how this scenario may come about, the paper explores four important trends that accelerated in 2025 and early 2026, and which could start a shift towards a multipolar AI market:

1. **The dual-use and defence tech boom.** In 2025, interest and growth in the market for defence and dual-use AI applications accelerated. Though the majority of leading commercial AI companies are still based in either the US or China, the market for dual-use AI applications has the potential to become more geographically diverse. For example, the European Union (EU), Israel, South Korea, the UK and Ukraine are all developing their own increasingly vibrant ecosystems.[3] High levels of defence spending, mounting concerns over sovereignty and efforts by governments to put cutting-edge innovation at the heart of rearmament efforts, are all helping to fuel this growth.

   The growth of innovation ecosystems on the back of military spending would not be without precedent. Silicon Valley itself has its origins in defence contracting, with many of its technologies ranging from semiconductors to GPS – even the internet – having been built as part of Cold War military contracts. In the long term, spillover benefits from dual-use innovation, as well as ecosystem growth fuelled by increased government spending and domestic adoption of AI, could see smaller AI ecosystems become more mature and better able to compete.

2. **The rise of 'patriotic tech', blurring the boundaries between civil and military use.** 2025 was characterized by an increasingly more intimate relationship between AI companies and governments, with many commercial companies now willing to explore the defence and national security applications of their AI products. Though this is a global dynamic, the trend

---

1 Stockholm International Peace Research Institute (2025), 'Unprecedented rise in global military expenditure as European and Middle East spending surges', press release, 28 April 2025, https://www.sipri.org/media/press-release/2025/unprecedented-rise-global-military-expenditure-european-and-middle-east-spending-surges.
2 Dual-use is a somewhat ill-defined term, with its origins in early Cold War-era nuclear debates. This paper employs an expansive definition of dual-use AI considering the full spectrum of largely commercial to primarily military solutions (noting also that AI is not a monolith, but a large set of technologies and applications, all at different stages of development and maturity). On the civilian end of the spectrum are primarily commercially focused cloud services that also underpin militaries' AI-enabled systems. Commercial large language models (LLMs) are also increasingly adapted and embedded into military systems used for rapid intelligence analysis, command and control, and targeting. At the military end of the spectrum, some AI use cases may appear to have limited dual-use utility – for instance, innovations in AI-enabled targeting in drones or autonomous missiles. However, these solutions have relevance in, for example the oil and gas industry, where these systems could potentially be used to monitor remote, hard-to-reach installations.
3 StepUp Startups Consortium (2025), *The role of AI in the EU's dual-use technology field*, report, Brussels: European Commission, https://digital-strategy.ec.europa.eu/en/library/ai-enabled-dual-use-tech-and-role-eus-startup-ecosystem.

is especially visible in the US, driven not just by new defence tech companies entering the market, but also by established Silicon Valley 'hyperscalers' like Alphabet and Microsoft and frontier AI labs like OpenAI and Anthropic pursuing contracts with the US Department of Defense and allied defence ministries, and presenting themselves as working in support of US government (and, by extension, NATO) objectives.

Closer collaboration between tech companies and the military will likely draw in larger parts of the economy, which would especially benefit smaller markets that can then allocate finite resources more effectively towards shared strategic ends. This increased entanglement and mutual dependence may, however, give rise to a new powerful type of tech–industrial complex, with tech companies and militaries become increasingly mutually interdependent. Such a development could sow further distrust between countries, and encourage further decoupling efforts. The recent spat between the Pentagon and Anthropic also shows the perils of this kind of intimate relationship for the private sector.

3. **A global push towards sovereignty and decoupling of interdependencies.** Globally, there has been a clear push by governments to become more self-reliant in defence, AI and technology more widely. As the geopolitical climate grows progressively more tense and the geostrategic utility of having independent AI capabilities becomes more evident, many countries have started to reassess the composition of their technology stacks. This national security-driven reassessment has put a renewed focus on the development of sovereign capabilities and resilient supply chains (even if that comes at a higher cost or means a transition towards less mature solutions), as countries seek to disentangle themselves from a perceived over-reliance on foreign AI and AI infrastructure suppliers.

   This concern over sovereignty may see more competitive alternative AI ecosystems emerge. Rhetoric around sovereignty is also likely to become a growing source of friction between countries, as Washington and Beijing will seek to preserve the market positions of their respective AI 'champions'.

4. **Growing concerns about a potential AI valuation bubble.** Throughout 2025, concern became increasingly apparent over the levels of spending by and valuations of companies in the AI and wider tech industry. Large US-based hyperscalers continued to invest significant amounts – over $300 billion in 2025 alone – into new data centres, computing resources and other infrastructure to maintain an edge in the race to develop frontier AI capabilities.[4] Investors, meanwhile, are becoming more sceptical about the likelihood of frontier AI spending generating the promised financial returns.

4 Sriram, A. (2025), 'The great AI buildout shows no sign of slowing', Reuters, 31 October 2025, https://www.reuters.com/legal/transactional/great-ai-buildout-shows-no-sign-slowing-2025-10-31.

The securitization of the AI race may allow such high levels of spending to persist for longer, as geostrategic considerations can put pressure on governments to step in and keep the market afloat. The big AI spenders are already pursuing government contracts and support, further amplifying the trend towards 'patriotic tech' discussed above.

A potential market correction could, however, also lead to the geostrategic competition being reconfigured, as focus could move away from highly capital-intensive frontier AI development towards cheaper, open-source models.

As access to investment and cutting-edge infrastructure remains among the main barriers to smaller AI ecosystems catching up with the major players, a shift towards 'good enough' tech development, and rapid diffusion and adoption could allow more actors to gain a larger market share.[5] If the AI race is considered as three parallel races – the race towards the frontier (the development of the most cutting-edge AI), the race towards diffusion (spreading AI throughout the economy), and the race towards application (finding different use cases for the technology) – emphasis may shift towards the latter two. In these two races, China, but also smaller actors, will find themselves better positioned.

About this paper

The remainder of this paper is made up of two parts. The first part focuses on the four key trends outlined above. These four trends were selected on the basis of an extensive literature review, and were stress-tested by a diverse range of domain and regional experts.

The final part draws conclusions and presents recommendations on how the private sector can best prepare for a more geopolitically charged and multipolar AI environment. While the art of prediction is necessarily inexact, by extrapolating from ongoing trends and drawing on subject expertise, the paper seeks to provide decision-makers with the tools to better anticipate changes to their operational environment.

The paper focuses primarily on the political economy of AI, especially dual-use AI systems. Critical though other issues may be, the analysis does not extend to the ethical implications, or actual battlefield utility, of AI solutions. Nor does the paper seek to comment on how dual-use technologies should be governed.

Though this paper draws on existing trends and developments in AI, its conclusions and the trajectories it sets out are inevitably speculative. Many of the dynamics discussed remain uncertain, and are subject to a highly volatile geopolitical environment and rapidly evolving AI space, in which assessments of the technology's current state can become obsolete in months or even weeks.

5 Chow, V. (2026), Jeffrey Ding on why diffusion, not innovation, is the secret to victory in the AI race', *South China Morning Post*, 26 January 2026, https://www.scmp.com/tech/tech-trends/article/3340976/jeffrey-ding-why-diffusion-not-innovation-secret-victory-ai-race.

However, given the potentially transformative impact that securitization of AI may have on the global marketplace, and the reconfiguration of the AI race that may result, decision-makers in business (as well as in government and elsewhere) must be proactive in thinking about what this direction of travel may mean for their own operations.

02
How current trends could lead to a more securitized, multipolar AI race

A combination of a growing interest in dual-use technologies and government contracting, concerns over sovereignty and an AI valuation bubble could open up the global AI race to a wider range of competitors.

The following chapter is split into four subsections, each focusing on a significant trend in the AI sector observed in 2025 and early 2026. These sections identify specific dynamics that could result in a further securitization and levelling of the AI race. The section then analyses where those dynamics may lead. The trends under discussion include: the dual-use and defence AI boom; the rise of 'patriotic tech'; the growing push for sovereignty in AI and defence; and concerns over an AI valuation bubble in financial markets.

A lot can change in 12 months. This chapter therefore adopts a relatively short time-horizon and assumes a relatively stable progression in terms of technological advancement. The potential for any AI company to achieve artificial general intelligence (AGI) is outside the paper's scope for several reasons, including the lack of expert consensus on what achieving AGI would actually entail; the emerging consensus that such a breakthrough remains hypothetical and, at a minimum, several years away from happening; and the profound societal and economic upheaval AGI might bring.

Trend 1: A 'boom' in dual-use and defence tech

Investment in dual-use and defence AI has increased sharply in recent years. Venture capital (VC) spending on defence tech reached record levels in 2025, with VC-backed defence startups in the US and Europe, by some estimates, raising a combined $7.7 billion between January and October in that year – more than double 2024's total. Overall private defence investment in 2025 exceeded $48 billion, driven by large funding rounds for companies in the AI and autonomous drone sectors.[6] This growing interest is largely a result of the promise of high levels of government spending on defence and heightened interest in AI's battlefield utility, which at time of writing is being put to the test in several ongoing conflicts.

The war on Ukraine has not only spurred a significant increase in global military spending, but has also showed the utility of commercial, off-the-shelf technology innovations on the modern battlefield.

Though investment in battlefield autonomy and AI for military purposes dates back many decades, Russia's full-scale invasion of Ukraine in 2022 has been a major factor behind the resurgent interest in dual-use and defence technologies. The war on Ukraine has not only spurred a significant increase in global military spending, but has also showed the utility of commercial, off-the-shelf technology innovations on the modern battlefield. While large platforms and traditional weapons systems will not lose their importance in war, Ukraine has revolutionized the extensive and innovative use of cheap, disposable drones,[7] enabled by dual-use systems like Starlink. For many military planners, the Ukraine war has reinforced the lesson that success in modern warfare will depend on a country's ability to leverage not just their defence–industrial bases, but also their commercial technology ecosystems and the innovation that flows from them.

However, collaboration between commercial ecosystems and the defence sector has in the post-Cold War era been constrained by several structural challenges. These hurdles include the difficulty for the public sector of competing with commercial investors and markets, opaque and burdensome procurement processes, and public scepticism towards companies working with the military.

To overcome these hurdles, many governments have begun implementing policies aimed at opening up investment, reducing procurement friction, and encouraging commercial technology companies and new defence startups to participate more actively in defence contracts. In some cases, this effort has included broader industrial

6 Javaheri, A. (2025), *2025 vertical snapshot: Defense tech*, report, PitchBook, 5 August 2025, https://pitchbook.com/news/reports/2025-vertical-snapshot-defense-tech.
7 Kunertova, D. (2023), 'The war in Ukraine shows the game-changing effect of drones depends on the game', *Bulletin of the Atomic Scientists*, 79(2), pp. 95–102, https://doi.org/10.1080/00963402.2023.2178180.

policy initiatives, or, on a smaller scale, the creation of new specialized agencies designed to make it easier for non-traditional players to work with the military.[8]

These efforts appear to be bearing some fruit. In the post-Cold War era, most defence markets have come to be dominated by a small number of incumbents (or 'primes'), such as the UK's BAE Systems, the US company Lockheed Martin and Italy's Leonardo. But recent years have seen a rapid influx of a far more heterogeneous set of competitors into the sector, in part spurred on by governments' increased push for dual-use technologies. Although traditional defence companies remain key beneficiaries of the defence spending surge, so-called 'neo-primes', such as Germany's Helsing, the US's Anduril and Finland's ICEYE, have also entered the marketplace, keen to capitalize on renewed interest and the promise of sustained high levels of government defence spending.

