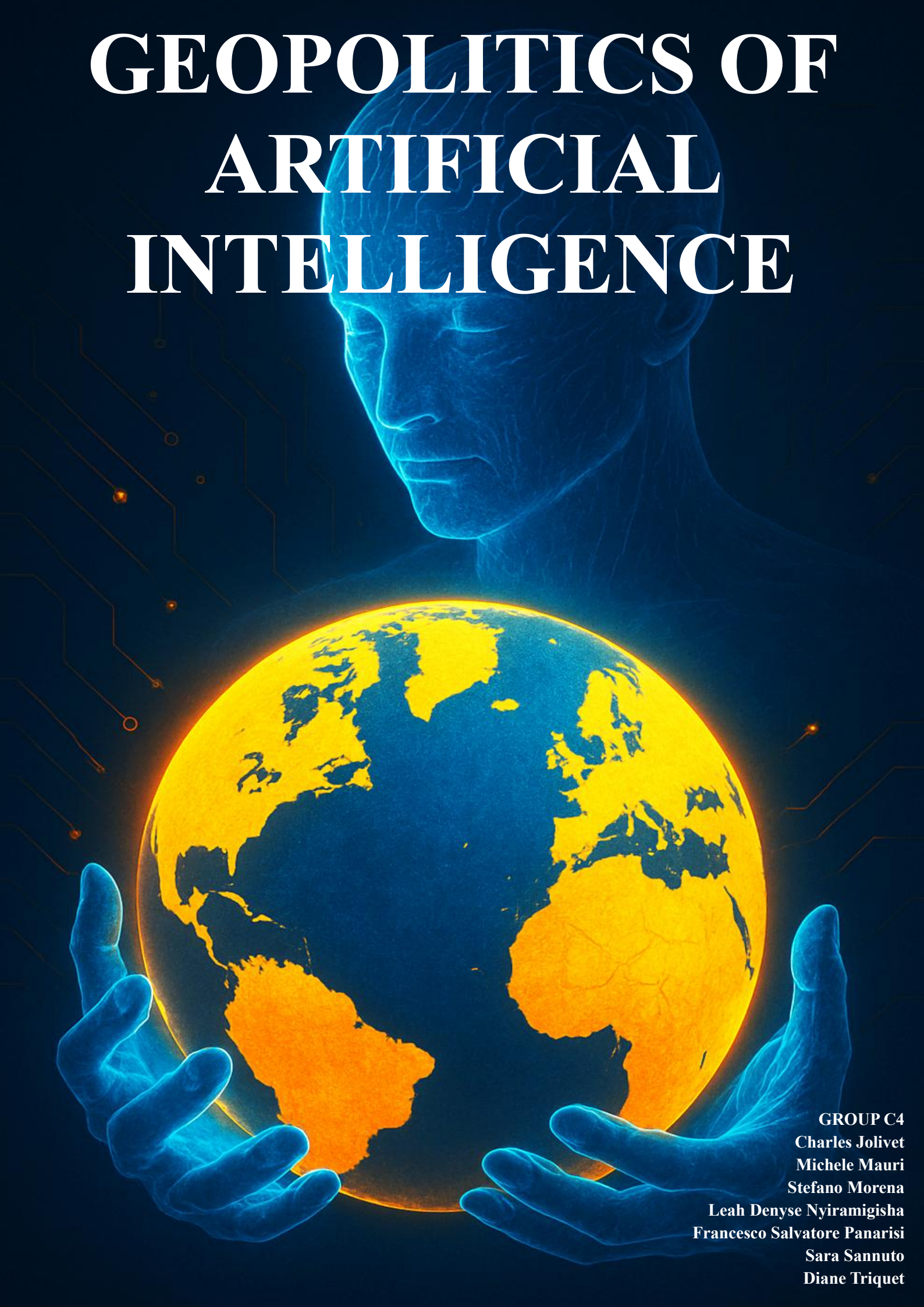
GEOPOLITICS OF ARTIFICIAL INTELLIGENCE



GROUP C4
Charles Jolivet
Michele Mauri
Stefano Morena
Leah Denyse Nyiramigisha
Francesco Salvatore Panarisi
Sara Sannuto
Diane Triquet

TABLE OF CONTENTS

1 INTRODUCTION

Control over technology has always been a cornerstone of geopolitical power. Today, Artificial Intelligence (AI) is not just a disruptive innovation – it is the primary battleground for global dominance. AI is reshaping several core dimensions of the geopolitical landscape – including economic and technological competition, global inequality, defence, energy, and more – and is therefore poised to become a decisive factor in shaping the next world order.

AI's global relevance is best understood by recognizing its nature as a General-Purpose Technology: broadly applicable across sectors, continuously improving, and capable of driving complementary innovations. Its transformative effects include deep shifts in productivity, labour markets, global power dynamics, and governance systems. Due to its boundless potential, nations around the world are fiercely competing to assert dominance in the AI race – deploying techno-nationalist strategies and weaponizing the entire value chain that underpins this transformative technology.

This report explores the geopolitical significance of Artificial Intelligence (AI) by analysing both its impact on traditional power dynamics and the new challenges it introduces. The analysis unfolds across two complementary levels: a state–based assessment of key countries – such as the United States, China, and others – and companies, and a thematic exploration of cross–cutting issues like digital colonialism, infrastructure, and governance. Particular emphasis is placed on the growing rivalry between the U.S. and China, which epitomises the broader geopolitical tensions around AI. The final section presents two case studies: the deployment of Huawei's Safe City surveillance system in Serbia, and the rise of DeepSeek's open-source AI model in China, both of which illustrate how AI is already being used as a strategic asset to project power and reshape the global order.

2 AI AS A GLOBAL STRATEGIC RESOURCE

2.1 WHY IS IT RELEVANT?