The large technology companies, including the major US-based 'hyperscalers', have been increasingly active participants in the defence industry. Between 2018 and 2022, the Pentagon signed contracts worth an estimated $53 billion with such firms.[9] By 2025, Anthropic, Meta and OpenAI each signed deals with the US Department of Defense to embed their AI solutions into the US military.[10] Several are part of the Pentagon's Project Maven and its GenAI.mil platform, launched by the Pentagon in December 2025 to provide secure generative AI access to its 3 million staff members.[11] GenAi.mil, among others, embeds Anthropic's Claude, Google's Gemini, xAI's Grok and OpenAI's ChatGPT models. (Although it should be noted that, at time of writing, Anthropic's involvement was in question after a highly publicized stand-off between the company and the White House over the use of the former's products.)[12]

A similar shift can be observed in terms of financing. Traditional commercial funders, which historically had steered clear of defence investments and were frequently institutionally or legally restricted, or even barred, from doing so, are now becoming more active. Across the globe, both governments and, increasingly, VC firms, banks and other investors are pouring money into companies developing military or dual-use AI applications, with investment rising particularly rapidly in Europe, the US and, to a lesser extent, the Middle East and Indo-Pacific. In Europe, at least five new specialist defence-technology venture funds were established in 2025, increasing the continent's total to 13. The newest of these funds, DTCP's Liberty

---

8 Governments are setting up dedicated innovation bodies to incentivize dual-use technologies, with examples including India's Innovations for Defence Excellence (iDEX) and the UK Defence Innovation organization (UKDI), which consolidates several different defence innovation-focused government funds. The NATO Innovation Fund and Defence Innovation Accelerator for the North Atlantic (DIANA) are significant examples of dual-use innovation becoming institutionalized at the intergovernmental level, as well as by states.

9 Bratton, L. (2024), 'The Pentagon is spending billions on Big Tech and Silicon Valley startups as it goes all-in on AI', Quartz, 13 May 2024, https://qz.com/the-pentagon-is-spending-billions-on-big-tech-and-silic-1851423069.

10 Konkel, F. (2025), 'Pentagon awards multiple companies $200M contracts for AI tools', Defense One, 14 July 2025, https://www.defenseone.com/defense-systems/2025/07/pentagon-awards-multiple-companies-200m-contracts-ai-tools/406700.

11 US Department of Defense (2025), 'The War Department Unleashes AI on New GenAI.mil Platform', press release, 9 December 2025, https://www.war.gov/News/Releases/Release/Article/4354916/the-war-department-unleashes-ai-on-new-genaimil-platform.

12 O'Brien, M. and Toropin, K. (2026), 'Pentagon says it is labeling AI company Anthropic a supply chain risk 'effective immediately', AP News, 6 March 2026, https://apnews.com/article/pentagon-ai-anthropic-claude-dario-amodei-openai-d4608c7dd139245ac8ad94d5427c505a.

Fund, allocated $500 million to European technology companies.[13] At the same time, large financial institutions are beginning to move more decisively into the sector. For example, JPMorgan Chase announced in October 2025 that it would invest $10 billion annually in US national security and resilience solutions.[14]

The US and China continue to dominate the defence technology landscape, mirroring their leadership of the global AI marketplace. These two markets account for the largest share of global defence-technology investment. Defence tech investments in the US are still approximately three times higher than in the combined European NATO countries.[15]

The EU cumulatively spent approximately €381 billion on defence in 2025, nearly double what it spent a decade earlier, with an increasing share of this spending directed towards new technologies, including AI-enabled capabilities.

Yet, while the US and Chinese markets continue to dominate in terms of absolute numbers, the rate of growth in those markets is not necessarily the fastest. Investment in defence AI has been growing rapidly in Europe, driven by rising market demand, higher defence spending by European governments and a growing emphasis on strategic autonomy. The EU cumulatively spent approximately €381 billion on defence in 2025, nearly double what its member states spent a decade earlier, with an increasing share of this spending directed towards new technologies, including AI-enabled capabilities.[16] The EU is now one of the fastest-growing major markets for dual-use AI investment, with VC-backed investment increasing by around 80 per cent between 2024 and 2025 by some estimates, and the highest in terms of numbers of deals (though later-stage, higher-value deals remain elusive).[17] It is important to put these numbers in perspective: the European market starts from a far lower base, and many institutional and financial barriers remain. Nevertheless, where Europe's technology industry was previously wary of working with the military, several of the continent's largest so-called 'unicorns' – such as Helsing and Portugal's Tekever – are now primarily active in the military AI sector. Cities like Stockholm, London, Paris and Munich are emerging as key defence-technology hubs.

---

13 Digital Transformation Capital Partners (2026), 'DTCP launches €500 million fund for defense and security technologies in Europe', press release, 16 January 2026, https://www.dtcp.capital/news-and-insights/detail/dtcp-launches-eur500-million-fund-for-defense-and-security-technologies-in-europe.
14 JPMorgan Chase (2025), 'JPMorganChase launches $1.5 trillion security and resiliency initiative to boost critical industries', press release, 13 October 2025, https://www.jpmorganchase.com/newsroom/press-releases/2025/jpmc-security-resiliency-initiative.
15 Mckinsey & Company (2026), 'European defense by the numbers', article, 12 February 2026, https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/european-defense-by-the-numbers.
16 European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2025), *Preserving Peace – Defence Readiness Roadmap 2030*, , joint communication, 16 October 2025, https://op.europa.eu/en/publication-detail/-/publication/2d3f6ebf-ab5f-11f0-89c6-01aa75ed71a1.
17 StepUp Startups Consortium (2025), *The role of AI in the EU's dual-use technology field*.

For the US, the goals of leading on military AI development and integrating the technology into systems to gain a battlefield edge are intimately intertwined with wider ambitions to win the AI race and gain dominance over the technology. Successive US administrations have described such dominance as the geostrategic determinant of the 21st century.[18] Export controls preventing Chinese rivals from accessing the advanced semiconductors required to develop frontier AI, which Washington fears could aid in the PLA's modernization, are a key manifestation of this, The increasingly intimate relationship between the Pentagon and Silicon Valley is another. For China, winning the AI race similarly means being the most effective at deploying AI solutions in its military – with new domestic tech challengers seen as vital to helping Beijing achieve this objective.

Other, smaller actors also give defence and dual-use AI heightened importance. Governments are increasingly treating the military deployment of AI as a 'silver bullet' that may help solve critical challenges across a range of geostrategic, political and economic objectives. AI is believed to be able to help ease personnel shortages and may bring real battlefield advantage. But it could also bring spillover economic benefits, help countries to cultivate a wider range of sovereign AI systems and grow their global influence and market share.

AI's potential as a force multiplier and, more mundanely, the efficiency gains predicted from its use are the most important reasons why governments and the private sector (keen to cultivate governments as customers) are dedicating substantial resources towards building domestic defence AI industries and solutions. These ambitions are as frequently about addressing persistent structural weaknesses, such as constraints of time, money and manpower, as they are about countries seeking to place themselves at the absolute frontier.

Government spending in cutting-edge technologies on the battlefield, and rearmament more generally, are often presented as an opportunity for economic growth, job creation and generating spillover benefits from AI developed for military ends. The 'defence dividend' from high-tech investment (i.e. the idea of using higher levels of military spending to generate wider economic growth) has frequently been referred to by governments in the UK and elsewhere as an important opportunity.[19]

The perceived benefits of dual-use AI go beyond domestic economic growth to foreign policy. The development of a sovereign, competitive and independent dual-use AI and technology industry could simultaneously serve as an instrument of both soft and hard power to expand a country's influence. The US and China have been able to achieve this. Middle powers with a relatively large defence footprint can do the same at a smaller scale. For example, the UK, France and Russia have well-developed defence export industries and are keen to replicate

18 See, for example, The White House (2025), *Winning the Race: America's AI Action Plan*, https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf.
19 UK Prime Minister's Office, 10 Downing Street and The Rt Hon Sir Keir Starmer KCB KC MP (2025), *Prime Minister to set out vision for 'defence dividend' in a changed world*, press release, 8 May 2025, https://www.gov.uk/government/news/prime-minister-to-set-out-vision-for-defence-dividend-in-a-changed-world.

this strength in defence AI. Turkey and Ukraine, too, have been using their defence equipment exports and expertise in drone development – which increasingly involve degrees of autonomy – as a means of building wider partnerships.[20]

How this trend may lead to multipolarization

Higher defence spending by middle powers can lead to innovation spillover

Just as the initial rise of Silicon Valley relied on large defence contracts, other sectors may similarly find themselves with an opportunity to grow on the back of high levels of defence spending. This opportunity could be especially relevant in the case of a general-purpose technology like AI, which has significant dual-use applications – meaning that innovations made with a primarily military objective in mind may eventually find civilian uses (or vice versa).

South Korea has been notably successful in cultivating dual-use technology and reaping some of the spillover benefits. This in no small part because, unlike its partners in the West, it has maintained a constant state of war readiness given tensions with North Korea. South Korea has been able to cultivate a large domestic market and fostered a symbiotic, government-led relationship, geared towards bringing the country's large national corporations and its well-developed tech sector into military production. Though initially primarily focused on satisfying its domestic market, South Korea has become an important exporter of military equipment to partners in Asia, Europe and the Middle East.

As access to capital and talent remain among the main obstacles preventing alternative AI ecosystems from competing, the emergence of innovation clusters around specific defence applications may also provide the seed for the growth of a more mature commercial funding ecosystem focused on wider applications. Governments in places like the EU and Japan are reducing some of the investment barriers to market growth – for example, by making it easier for pension funds and other institutional funders to invest in dual-use applications.[21]

Defence spending, in this scenario, functions as industrial policy and is used to promote domestic innovation. As governments and militaries are the primary customers of defence AI applications as well as dual-use applications like logistics systems, cloud services and AI-enabled space-based applications, strategic spending can help strengthen a wider ecosystem. High levels of defence spending may, for example, be used to help overcome some of the challenges around scaling – which has hitherto been among the biggest difficulties faced by European startups and has led to promising new businesses relocating to the US, the Gulf and other markets to access sufficient capital. The growing interest in dual-use AI, and the formation of small clusters, can also concentrate more AI talent in a specific location – the 'agglomeration effect' – from which other new actors outside of the defence-tech sector may benefit in terms of transfers of ideas and people.

---

20 Shahbazov, F. (2025), 'Exporting Power: Türkiye's defense industry and the politics of strategic autonomy', TRENDS Research & Advisory, 17 December 2025, https://trendsresearch.org/insight/exporting-power-turkiyes-defense-industry-and-the-politics-of-strategic-autonomy/?srsltid=AfmBOoqbfZwkxNzKWTzc4dlbiTqt5a1QO0xrAuKWDIwMrFlXl1nbXhtB.

21 Greenacre, M. (2025), 'EIC will invest in dual-use start-ups, Commission says', Science|Business, 20 March 2025, https://sciencebusiness.net/news/european-innovation-council/eic-will-invest-dual-use-start-ups-commission-says.

Battlefield experience can give small and medium-sized countries a comparative advantage

Ukraine has been referred to as an 'AI war lab',[22] with both Ukraine and Russia increasingly deploying AI-enabled solutions in decision-making processes or scaling up drone operations that have been a defining aspect of the four-year conflict.[23] For Ukraine, bringing technology startups and other providers of cutting-edge solutions into the military became a wartime necessity. But the country's burgeoning defence-tech industry, its growing tech talent pool and a permissive regulatory environment that allows for the rapid testing and procurement of new solutions provide a potential model for its post-war economy.[24] Ukraine is seeking to build on its experience with rapid war-time innovation in AI and drones in particular, brokering partnerships with large defence contractors elsewhere in Europe and striking deals with the US and in the Middle East to scale production and export its knowledge.[25]

Ukraine has been referred to as an 'AI war lab', with both Ukraine and Russia increasingly deploying AI-enabled solutions in decision-making processes or scaling up drone operations that have been a defining aspect of the four-year conflict.

Another example of a country that has turned battlefield experience into developing its wider technology sphere is Israel, which maintains one of the world's most tech-mediated and AI-powered military and intelligence apparatuses.[26] It has turned this expertise and battlefield experience – coupled with the fact that many of its tech workers have served in the Israel Defence Forces (IDF) – into a competitive cyber and defence tech industrial complex. By some measures, Israel's AI industry ranks seventh in the world,[27] despite the country ranking 29th in terms of GDP and 97th in terms of population.

---

22 Bergengruen, V. (2024), 'How Tech Giants Turned Ukraine Into an AI War Lab', *Time*, 8 February 2024, https://time.com/6691662/ai-ukraine-war-palantir.

23 The degree of autonomy in these solutions should not be overstated. In the case of drone warfare, for example, AI solutions are employed primarily to support drone pilots with locking-in targets and bypassing Russian attempts at jamming signals between drones and their pilots. Development of automated solutions is nonetheless rapid and is spilling over into a growing range of use cases. See Bates, E. and Quick, S. R. (2025), 'Drones aren't swarming yet – but they could', War on the Rocks, 4 August 2025, https://www.warontherocks.com/2025/08/drones-arent-swarming-yet-but-they-could.

24 Russia has also become more adept at fostering collaboration between its tech startups and the military, with a particular focus on AI. Though Russia's AI spending remains low in global terms, its ambitions are big – with Moscow believing it may be able to significantly rebuild its military using the technology.

25 Crebo-Rediker, H. E. (2026), 'Securing Ukraine's Future in Europe: Ukraine's Defense Industrial Base—An Anchor for Economic Renewal and European Security', Council on Foreign Relations, 24 February 2026, https://www.cfr.org/articles/securing-ukraines-future-in-europe-ukraines-defense-industrial-base-an-anchor-for-economic-renewal-and-european-security.

26 Moskvitch, K. (2011), 'How Israel turned itself into a high-tech hub', BBC News, 22 November 2011, https://www.bbc.com/news/business-15797257; Hammad, N. (2026), 'The proliferation of AI-enabled military technology in the Middle East', International Institute for Strategic Studies, 2 April 2026, https://www.iiss.org/online-analysis/charting-middle-east/2026/04/the-proliferation-of-ai-enabled-military-technology-in-the-middle-east.

27 Mostrous, A., Cesareo, S. and White, J. (2024), 'The Global Artificial Intelligence Index 2024', *The Observer*, 19 September 2024, https://observer.co.uk/news/science-technology/article/the-global-artificial-intelligence-index-2024.

These examples show that growing investment in dual-use AI can potentially be a leveller for small and medium-sized countries that are able to internalize battlefield knowledge and find opportunities to apply it to other domains.

Real-world use can enable less-advanced countries to catch up in the defence AI race

Ukraine's creative use of these technologies, and its ability to test and rapidly iterate them directly on the battlefield while developing doctrines for their use, will inevitably have implications for AI deployment beyond the frontline. According to several reports, Ukrainian AI and drone systems routinely outperform those from Western companies, many of which are also using the war to analyse the strength of their technologies.[28]

The US and China may still be able to capitalize on their sizable lead to gain battlefield advantage and pull further away from less-advanced peers in the race. But equally, others may have a chance to catch up. As AI systems are deployed more in combat, grand promises will be tested against operational reality. The true state of the defence AI market will become clearer, revealing the actual utility of technologies and moving discussions beyond simple comparisons between the size of national markets or the scale of investment. A case in point is the fact that Ukrainian drone tech experts have been called in to support Gulf Arab countries, as well as the US military, to help them defend against Iranian drone attacks.[29]

Trend 2: The rise of 'patriotic tech' and the blurring of boundaries between civil and military

2025 was characterized by a more intimate relationship between AI companies and governments, with many commercial operators becoming increasingly open in their willingness to explore the defence and national security applications of their AI products. Though this is a global dynamic, the trend is especially visible in the US, driven not just by new defence tech companies entering the AI marketplace, but also by the hyperscalers and frontier AI labs pursuing contracts with the Pentagon and allied defence ministries, and presenting themselves as working in support of US government (and, by extension, NATO) objectives.

Just as governments have become increasingly proactive in courting the companies behind cutting-edge AI solutions, so too have commercial companies become more interested in pursuing military contracting and exploring the dual-use and defence applications of their products. This is the result of sustained levels of high government spending and the implied prestige of developing high-tech

28 *The Economist* (2025), 'Western drones are underwhelming on the Ukrainian battlefield', 23 October 2025, https://www.economist.com/europe/2025/10/23/western-drones-are-underwhelming-on-the-ukrainian-battlefield.
29 Landale, J. (2026), 'Zelensky sends drone teams to Middle East, touting Ukraine's expertise', BBC News, 11 March 2026, https://www.bbc.co.uk/news/articles/cgl5jeg5r15o.

solutions for the military, but also a heightened, more insecure and combative security environment, in which private sector actors are encouraged to do their 'patriotic duty'.[30]

The latter is particularly important. In the US, just like everywhere else in the West, the end of the Cold War ushered in an era in which defence spending declined precipitously and the defence industry rapidly consolidated into a smaller number of large companies.[31] During this time, the focal point of innovation shifted away from the Cold War model in which government-supported laboratories and government-aligned companies developed defence solutions which would eventually flow down into the commercial sphere (such as GPS, the semiconductor and the internet, which all originated from government contracts), towards a commercial-first approach. This narrative shift is now almost fully complete, with especially leading-edge private sector companies in Silicon Valley driving frontier innovation, while militaries and defence contractors purportedly struggling to fully harness these solutions.

The inability of the US military to benefit in full from the country's cutting-edge technology companies and their innovations has become a source of bipartisan fear in Washington that US military capabilities are atrophying, while more agile rivals – above all China – better able to use the full strength of their domestic ecosystems, are rapidly catching up. As a result, from the 2010s onwards, the US government has made repeated appeals to Silicon Valley to bring more of their frontier AI technologies and expertise into the military. The Defense Innovation Unit (DIU), for example, was created under President Barack Obama to help bridge the gap between Silicon Valley and the Pentagon, by making it easier for tech companies to speedily and easily access funding and providing them with support to rapidly test and scale solutions for military use.[32] The intent behind DIU, the remit and funding of which has increased with each administration, is not just about opening up new sources of funding, but also about building trust between government and tech companies, and allaying concerns about complex bureaucracies and the ethics of working with the military.

Especially under the current US administration – which has set the ambition to accelerate America's AI dominance by becoming an AI-first warfighting force[33] – closer ties between the tech industry and the military appear to have taken on a distinctly ideological dimension, over and above commercial incentives. While, for a long time, Silicon Valley companies had preferred to keep a certain distance from the state, presenting themselves as more neutral, and global, entities, many are now beginning to position themselves as key actors in preserving US hegemony, security and providing the government with support in its competition with China.

---

30 Holmes, A. (2020), 'Read the letter Palantir's CEO wrote attacking Silicon Valley companies as unpatriotic 'engineering elites' and allying itself with the Trump administration', Business Insider, 26 August 2020, https://www.businessinsider.com/palantir-s1-ipo-silicon-valley-military-tech-patriotic-alex-karp-2020-8.
31 Kirshner, J. and Green, J. (2024), 'The 'Last Supper' era is over – it's time for the 'First Breakfast'', Breaking Defense, 18 December 2024, https://breakingdefense.com/2024/12/the-last-supper-era-is-over-its-time-for-the-first-breakfast.
32 Shah, R. M. and Kirchhoff, C. (2024), *Unit X: How the Pentagon and Silicon Valley are transforming the future of war*, New York: Simon & Schuster.
33 US Secretary of Defense (2026), 'Artificial Intelligence Strategy for the Department of War', memorandum, US Department of War, 9 January 2026, https://media.defense.gov/2026/Jan/12/2003855671/-1/-1/0/ARTIFICIAL-INTELLIGENCE-STRATEGY-FOR-THE-DEPARTMENT-OF-WAR.PDF.

Some new tech 'primes' present themselves explicitly as exponents of US power. For example, Palantir's CEO, Alex Karp, has repeatedly said that his company's mission is to 'defend the West' and to ensure the latter continues to 'dominate' technologically.[34] Palantir's 2026 manifesto notably states that 'Silicon Valley owes a moral debt to the country that made its rise possible' and that 'the engineering elite of Silicon Valley has an affirmative obligation to participate in the defense of the nation'.[35] It has also been widely reported that executives at several large tech companies have joined the military to gain more personal battlefield experience and to bring tech expertise directly into the US Army.[36]

This turn is not just reflected in rhetoric, but increasingly also in decisions around investment, partnerships and the activities these companies are involved in. Project Maven, the Pentagon's programme to help accelerate the military's adoption of AI launched in 2017, illustrates this evolution. When news reports emerged in 2018 that Alphabet had been supporting the initiative, the backlash was so immediate that employees staged a walkout – which ultimately prompted the company to limit its involvement.[37] As of 2026, several large US tech companies now openly take part.

Under Beijing's doctrine of 'civil–military fusion', private companies are expected to contribute directly to national technological self-reliance, an objective which has gained further momentum amid increased competition from the US and its allies.

Although the US is currently in the process of giving shape to this evolving tech–military relationship, close relations between state and the private sector are long-standing and more explicitly formalized in China. Under Beijing's doctrine of 'civil–military fusion', private companies are expected to contribute directly to the modernization of the People's Liberation Army (PLA) and to national technological self-reliance, an objective which has gained further momentum amid increased competition from the US and its allies. The Chinese state, including the military, acts as a major patron and customer of new solutions, providing early scale and support and championing the most promising domestic challengers.[38]

Several of China's largest tech champions, such as Huawei, reportedly have their roots in the PLA. While the maturity of China's ecosystem means these companies

34 Haskins, C. (2025), 'Palantir wants to be a lifestyle brand', Wired, 22 September 2025, https://www.wired.com/story/palantir-wants-to-be-a-lifestyle-brand.
35 Palantir Tech via X (2026), 'Because we get asked a lot. The Technological Republic, in brief […]', 19 April 2026, https://x.com/PalantirTech/status/2045574398573453312.
36 Harper, J. (2025), 'Army recruits officers from Meta, OpenAI and Palantir to serve in new detachment', Defense Scoop, 13 June 2025, https://defensescoop.com/2025/06/13/army-detachment-201-executive-innovation-corps-meta-openai-palantir.
37 BBC News (2018), 'Google 'to end' Pentagon Artificial Intelligence project', 2 June 2018, https://www.bbc.co.uk/news/business-44341490.
38 Umback, R. (2019), 'Huawei and Telefunken: telecommunications and rising powers', The Strategist, 17 April 2019, https://www.aspistrategist.org.au/huawei-and-telefunken-telecommunications-and-rising-powers.

are now less dependent on government as a customer, many now primarily commercial companies remain entangled with China's military. For example, one of China's open-source AI champions, DeepSeek, now underpins some of the PLA's experiments in UAV autonomy and is being diffused and integrated across China's military, to help it transition towards what it calls 'intelligentized warfare'.[39]

This growing intimacy between the state and private AI sector is not just the preserve of China and the US. Significant parts of Israel's tech ecosystem are intimately intertwined with the IDF, while South Korea has long embraced self-reliance in its defence production. The latter's successful embrace of dual-use technology development in no small part relies on extensive government involvement and deep defence–civilian integration. While Korean companies initially participated in this system for mostly patriotic reasons, the country's emergence as a leading global defence exporter has created additional commercial incentives.

The EU is home to a rapidly growing and increasingly well-funded sector of AI and other tech startups actively pursuing military contracts, with many of these companies explicitly citing strengthening European strategic autonomy as a motivation. For example, Torsten Reil, the co-founder of Helsing, has said: '[Europe] should develop homegrown systems that we control, both in terms of actually controlling the whole technology, but also the ethics side of it… what degree of autonomy are we prepared to accept is something that we need to be able to control.'[40]

How this trend may lead to multipolarization

The phenomenon is spreading

Russia's full-scale invasion of Ukraine has prompted an interest in defence tech among young European entrepreneurs.[41] Many founders cite their ambition to strengthen Europe's tech ecosystem as an important motivator. This phenomenon is set to continue: in 2026, for the first time, tech workers leaving the US for Europe outnumber those going the other way.

Europe's existing champions and new entrants alike are calling for more concerted action to strengthen Europe's competitiveness and security. These endeavours are now frequently framed as attempts to strengthen European strategic autonomy, rather than that of individual member states. One of the major hinderances to the growth of both Europe's technology and defence sectors has been fragmentation of efforts. This new wave of entrepreneurs may be better placed to overcome some of these barriers.

The resulting intimacy between defence tech players and governments is unlikely to decline in the near future. Increased entanglement can be used to grow the market for companies' AI solutions and to strengthen the overall competitiveness and strategic alignment of domestic AI ecosystems. This dynamic may especially

---

39 Baptista, E. and Potkin, F. (2025), 'How China could use DeepSeek and AI for an era of war', Reuters, 27 October 2025, https://www.reuters.com/world/asia-pacific/robot-dogs-ai-drone-swarms-how-china-could-use-deepseek-an-era-war-2025-10-27.
40 Resilience Media (2025), 'Helsing CEO Torsten Reil Urges Europe to Build for Defence Tech Sovereignty', 29 October 2025, https://resiliencemedia.co/helsing-torsten-reil-urges-europe-to-build-for-tech-sovereignty.
41 Sterling, T. (2025), 'Europe's defence challenge energises young techies at hackathon', Reuters, 31 March 2025, https://www.reuters.com/business/aerospace-defense/europes-defence-challenge-energises-young-techies-hackathon-2025-03-31.

benefit challenger markets with more limited resources. One of the current race leaders – China – provides an example of how governments and companies working in close harmony to shape markets can rapidly scale-up domestic tech industries to compete with a hegemonic power. Israel and South Korea also provide models at a smaller scale.

This kind of symbiosis may allow new challenger markets to gain an advantage and become better able to direct the full strength of their domestic industry towards the pursuit of strategic goals. It can, however, create a dynamic in which both the government and private sector become increasingly reliant on each other – where both sides could feel pressured into removing safeguards and rushing potentially harmful deployment.

'Civil–military fusion' could raise concerns over coercion

Symbiosis between the AI sector and governments – whether real or merely perceived – can also become a source of global tension and fragmentation, which may further spur on national sovereignty and decoupling efforts.

China's doctrine of 'civil–military fusion' is often cited by policymakers in Washington as the motivation behind the US's increasingly all-encompassing (although, under the Trump administration, somewhat unfocused) export-control regimes targeting Beijing's ability to develop frontier AI. US concerns centre around the perception that, owing to this doctrine, virtually all technology developed by China is inherently dual-use in nature because any company can be called on to 'do its civic duty'. Similar perceptions of a lack of neutrality may start to take hold in relation to other markets, as more governments become more actively involved in cultivating and scaling their own sovereign champions (see Trend 3, below). Customers around the world may grow increasingly concerned that the products they buy and use are contingent on the strategic objectives of the home governments of countries where suppliers are domiciled.

Governments may, in turn, come under rising pressure to reduce the regulatory burden on, or even to bail out, companies that are regarded as pivotal for national prestige and security. The companies involved would in turn become more reliant on government and military funding and contracts, and may find themselves pressured to, for example, take actions to support geopolitical objectives that further augment the power of the state. Private sector actors may find themselves increasingly pressured to become involved in the state's international affairs. For example, the International Criminal Court (ICC)'s chief prosecutor was reported to have had their access to email and many other cloud-based services removed in July 2025, following the Trump administration's imposition of sanctions against the ICC over its actions against the Israeli government.[42]

In an era of weaponized interdependence, governments with closer ties to (or even holds over) their private sectors are better able to co-opt the power of these companies. In a farewell address from the White House in January 2025, Joe Biden spoke of his concern about the possible rise of a 'tech-industrial

42 Quell, M. (2025), 'Trump's sanctions on ICC prosecutor have halted tribunal's work', Associated Press, 15 May 2025, https://apnews.com/article/icc-trump-sanctions-karim-khan-court-a4b4c02751ab84c09718b1b95cbd5db3.

complex'.[43] This dynamic will leave the private sector trying to achieve a delicate balance. Refusing to comply with their home government's demands could lead to serious repercussions. Anthropic, for example, at the time of writing, still faces a supply-chain risk designation in the US, which could lead to the US government, as well as companies doing business with it, being barred from working with the company. However, complying and working closely with a government that is increasingly seen to be engaging in coercive diplomacy can also erode global trust in a company's brand and the reliability of their services. Over time, companies domiciled in countries which are seen to be adhering to the rule of law, may benefit by attracting talent and customers.

Trend 3: The pursuit of sovereign AI

As the geopolitical climate becomes more tense and the geostrategic utility of having independent AI capabilities more evident, a growing cohort of countries has started to reassess the composition of their technology stacks – encompassing everything from the underpinning physical infrastructure (e.g. undersea cables and data centres, computing power, chips and so on), to the protocols, standards and code, as well as the software and solutions that run on top. This reassessment has added urgency to existing calls for governments to develop their own sovereign capabilities and sees countries attempt to disentangle themselves from a perceived over-reliance on external AI companies and solutions, and instead aligning with trusted domestic or allied partners that can contribute to more resilient supply chains and software stacks.

Sovereign AI strategies and ambitions, in which countries try to cultivate either fully or partially independent AI capabilities, should be seen as laying on a spectrum. Some countries or groupings – such as China and, to a lesser extent, the EU – are aiming to develop their own capabilities across all layers of the AI stack. Other middle and smaller powers – countries ranging from Brazil to Pakistan and Vietnam – are pursuing more limited strategies, focused on a variety of approaches. These strategies include hedging between Chinese, US and others' AI products, developing their own niches in the AI industry and underpinning supply chains, adopting cheaper, open-source AI solutions, opening up access to digital public AI infrastructure, and ensuring that the most critical capabilities for national security remain under domestic control. Rather than seeking full technological self-sufficiency (which – with the possible exception of China – is in practice not achievable), these strategies typically aim for greater strategic autonomy through reducing external dependencies, cultivating domestic capabilities and, in some cases, creating technological 'chokepoints' that can be used as leverage against others.

These efforts are not new, but were initially primarily motivated by economic considerations. They have increasingly taken on a national security dimension, as governments worry about dependencies in supply chains and solutions that may be weaponized against them. Japan and India illustrate this point. Japan has

43 The American Presidency Project (2025), 'Farewell Address to the Nation: Speech by President Joseph R. Biden, Jr, The White House, Washington, DC, 15 January 2025', https://www.presidency.ucsb.edu/documents/farewell-address-the-nation-4.

increased its efforts to cultivate a sovereign AI stack by seeking greater control over foundational infrastructure and reducing reliance on external cloud and AI providers.[44] Tokyo subsidizes domestic cloud capacity, supports homegrown AI companies and aims to increase self-sufficiency in AI infrastructure, partly by leveraging the country's long-standing strengths in semiconductor manufacturing. These initiatives are linked to Japan's broader economic security agenda and reassessment of its post-Second World War security posture and are complemented by efforts to stimulate domestic defence AI innovation. In 2026, Japan made diverting government R&D spending towards dual-use innovation a priority, and also seeks to promote these activities through its Acquisition, Technology and Logistics Agency (ATLA), as well as cooperation frameworks such as Pillar II of AUKUS and the Quadrilateral Security Dialogue group (or Quad).[45]

India, similarly motivated by concerns about strategic dependence and by recent security tensions with Pakistan (during which its high-tech solutions were perceived to have underperformed), has begun leveraging its growing commercial technology ecosystem to strengthen sovereign dual-use capabilities and homegrown defence AI.[46] In 2025, New Delhi launched a dedicated technology fund and expanded initiatives such as Innovations for Defence Excellence (iDEX),[47] aimed at cultivating domestic high-tech defence companies and reducing reliance on imported equipment from the US, Russia and elsewhere. Sovereign AI was also a main theme of the 2026 AI Summit hosted by India – a forum which the Indian government also used to promote its latest defence innovations. These initiatives exist in parallel with its long-standing, and already successful, efforts to build public digital infrastructure, which have allowed India to build its own independent payment and identity systems.[48]

The EU has long treated the need to grow its presence in the global AI markets and achieve strategic autonomy in both AI and the wider technology sector as a policy priority. Previously, these efforts were largely seen through an economic and competitiveness lens. Policymakers in Brussels and member-state capitals have long recognized that the continent's lagging domestic AI and wider digital technology industry present a serious challenge to its long-term competitiveness, democratic resilience and independence. The Draghi report,[49] for example, pointed out that the divergence between US and EU productivity growth – and GDP – from the 2007–08 financial crisis onwards can to an extent be explained by the rapid expansion of the US tech industry, contrasted against the EU's apparent inability to create any major

---

44 Cabinet Office of Japan (2025), *Artificial Iintelligence Basic Plan – "Japan Rebooted" through "Trustworthy AI"*, 23 December 2025, https://www8.cao.go.jp/cstp/ai/ai_plan/aiplan_eng_20260116.pdf.
45 Castillo, D. (2024), 'Bridging the gap: How innovation will see Japan become the first nation integrated into AUKUS Pillar II', *UWA Defence & Security Policy Brief*, 12 November 2024, https://defenceuwa.com.au/publications/policy-briefs/bridging-the-gap-how-innovation-will-see-japan-become-the-first-nation-integrated-into-aukus-pillar-ii; Fraser, D. (2023), 'The Quad: a backgrounder', Asia Society, 16 May 2023, https://asiasociety.org/policy-institute/quad-backgrounder.
46 Landrin, S. and Vincent, E. (2025), 'Military operation in Pakistan reveals weaknesses of India's air force', *Le Monde*, 8 May 2025, https://www.lemonde.fr/en/international/article/2025/05/08/military-operation-in-pakistan-reveals-weaknesses-of-india-s-air-force_6741047_4.htm.
47 *The Economist*, (2025), 'India's defence-tech startups are thriving', 3 December 2025, https://www.economist.com/asia/2025/12/03/indias-defence-tech-startups-are-thriving.
48 Varela Sandoval, F. J., Wilkinson, I., Krasodomski, A. and Wilkinson, R. (2026), *How middle powers can weather US and Chinese AI dominance: The case for 'sovereign AI' strategies*, Research Paper, London: Royal Institute of International Affairs, https://doi.org/10.55317/9781784136710.
49 Draghi, M. (2024), *The future of European competitiveness – A competitiveness strategy for Europe*, Brussels: European Commission, https://commission.europa.eu/topics/competitiveness/draghi-report_en.

new market-leading technology companies since 2000. The EU is not currently home to any hyperscalers and its AI champions struggle to access the levels of (especially late-stage) funding available in the US especially.[50]

The lack of a competitive AI and digital tech industry has made European countries increasingly reliant on the US for their technology stacks, a dependency which in turn has made it difficult for European companies to compete.

This lack of a competitive AI and digital tech industry has made European countries increasingly reliant on the US for their technology stacks, a dependency which in turn has made it difficult for European companies to compete. Just three US-based companies (Amazon, Google and Microsoft) account for around 70 per cent of the European cloud storage market, for example.[51] However, with transatlantic tensions increasing throughout 2025 and early 2026, these kinds of external dependencies are now widely perceived as a serious national (and continent-wide) security risk. A March 2026 poll found that 86 per cent of Europeans now consider the possibility of the US government suddenly restricting Europe's access to critical technologies and digital services to be 'plausible' and something that 'should not be ruled out', and express preferences for decoupling.[52]

This change in narrative was spurred by several events. The first arrived in February 2025, when the Trump administration threatened to turn off Ukraine's access to SpaceX's Starlink systems and briefly requested US commercial satellite imagery provider Maxar to disable Ukraine's access, in a bid to convince Kyiv to sign a controversial deal on access to critical minerals.[53] This episode raised immediate questions about whether Washington might use access to its technology solutions, even those owned by commercial providers, as a coercive tool in negotiations with other supposed partners in Europe, as well as the trustworthiness of especially military systems which rely on US software support and maintenance. The Trump administration's actions against the ICC (see above),[54] and its later threats to raise

---

50 European Investment Bank InvestEU Advisory Hub (2025), 'Clearing the funding hurdles', 7 February 2025, https://advisory.eib.org/stories/clearing-the-funding-hurdles.
51 Baburajan, R. (2025), 'US cloud providers dominate 70% of €70 bn European market in 2024', InfoTechLead, 25 July 2025, https://infotechlead.com/cloud/us-cloud-providers-dominate-70-of-e70-bn-european-market-in-2024-90476.
52 Pollet, M. (2026), 'Europeans think Trump can shut down their internet', Politico, 19 March 2026, https://www.politico.eu/article/europeans-donald-trump-internet-technology-us.
53 Baio, A. (2025), 'U.S. threatened to cut off Musk's Starlink to Ukraine in mineral negotiations, says report', *The Independent*, 22 February 2025, https://www.independent.co.uk/news/world/americas/us-politics/musk-starlink-ukraine-minerals-negotiations-b2702861.html; Körömi, C. (2025), 'US curtails Ukraine access to satellite imagery', Politico, 7 March 2025, https://www.politico.eu/article/us-satellite-company-maxar-cuts-off-ukraine-access-imagery-report-says.
54 Satariano, A. and Smialek, J. (2025), 'Europe's growing fear: How Trump might use U.S. tech dominance against it', *New York Times*, 20 June 2025, https://www.nytimes.com/2025/06/20/technology/us-tech-europe-microsoft-trump-icc.html.

tariffs against the EU and the UK if they did not agree to relax their regulation of US tech companies, brought further momentum to the European push towards strategic autonomy.[55]

Recent threats against the territorial integrity and sovereignty of Greenland, and rising questions about the US commitment to NATO, added further urgency to this debate, and its implications for Europe's position to withstand coercive pressure or even a potential military incursion, when its tech systems are not under its full control. Several European governments have since 2025 expressed concern that, for example, military cloud access could be turned off during a conflict or that platforms like F-35 fighter jets supplied by the US could similarly be subject to 'kill switches' in the form of disruptions of software and maintenance support.[56] The US CLOUD Act, which allows US law enforcement to compel US companies to disclose user data, even if physically stored abroad, is of particular concern.

These flashpoints have sparked serious private, civil society and government efforts across Europe to diversify its AI and technology stacks, reduce weaponizable external dependencies and build and drive adoption of its own solutions. Strategic autonomy in AI has become an area of strategic focus in European Commission agendas,[57] and featured prominently during Commission president Ursula von der Leyen's 'State of the Union' address in September 2025.[58] Notable examples include the EuroStack initiative, which brings together a wide range of European defence and technology companies, to build and implement sovereign European solutions, especially in AI.[59] German chancellor Friedrich Merz and French president Emmanuel Macron hosted a joint summit in November 2025 to put action behind European digital sovereignty, with both leaders stressing the vital importance of strengthening Europe's own AI and defence tech systems.[60] The Austrian army migrated its IT solutions from a US provider to a European alternative,[61] while the Dutch Ministry of Defence announced in 2026 that it would build a homegrown, sovereign cloud in an explicit bid to reduce its reliance on the US.[62] The French government is currently in the process of transitioning away from US conferencing

---

55 Sweeney, M. (2025), 'Trump threatens tariffs on countries that 'discriminate' against US tech', *Guardian*, 26 August 2025, https://www.theguardian.com/us-news/2025/aug/26/donald-trump-tariffs-us-tech-uk-digital-services-tax-eu.
56 Neuman, S. (2025), 'Trump's handling of Ukraine and tariffs has NATO rethinking the U.S.–made F 35 fighter', NPR, 19 March 2025, https://www.npr.org/2025/03/19/nx-s1-5330475/f35-fighter-nato-trump-gripen.
57 European Commission (2025), *Apply AI Strategy*, policy document, Brussels: European Commission, https://digital-strategy.ec.europa.eu/en/policies/apply-ai.
58 European Commission (2025), 'State of the Union 2025', speech, 10 September 2025, https://commission.europa.eu/strategy-and-policy/state-union/state-union-2025_en.
59 EuroStack (undated), 'Building Europe's digital future', https://eurostack.eu.
60 Federal Government of Germany Press and Information Office (2025), 'Summit on European Digital Sovereignty delivers landmark commitments for a more competitive and sovereign Europe', press release, 18 November 2025, https://www.bundesregierung.de/breg-de/aktuelles/summit-on-european-digital-sovereignty-delivers-landmark-commitments-for-a-more-competitive-and-sovereign-europe-2394368.
61 Linux Security (2025), 'Austria: Enhancing Military IT Security and Sovereignty with LibreOffice', 3 October 2023, https://linuxsecurity.com/news/government/linux-security-defense.
62 Netherlands Ministry of Defence (2026), 'Defensie bouwt cloud voor staatsgeheime gegevens' [Defence Ministry builds cloud for classified data], press release, 9 April 2026, https://www.defensie.nl/actueel/nieuws/2026/04/09/defensie-bouwt-cloud-voor-staatsgeheime-gegevens.

services towards European-made, open-source alternatives.[63] Dutch technology giant ASML, meanwhile, invested €1.3 billion in the French AI company Mistral AI, explicitly citing the need to enhance European strategic autonomy.[64]

Such developments are still at an early stage. The depth of entanglement, plus the lack of a clear, shared vision for how to address the challenge among European governments and companies, mean that Europe is unlikely to wean itself of US technologies in the immediate term. Moreover, some of the dependencies – especially in the military realm – may take over a decade to replace. Similar concerns surround the continent's increased dependence on Chinese tech solutions and supply chains.

The increasingly urgent and public discussion of strategic autonomy is nevertheless significant. An autonomous European AI sphere is becoming more tangible, especially as governments and companies become more willing to pay the increased costs involved. This is not a dynamic confined to Europe alone, but one especially visible in countries previously reliant on both the US security umbrella and relatively open, globalized supply chains.

Rhetoric and actions on sovereignty are also likely to become a growing source of friction between those smaller players and the current leaders in the AI race. As global efforts to decouple become more explicit, Washington and Beijing will likely become more concerned about the market positions of their respective technology champions.

How this trend can lead to multipolarization

More countries will pay the 'sovereignty premium' and embrace domestic solutions over the cutting edge

The push towards decoupling and developing sovereign AI stacks could see more countries favour domestic champions in their procurement and start to prefer products from national providers over frontier solutions from politically unreliable external markets. This combination of increased spending, industrial policy, the use of government and private sector purchasing power to shape the marketplace, and an embrace of 'good enough' solutions over those at the cutting edge of development may provide those markets that are currently lagging behind with a way to catch up with the leaders.

2025 provided some early evidence of this dynamic in action. For example, European satellite-maker Eutelsat's OneWeb constellation had previously struggled to compete with large US-based market leader Starlink, but saw its stock price surge and order book expand, as European countries and others grew increasingly concerned that a dependency on US companies could be weaponized against them.[65] Geopolitical reliability trumped immediate performance in this equation – as Starlink's constellation remains by far the most mature LEO satellite solution. In October

63 Davies, P. (2026), 'France to ditch US platforms Microsoft Teams, Zoom for 'sovereign platform' citing security concerns', euronews, 27 January 2026, https://www.euronews.com/next/2026/01/27/france-to-ditch-us-platforms-microsoft-teams-zoom-for-sovereign-platform-amid-security-con.
64 ASML (2025), 'ASML, Mistral AI enter strategic partnership', press release, 9 September 2025, https://www.asml.com/news/press-releases/2025/asml-mistral-ai-enter-strategic-partnership.
65 Liguid, G. (2025), 'Eutelsat shares soar on Ukraine Starlink replacement rumors', Nasdaq, 11 March 2025, https://www.nasdaq.com/articles/eutelsat-shares-soar-ukraine-starlink-replacement-rumors.

2025, Greenland signed a deal with Eutelsat to provide connectivity to the island.[66] Demand has also come from outside of Europe. Taiwan, which is investing in LEO satellite systems to provide back-up connectivity during a possible invasion, has also turned to the European alternative as one of the more geopolitically secure options.[67] Similar evidence emerged in the European cloud storage market, where local providers have seen their market grow.[68] Though some concerns about friction, scalability and availability of many of these alternatives remain, countries are likely to become increasingly willing to pay a 'sovereignty premium', and accept more expensive or less mature but geopolitically reliable solutions over the less secure technological cutting-edge.

These efforts may not stay limited to the markets embracing sovereignty. A more wholesale change in global market preferences could emerge, as also other markets start to prefer technologies from trusted, allied partners over those provided by countries that have shown themselves willing to weaponize their dominance in technology and supply chains for their own geopolitical ends.

Distrust between the US and its traditional partners may grow

European attempts to strengthen its own technology stack and defence-industrial base were received unfavourably by the US, with Secretary of State Marco Rubio stating that 'any exclusion of US companies from European tenders would be seen negatively by Washington'.[69] Since then, the Trump administration has increased the pressure on leaders in Canada, Europe and Asia to continue to favour US technology, including through coercive mechanisms – for example, the threat of tariffs.

While aggressive measures may work in the short term, they may also become an increased source of geopolitical tension, and are likely to spur further fragmentation and decoupling in the longer term. A case study of how overplaying a dependency may expedite decoupling is China. China has long had the ambition to become fully self-reliant across the technology sphere and beyond – driven by important historical factors, as well as increasingly far-reaching restrictions imposed on Beijing by the US and its allies on the country's ability to access to high-end semiconductors, microchips and other strategic inputs critical for the development of frontier AI and other technologies.[70]

In 2025, China's apparent success in indigenizing its AI supply chains caused alarm in Washington, and resulted in the Trump administration further tightening restrictions on the export of semiconductors and other inputs. Though Chinese leaders recognize that these restrictions have hampered China's AI development

---

66 Russell, L. (2025), 'Eutelsat signs deal with Greenland national telco Tusass for LEO services', Data Centre Dynamics, 8 October 2025, https://www.datacenterdynamics.com/en/news/eutelsat-signs-deal-with-greenland-national-telco-tusass-for-leo-services.
67 France24 (2025), 'Taiwan running out of time for satellite communications, space chief tells AFP', 19 September 2025, https://www.france24.com/en/live-news/20250919-taiwan-running-out-of-time-for-satellite-communications-space-chief-tells-afp.
68 Salamone, S. (2026), 'Sovereign Cloud Gains Steam in EU', CD Insights, 1 February 2026, https://www.clouddatainsights.com/sovereign-cloud-gains-steam-in-eu.
69 Slattery, G., Irish, J. and Psaledakis, D. (2025), 'US officials object to European push to buy weapons locally', Reuters, 2 April 2025, https://www.reuters.com/world/us-officials-object-european-push-buy-weapons-locally-2025-04-02.
70 Doshi, R. (2021), *The Long Game: China's Grand Strategy to Displace American Order*, Oxford: Oxford University Press; Xi, J. (2023), 'Full text of Xi Jinping's speech at the first session of the 14th National People's Congress', speech, Xinhua, 14 March 2023, https://english.news.cn/20230314/38b6491926ea4c6b82bf7d58d0518a48/c.html.

and hindered its ability to fully reap the rewards of military AI deployment and other use cases, the Chinese technology industry has made rapid progress both in finding ways around these curbs and in expanding its own semiconductor and chip production to compensate.[71]

Experts disagree about whether US-led efforts to prevent China from accessing frontier AI will ultimately prove effective. The pace of development in chips used for training AI systems is non-linear. The speed at which performance and quality improves will limit China's ability to catch-up, meaning that the gap between the AI computing resources that China's AI companies are able to access and that available to the US and to its allies, is only set to increase.[72]

While attempts to maintain a hold over others may be effective in the short term, such influence will diminish over time. This dynamic could then lead to a multipolar AI marketplace, where chokepoints are less geographically concentrated.

For some of these weaponized chokepoints in AI supply chains, alternatives will take many years to develop – with some analysts suggesting that for some it may not be possible at all. The most profound challenge is presented by ASML's ultra-violet lithography (EUV) machines. This highly specialized technology is vital for high-end chip production and can credibly claim to be the most complex machine ever made.[73] But ASML's most advanced technology has been subject to US-led export restrictions since 2019, prompting state-funded efforts by China to develop its own leading-edge EUV machines. Despite the complexity of the task, scarcity can lead to rapid innovation: in December 2025, Reuters reported that China's 'Manhattan Project' to build its own version of ASML's machines had made significant technical breakthroughs.[74]

Though it seems that this, and similar, reporting, may oversell China's progress made to date, the lesson is clear: weaponizing a technological dependency will motivate those on the receiving end to try and free themselves. While attempts to maintain a hold over others may be somewhat effective in the short term, such influence will diminish over time. This dynamic could then lead to a multipolar AI marketplace, where chokepoints are less geographically concentrated. China again provides an example of this, as it is at risk of losing one of its own – in critical mineral processing – as a result of its own overzealous use of this coercive lever.[75]

---

71 Balbontin, R. (2025), 'Backfire: Export controls helped Huawei and hurt U.S. firms', report, Washington, DC: Information Technology & Innovation Foundation (ITIF), https://itif.org/publications/2025/10/27/backfire-export-controls-helped-huawei-and-hurt-us-firms.
72 McGuire, C. (2025), 'China's AI chip deficit: Why Huawei can't catch Nvidia and U.S. export controls should remain', Council on Foreign Relations, 15 December 2025, https://www.cfr.org/articles/chinas-ai-chip-deficit-why-huawei-cant-catch-nvidia-and-us-export-controls-should-remain.
73 *The Economist* (2025), 'The race is on to build the world's most complex machine', 12 March 2025, https://www.economist.com/science-and-technology/2025/03/12/the-race-is-on-to-build-the-worlds-most-complex-machine.
74 Potkin, F. (2025), 'How China built its 'Manhattan Project' to rival the West in AI chips', Reuters, 17 December 2025, https://www.reuters.com/world/china/how-china-built-its-manhattan-project-rival-west-ai-chips-2025-12-17.
75 Bego, K. (2026, forthcoming), *Deep Connections: the hidden battles to control subsea cables*, Cambridge: Polity.

Trend 4: Growing concerns about a potential AI valuation bubble

The AI race is usually presented as a binary one between the US and China, not only due to the significant technological lead that existing companies in those countries already enjoy, but also the vastly larger amounts of spending and computing power that the US in particular is able to mobilize.

By some estimates, US-based companies attracted 75 per cent of total global VC investment in AI in 2025, with AI capturing 61 per cent of all global VC spending in that year. By contrast, the combined EU attracted only 6 per cent.[76] The UK and China[77] accounted for 5 per cent each. (China's AI ecosystem is far more reliant on government funding than any of the other examples – of the estimated $98 billion invested in AI in China in 2025, around $56 billion came from government funding.)

AI infrastructure investment from different sources is also dominated by the US. China and the US especially also dominate AI infrastructure spending and availability. In mid-2025, around 75 per cent of high-performing GPU clusters were in the US and 15 per cent were in China, while other markets had much smaller shares.[78]

No other market players or ecosystems are currently in a credible position to match the levels of US private sector spending and reproduce existing market fundamentals. A growing share of these investments, especially in the US, is being allocated to spending on infrastructure such as data centres, which many AI developers and investors argue is a necessary precondition for the development of frontier AI. If the AI race is considered as constituting three parallel races – the race towards the frontier (the development of the most cutting-edge AI), the race towards diffusion (spreading AI throughout the economy), and the race towards application (finding different use cases for the technology) – this spending 'arms race' primarily treats the first of those as the key objective. A market correction in response to growing concerns about the ability of AI investment to return a profit may revise some of these fundamental assumptions – moving the focus towards the rapid, often far cheaper, diffusion and application of the technology. With such a revision, the overall AI race could be significantly reconfigured.

Throughout 2025 and early 2026, major investment banks and market analysts issued warnings that the recent surge in AI company valuations and the vast amounts of AI infrastructure spending presented all the characteristics of a market bubble.[79] These warnings claim that valuations and spending appeared increasingly divorced from the financial forecasts on the technology's ability to generate returns – especially as monetizable adoption has yet to match expectations. In 2025 alone, the major hyperscalers – including Alphabet, Amazon's AWS, Microsoft, Meta

---

76 Organisation for Economic Co-operation and Development (2026), 'AI firms capture 61% of global venture capital in 2025', press release, 17 February 2026, https://www.oecd.org/en/about/news/announcements/2026/02/ai-firms-capture-61-percent-of-global-venture-capital-in-2025.html.
77 Kaur, D. (2025), 'China to deploy $98bn in AI investment this year amid US tech rivalry', TechWire Asia, 26 June 2025, https://techwireasia.com/2025/06/china-ai-investment-98-billion-2025-us-rivalry.
78 Pilz, K. F. et al. (2025), 'The US hosts the majority of GPU cluster performance, followed by China', data insight, Epoch AI, 5 June 2025, https://epoch.ai/data-insights/ai-supercomputers-performance-share-by-country.
79 Goldman Sachs (2025), 'AI: in a bubble?', 28 October 2025, https://www.goldmansachs.com/insights/top-of-mind/ai-in-a-bubble.

and Oracle – spent at least $300 billion on new AI infrastructure and computing hardware such as data centres, access to GPUs, chips and servers, as well as power and cooling infrastructure to enable energy-intensive AI training and inference.[80] More recent projections suggest that this spending could reach $700 billion in 2026. New investments by hyperscalers and other US AI champions like OpenAI and Anthropic reached such heights in 2025 that they accounted for almost 2 percentage points of US GDP growth, and, by some estimates, may have kept the US economy from entering a recession.[81]

While AI is an important growth industry in markets outside of the US (and much of the physical infrastructure rollout mentioned above is not confined to the US, even if many of the investors and owners are), levels of spending in most markets elsewhere in the world have been more modest (certain investors in the Gulf and large-scale manufacturers of AI-enabling goods in Asia excepted).[82]

This US-led infrastructure 'arms race' could pose a significant risk of over-investment if demand slows or the technological promise of AI is not met. Throughout 2025 and early 2026, analysts expressed concern that the valuations of companies active in AI were overly optimistic, and that investors were pouring capital into AI firms based on future revenue expectations that were far from certain to ever materialize.

One particularly significant factor in this, with relevance to this paper's discussions of the ever-closer entanglement between governments and AI companies, is the challenging economics of AI investment. While the technology itself continues to rapidly improve, and will likely have a profound societal impact, monetizing it remains a challenge.

Deutsche Bank released an analysis in 2025 that suggested the major AI players would need to make up a shortfall of around $800 billion by 2028 to recoup the investments made to date.[83] AI companies' total revenues in 2025, however, remained far lower. Persistent uncertainty and supply-chain shocks resulting from the ongoing war in Iran, which threaten to delay AI infrastructure build-outs and negatively impact chip manufacturing and put into question the long-term financial commitment of the Gulf Arab countries to fuelling global AI investment, similarly threaten to undermine assumptions behind the current AI market rally.

Predicting the potential outcomes and future trajectory of spending on AI is difficult. Current high levels of investment in AI infrastructure and solutions may persist, especially if new, higher-revenue applications or technological breakthroughs lead to mass, monetizable adoption. Nonetheless, concerns about a bursting of the AI 'bubble' are already affecting AI investments and have led investors to pivot to different sectors – including defence tech.[84]

---

80 Morris, S. and Uddin, R. (2025), 'Big Tech lines up over $300bn in AI spending for 2025', *Financial Times*, 7 February 2025, https://www.ft.com/content/634b7ec5-10c3-44d3-ae49-2a5b9ad566fa.
81 Casselman, B. and Ember, S. (2025), 'The A.I. boom is driving the economy. What happens if it falters?', *New York Times*, 22 November 2025, https://www.nytimes.com/2025/11/22/business/the-ai-boom-economy.html.
82 Staiger, R. (2026), 'AI investment and Middle East conflict shape outlook for global trade', WTO Blog, 20 March 2026, https://www.wto.org/english/news_e/news26_e/blgrs_20mar26_332_e.htm.
83 Wheeler, K. (2025), 'Deutsche Bank: Why the AI boom risks a US$800bn shortfall', AI Magazine, 25 September 2025, https://aimagazine.com/news/deutsche-bank-why-the-ai-boom-risks-a-us-800bn-shortfall.
84 Herbert, E. (2025), 'Investors pour record sums into European stocks', *Financial Times*, 20 February 2026, https://www.ft.com/content/80173261-2b72-41f7-9eae-490aabb14623.

How this trend can lead to multipolarization

The need to find reliable sources of capital may lead to more 'patriotic tech' and government–private sector entanglement

The growing interest in the defence applications of AI, as well as its importance in geostrategic competition, could enable the current levels of spending to be sustained for longer, as the beneficiaries come to be seen as 'too big to fail' from a geostrategic point of view. AI companies – especially those focused on developing frontier AI models[85] – already have a powerful incentive to promote their solutions as geostrategic tools. If commercial growth opportunities start to disappear, further securitizing the technology and turning to government becomes an increasingly attractive alternative.

AI companies are already trying to find new sources of revenue and new customer bases, in order to generate a sustainable return on the enormous investments already made. Dual-use applications of their solutions appear to be among those that companies are exploring, as discussed in previous sections.

The announcement of 'Project Stargate' – a now apparently dormant commitment to spend $500 billion on new AI infrastructure – on the first day of President Trump's current term was similarly framed as a public–private partnership to keep the US in the lead on AI.

Although the military segment of the market remains small and is not currently able to offset the high levels of general AI capital spending, it is nevertheless growing. Deeper entanglement and growing mutual interdependence between AI companies and the government will also help further position these companies as strategically important. It may also lead governments to take over some of the infrastructural spending, should the market alone no longer be able to deliver.[86] OpenAI CEO Sam Altman has frequently described his company's mission as akin to a 'Manhattan Project', with winning the race for AGI as the single most geostrategically important objective for the US. The announcement of 'Project Stargate' – a now apparently dormant commitment to spend $500 billion on new AI infrastructure – on the first day of President Trump's current term was similarly framed as a public–private partnership to keep the US in the lead on AI.[87] The involvement of AI companies and AI infrastructure providers like Nvidia in the export-focused aspects of the

85 In the event of a collapse in the commercial AI market, especially one centred around a loss of trust in the return on investment from large language models, the interest in more specific defence or dual-use solutions will not necessarily follow immediately. It is important not to use the current interest in frontier AI models as shorthand for the full AI landscape, which is diverse, and includes many mature solutions with only limited connection to, or need for, the current capital-intensive data centre build-out.
86 Hammond, G. and Acton, M. (2025), 'Sam Altman says OpenAI is not 'trying to become too big to fail', *Financial Times*, 6 November 2025, https://www.ft.com/content/5835a5a3-36db-41d7-9944-d9823dbdffc5.
87 Gardizy, A. (2025), 'Inside OpenAI's Scramble to Get Computing Power After Stargate Stalled', The Information, 22 February 2026, https://www.theinformation.com/articles/inside-openais-scramble-get-computing-power-stargate-stalled.

US government's AI Action Plan,[88] which explicitly focuses on exporting the US AI stack to like-minded nations as a geostrategic instrument, also helps create commercial opportunities for these companies and can generate vendor lock-in in new markets.

This dynamic may further encourage the growing closeness between governments and the AI sector – which could expedite the trends towards patriotic tech, global distrust and sovereignty discussed in previous chapters.

The market may shift towards cheaper, open-source models if frontier models fail to deliver returns

Though no market will be immune from the wider economic fallout of a market correction in the US, not all AI ecosystems are equally exposed to this risk. China and, to an extent, the EU and certain middle powers like India, have placed an emphasis on the rapid diffusion of leaner, cheaper and frequently open-source models over the highly capital-intensive AI frontier.[89] Races over technology have not infrequently been won by the countries best able to implement and diffuse an innovation, rather than those that initially developed it. The AI bubble popping could validate this point again.

China's open-source AI players would be among the main beneficiaries of such a scenario, as already, their models do not significantly lag behind – and occasionally outperform – far more capital-intensive US models. Recent events demonstrate this dynamic in action. In the aftermath of the January 2025 launch of China's DeepSeek R1 model – a relatively cheap-to-train, open-source AI model, which by most metrics was only modestly behind more expensive US 'frontier' models in performance – suggested that high-performing AI models could be developed without spending big – or even having access to the most advanced AI chips.[90]

The ensuing brief market panic over DeepSeek suggests that any bursting of the AI market bubble could cause a more permanent shift towards cheaper, less capital-intensive innovation, which could make it possible for other actors to compete. Since then, many more even higher performing Chinese open-weight and open-source models have been launched.

Smaller countries may have a 'second-mover advantage'

In the aftermath of the AI bubble bursting, more established AI players could end up the beneficiaries of a correction through the reduction of competition, consolidation of their market share and ability to hoard cheap infrastructure,[91] intellectual property and talent. This could make it even more difficult for others to catch up. The dynamic could, however, also move the market in the other direction.

---

88 The White House (2025), *Winning the Race*.
89 Sheng, K.-S. (2026), 'China's 'Frugal Stack' and Its Path to AI Diffusion', The Diplomat, 20 January 2026, https://thediplomat.com/2026/01/chinas-frugal-stack-and-its-path-to-ai-diffusion.
90 There is still some dispute about the origins of the GPUs that DeepSeek was trained on.
91 There is, however, reason to believe that AI infrastructure, especially computing power, differs from the dot-com infrastructure oversupply, because of the relatively rapid depreciation of assets like GPUs.

Countries currently behind the leaders in the AI infrastructure rollout may find themselves with fewer stranded assets and access to cheaper computing power and other AI resources. This may allow them to avoid the costly mistakes made by others and integrate AI across their wider economies more efficiently and cost-effectively – what is known as a 'second-mover advantage'. Previous infrastructure bubbles, such as the one that led to the dot-com crash of the early 2000s, suggest that a widespread market collapse would leave a lot of stranded assets, unused infrastructure and resources, which other actors could then acquire at low cost.

Smaller competitors may also benefit from the greater availability of talent, with a lack of skilled AI engineers presently one of the main barriers to companies seeking to build or make use of the technology. Governments and militaries may also be able to bring more AI talent into their ranks. Such a reallocation could speed up dual-use AI development and deployment, and could further diversify (and securitize) the industry.

03
How can the private sector prepare? Likely outcomes and recommendations

The private sector will need to anticipate change and better equip itself to operate in this more fragmented, multipolar and securitized future. This chapter provides recommendations on how.

As AI starts to be embedded in systems across virtually all sectors of the economy, the technology will only become more central to geopolitical and economic competition. It is not just those directly involved in developing AI systems or those in the business of selling AI solutions that need to prepare for the consequences of multipolarization and fragmentation. The impact of the trends described above would inevitably cascade far beyond the tech industry itself.

Some of this reconfiguration can bring benefits. A more geographically diverse AI market would unlock new sources of funding and innovation. It would help private sector actors in currently smaller AI markets to better compete with those in the US and China, and could bring more innovation and vibrance to AI development more generally as ideas flow from a greater diversity of sources, reflecting a wider range of demands and perspectives. India's growing market for

government solutions specifically tailored to the needs of developing countries offers an example.[92] A growing number of European startups are looking beyond the dominant large language model (LLM) towards developing 'World models' (meaning AI solutions that interact and learn from the physical world).[93]

Private sector actors keen to adopt or invest in AI may similarly find themselves in a position to choose from a wider set of solutions, visions and technologies. Diversifying and decentralizing the market for a technology potentially as transformative as AI away from two countries – and, as importantly, a small number of dominant companies in those countries – would both reduce the leverage and power these actors have over the technology's development and limit their ability to weaponize dependencies. A more diverse market also reduces the risk of groupthink in the industry, and could help prevent a narrowing of perspectives of what kinds of AI solutions are developed.

This securitized, multipolar AI sphere may, however, also bring new risks, especially as these developments take place in an already more geopolitically tense, fractious global order. This final chapter explores the second-order impacts that may result from the developments discussed above. It then offers recommendations for how companies across different sectors may best prepare for this future.

A less open, more protectionist global technology marketplace

The current global push towards tech sovereignty could result in a more fragmented, less open global marketplace for innovation, especially in technologies perceived to be of great geostrategic importance – like AI. In such a world, private sector actors accustomed to operating across borders and jurisdictions may find themselves facing more restrictive operational environments, forced to overcome growing trust deficits and potentially pushed out of existing markets altogether.

By emphasizing their sovereign credentials, local firms may instead benefit from this shift and could see demand increase from both governments and private sector actors in their home markets and those closely aligned. Many governments are already becoming more proactive about using procurement and other tools to favour and help scale homegrown solutions. Private sector actors, too, are increasingly interested in supporting or switching to domestic suppliers, especially if customer demand for sovereign tech increases and concerns about external dependencies grow.

The push for sovereignty may, however, also become a source of friction for those buying and integrating AI tools into their own workflows. Paying the 'sovereignty premium' could come to be seen as a business imperative, especially if public and

92 Sahasranamam, S. (2026), 'How the Global South is reimagining the future of AI', opinion, World Economic Forum, 10 February 2026, https://www.weforum.org/stories/2026/02/how-the-global-south-is-reimagining-the-future-of-ai.
93 van Romburgh, M. (2026), 'Turing Winner LeCun's New 'World Model' AI Lab Raises $1B In Europe's Largest Seed Round Ever', Crunchbase News, 10 March 2026, https://news.crunchbase.com/venture/world-model-ai-lab-ami-raises-europes-largest-seed-round.

government pressure grows. Governments may start to implement more coercive measures to force the private sector to adopt domestic alternatives to major external AI providers. Measures imposing financial penalties on companies for their exposure to foreign dependencies (not unlike the model used for carbon taxes) or forced decoupling motivated by national security concerns could become more common.

Such pressures could present challenging new trade-offs. By opting for sovereign solutions – whether out of patriotic duty or in response to public pressure or government requirements – private sector consumers of AI may have to forgo what they perceive to be the most technologically mature or cutting-edge solutions. While 'good enough' tech can help strengthen the overall technology ecosystem in a market, a strategic transition to less established solutions may – especially in the shorter term – affect the ability of an economy to fully seize the opportunities of AI.

The transition to alternative suppliers could also introduce new security risks, as customers migrate away from sometimes long-embedded, deeply integrated tech stacks towards new, potentially less mature and well-vetted alternatives. These are risks that would likely reduce over time, as domestic alternatives scale and grow their market shares. Planners should, though, account for another less likely, but possible scenario in which a more permanent, multi-speed technology environment emerges, where some markets continue to rely on less advanced solutions – another parallel with the Cold War, during which supply chains and innovation diffusion were similarly far more arranged along political and ideological lines.

'Buy local' imperatives will pose an existential challenge for companies that already (or hope to) have a global presence, which may find themselves operating in a more restrictive marketplace.

'Buy local' imperatives will pose a potentially existential challenge for companies that already (or hope to) have a global presence, which may find themselves operating in a more restrictive marketplace. This risk is heightened for technology and defence companies, which could see themselves lose market share to sovereign alternatives. Even in the likelier scenario where companies will retain market access, these actors nonetheless are likely to face increased pressure to provide guarantees that their products are not contingent on the benevolence of their respective home governments. In practice, such guarantees may be difficult to provide in a global environment where national governments increasingly undermine international norms and laws, and seek to weaponize the strength of their private sector.[94]

94 The 2018 US CLOUD Act, for example, make it obligatory for any US company to share data stored on their services – even those stored abroad – with the US government, if national security concerns demand so.

This could present difficult trade-offs. In their attempt to diversify their own technology stacks to placate foreign customers, companies may find themselves under increased scrutiny from their home governments, which could perceive such actions as counter to their policies and perceived national interests.

How companies can prepare

- **Establish a permanent geopolitical risk function** to monitor geopolitically motivated operational risks, including the progress and nature of 'buy local' policies and government efforts to bolster their strategic autonomy in tech. More importantly, companies should map their own technological and supply-chain dependencies, and work to understand how these may be made more resilient or diversified. Diversifying dependencies does not necessarily have to mean reordering a full technology stack. It could also encompass more limited measures, such as ensuring that back-up solutions and multiple, redundant options are in place.
- **Conduct regular 'tech decoupling' stress tests** to model the implications of a sudden loss of market access or a forced supply-chain and infrastructure decoupling (e.g. localization of cloud storage).
- **Develop and design infrastructure architectures that can be replicated across a variety of markets** in order to comply with intensified sovereignty or data-localization requirements. Companies should ensure that systems are compatible with multiple cloud providers and AI solutions, and identify which aspects of their business activity may invite such scrutiny. For example, a pharmaceutical company may not need to use a local AI alternative for medicine discovery, but will need to consider switching to sovereign AI solutions if it plans to feed personal data into AI models.
- **Structure corporate entities and AI and wider tech stacks to allow genuine legal and operational separation across regions.** Companies should embrace the principle of openness in technology stacks. Diversifying inputs can not only bring greater resilience, but also avoids accusations of so-called 'sovereignty-washing' – where large incumbents present their existing solutions as sovereign or local by using artificial legal separations.

Fragmentation and regulatory uncertainty

As the AI sector securitizes and the geostrategic dimension of the AI race becomes so important that falling behind is increasingly considered to be an existential economic and security threat, governments' willingness to place regulatory guardrails on development of the technology will continue to diminish.

2025 already partially demonstrated this trend, with both the US and the EU revisiting earlier regulatory commitments on AI, and countries like Japan are relaxing rulebooks in favour of implementing pro-innovation regimes. For example, the EU temporarily watered down and delayed the implementation of its landmark AI Act, after member state concerns over the constraints placed on would-be European AI champions. The EU's Digital Omnibus, a package of amendments aimed

to simplify and reduce bureaucracy in its existing digital regulation, is about 'cutting red tape' to promote innovation and growth.[95] In the US, President Trump has revoked several of his predecessor's executive orders that placed limitations on the rollout of AI.[96]

The dynamics discussed in this paper may lead to more widespread deregulatory momentum and greater fragmentation in approaches to AI. In a multipolar AI marketplace, more countries would be able to establish themselves as builders of the technology and therefore as market 'shapers', not just market 'takers' reliant on regulation to influence AI's parameters. Incentives around regulation may change as a result. Although Europe has, for example, long relied on the so-called 'Brussels effect' (the idea that the EU could set global standards via strict regulation of its large internal market) to shape global markets, it is increasingly embracing the idea that control over infrastructure, rather setting the rules, is the main source of influence and power in the digital economy.

Military or national security (and, by extension, dual-use) applications of AI frequently enjoy exemptions from existing regulation, partly because of the ambitions in many central governments to put AI at the heart of their defence strategies. An example is the EU's AI Act, which does not cover technologies with an explicit national security or military application. Given the significant dual-use nature of AI, this is a distinction that is becoming increasingly porous. More companies exploring dual-use applications of their products will therefore shrink the pool of solutions covered under existing rulebooks. AI companies promoting the geostrategic importance of their solutions will have greater incentive to promote a reining-in of regulation (or, conversely push safety narratives that help cement their market position). Defence imperatives may also add to pressure on leading AI companies to lower safety standards. The recent spat between Anthropic and the Pentagon provides a particularly salient, high-stakes example.

A fragmenting global order, characterized by waning international cooperation and adherence to international law, paired with an accelerating AI arms race, leaves few incentives for countries to collaborate on developing global rules for a technology that many governments believe may be the key to power in the 21st century.

The rush to innovate and deploy AI impacts regulation and governance beyond the domestic level. A fragmenting global order, characterized by waning international cooperation and adherence to international law, paired with an accelerating AI

95 Carpenter-Zehe, O. (2025), 'Privacy and AI fears, in EU bonfire of digital red tape', euobserver, 18 October 2025, https://euobserver.com/25932/privacy-and-ai-fears-in-eu-bonfire-of-digital-red-tape.
96 The White House (2025), 'Removing Barriers To American Leadership In Artificial Intelligence', executive order, 23 January 2025, https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence.

arms race, leaves few incentives for countries to collaborate on developing global rules for a technology that many governments believe may be the key to power in the 21st century.

Coordination is especially unlikely when it comes to the more geostrategic applications of AI, such as those in the growing dual-use realm. While global governance initiatives like the annual AI Summit series and the Responsible AI in the Military Domain (REAIM)[97] continue to attract participation, both the depth of resulting communications, as well as the number of governments signing on to them, continues to decrease – with major powers like China and the US, as well as others like Russia, increasingly opting out.[98] The pace of military AI deployment and development in wars in the Middle East, Ukraine and elsewhere will make it difficult for any durable, global regulatory approaches to emerge.

A more fragmented, deglobalized technology landscape, in which countries increasingly cordon off access to their technology markets and develop alternative technical standards and regulatory frameworks, could even see different technology stacks become incompatible. A wholesale decoupling like this will be especially difficult to prepare for – and would result in a global economy vastly different from the one that has prevailed since the end of the Cold War.

Uncertainty about the degree and nature of these policy changes create a difficult environment for businesses. More restrictive, but predictable, regulatory regimes may frequently be preferable over a light-touch, but constantly changing, rulebook. Navigating a wide range of regulatory approaches, as well as persistent uncertainty as governments delay committing to long-term frameworks, is already a significant source of friction.

How companies can prepare

- **Continue to invest in robust internal AI governance processes** in the absence of binding frameworks, to pre-empt regulatory shocks and reduce internal risks. Establishing robust safety standards and processes (including documentation, red-teaming, transparency and auditability) can also become a competitive edge, allowing a company to be seen as more trustworthy by some customers.
- **Design modular governance frameworks that can be adapted to diverging regulatory regimes.** Ensure that in-house knowledge of AI use is retained, so that risks can be mapped and mitigated ahead of time, and processes put in place to adapt to potentially stricter future standards.
- **Work closely with private sectors peers to strengthen regulatory collaboration and promote shared standards.** In the absence of coordinated government action, the private sector – especially companies in high-risk sectors

97 Spanish Ministry for Foreign Affairs, the European Union and Cooperation (2026), 'REAIM', https://www.exteriores.gob.es/en/REAIM2026/Paginas/Cumbre26.aspx.
98 Waldersee, V. (2026), 'US, China opt-out of joint declaration on AI use in military', Reuters, 5 February 2026, https://www.reuters.com/business/aerospace-defense/us-china-opt-out-joint-declaration-ai-use-military-2026-02-05.

such as healthcare, law enforcement and defence – can play an important role in pushing governments to adopt robust, enforceable and predictable standards for AI safety and other considerations.

Heightened security risks

A more fragmented AI market may also lead to new and increased security risks, as harmful AI solutions proliferate and the deteriorating global security environment means bad state and non-state actors become more willing and able to exploit weaknesses.

As advanced AI tools become cheaper, easier to deploy and less dependent on large pools of specialized expertise, smaller states and non-state actors will be better able to catch up with traditionally dominant players, altering established power dynamics. Such democratization, however, also provides more opportunities for dangerous capabilities to diffuse. In this more multipolar AI environment, some countries could start to make an absence of guardrails and a willingness to export offensive, high-risk tools selling points for their respective AI offerings. This risk is not hypothetical: countries like Russia are increasingly building – and field-testing – sophisticated dual-use AI solutions of their own and may well see a financial and strategic opportunity in exporting these capabilities.

While some countries and companies, in a bid to improve safety or avoid controversy, already limit the extent to which certain dual-use solutions can be accessed (Anthropic's recent decision to delay the release of its Mythos model due to concern over its capabilities is an example),[99] others with fewer scruples may be motivated to fill the resulting market vacuum. While existing, widely available commercial AI tools can already be used to great effect to increase the effectiveness and scale of, for example, cyberattacks and misinformation campaigns, in this scenario far more sophisticated capabilities could become available 'off-the-shelf'. This is a dynamic not dissimilar to the proliferation of spyware tools,[100] which has similarly become a niche, but lucrative area of tech development dominated by a select few countries, which in particular relies on selling high-end capabilities to governments that frequently lack the domestic capacity to develop them.

Democratization of a technology generally makes it far more difficult to limit the proliferation of harmful capabilities and prevent unscrupulous actors from gaining access to more advanced tools. For private sector actors, this means that the AI-enabled cyber and kinetic threats they face could become more frequent, more sophisticated and more harmful. Further investment in bolstering cybersecurity capabilities and capacity will then be necessary, as will the hardening of physical infrastructure. Physical infrastructure used for AI is also becoming a prime target as the strategic and economic significance of the technology grows. For example,

---

99 Vicens, A. J. and Satter, R. (2026), 'AI-boosted hacks with Anthropic's Mythos could have dire consequences for banks', Reuters, 13 April 2026, https://www.reuters.com/legal/litigation/ai-boosted-hacks-with-anthropics-mythos-could-have-dire-consequences-banks-2026-04-13.
100 Shires, J. (2024), *Principles for state approaches to commercial cyber intrusion capabilities*, Research Paper, London: Royal Institute of International Affairs and RUSI, https://doi.org/10.55317/9781784136277, ch. 2.

in early 2026, Iran targeted data centres owned by US hyperscalers in the Gulf Arab countries to complicate ongoing military operations, but also to undermine these countries' ambitions to diversify their economies through AI investment.[101]

A more fragmented technology environment in which countries are less interconnected may also see barriers to escalation in the cyber and hybrid domains lowered. Concerns about retaliation through the same technical systems, and about potential spillover and 'blowback' (where an attack targeting another country's systems undermines the attacker's own) serve as deterrent factors that could encourage states to practice restraint. An example of such blowback resulting from cyber activities was the 2017 NotPetya cyberattack, which generated an estimated $10 billion[102] in damages worldwide and was attributed to Russian proxies intending to undermine Ukrainian systems, but in the process caused significant harm to Russian-linked systems and entities.[103] As technological systems are delinked, and countries become less reliant on AI and dual-use solutions provided by others, some of this restraint may start to fall away.

Examples of this dynamic are already apparent in the hybrid and cyber domains, where so-called 'spoilers' in the system – countries like Iran, North Korea and Russia, which are considered to have relatively little to lose from undermining global systems they exist outside of – have become more brazen in their operations. In a securitized, fragmented world, systems will likely be targeted even more often by state actors and their proxies. As much of the critical infrastructure and systems behind AI is privately owned, attacks like these will be a source of increased risk companies will need to prepare for.

How companies can prepare

- **Invest in bolstering cyber defence capabilities** – for example, in-house cyber capacity, red-teaming activities to identify weaknesses, 'airgapping' and duplication critical systems, decentralization of data storage, redundancy and data protection practices, and development of crisis responses and protocols – to better prepare for a more volatile world, in which AI will serve as an increasingly important force multiplier for states and non-state actors alike.
- **Map the potential weaknesses and vulnerabilities in physical systems and infrastructure** that may be targeted through AI-enabled physical sabotage attacks (e.g. via increased drone activity or targeting of undersea power lines or fibre-optic telecommunications cables). Companies should work closely with governments and militaries to allocate responsibility during a crisis and develop protocols. They should also consider ways in which critical infrastructure may be made less vulnerable to attack, and seek to improve deterrence.

---

101 Nisha, R. (2026), 'How conflict is threatening the Gulf's cloud infrastructure', Technology Magazine, 13 March 2026, https://technologymagazine.com/news/how-war-is-damaging-the-middle-easts-data-centre-ambitions.
102 Johansmeyer, T. (2025), 'NotPetya, Ukraine, and the Limits of Economic Impact from Cyber Attacks', European Consortium for Political Research The Loop blog, 18 August 2025, https://theloop.ecpr.eu/notpetya-ukraine-and-the-limits-of-economic-impact-from-cyber-attacks.
103 Foreign & Commonwealth Office, National Cyber Security Centre and Lord (Tariq) Ahmad of Wimbledon KCMG (2018), 'Foreign Office Minister condemns Russia for NotPetya attacks', press release, 15 February 2018, https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks.

About the author

Katja Bego is a senior research fellow in Chatham House's Europe Programme. Prior to joining the Europe Programme, she was a senior research fellow in the institute's International Security Programme, where she was also the co-editor of the *Journal of Cyber Policy*. Her upcoming book, *Deep Connections: The Hidden Battles to Control Subsea Cables*, will be published by Polity in September 2026.

Katja's primary expertise lies in topics related to European security, strategic autonomy and competitiveness, as well as the geopolitical and geoeconomic competition over emerging technology. She has a particular interest in topics related to Europe's role in a rapidly changing global order, tech sovereignty, and economic and grey-zone warfare.

Acknowledgments

The author would like to thank the anonymous peer reviewers for their valuable feedback, as well as Chatham House colleagues in publications for their support and advice throughout the editorial process. Thanks are also due to the colleagues and external experts who generously contributed their time and insights in interviews and workshops. Finally, the author would like to acknowledge the support of the AI Collaborative at the Howard Baker Forum in making this work possible.

Cover image: HX-2 AI strike drones by German defence technology company Helsing are displayed at the Bundeswehr Innovation Centre in Erding, Bavaria, 2 February 2026.
Photo credit: Copyright © Michaela Stache/AFP/Getty Images

ISBN 978 1 78413 681 9
DOI 10.55317/9781784136819

Cite this paper: Bego, K. (2026), *How a surge in defence and dual-use technology investment could reconfigure the global AI race*, Research Paper, London: Royal Institute of International Affairs, https://doi.org/10.55317/9781784136819.

This publication is printed on FSC-certified paper.
designbysoapbox.com

Independent thinking since 1920

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700
contact@chathamhouse.org | chathamhouse.org

Charity Registration Number: 208223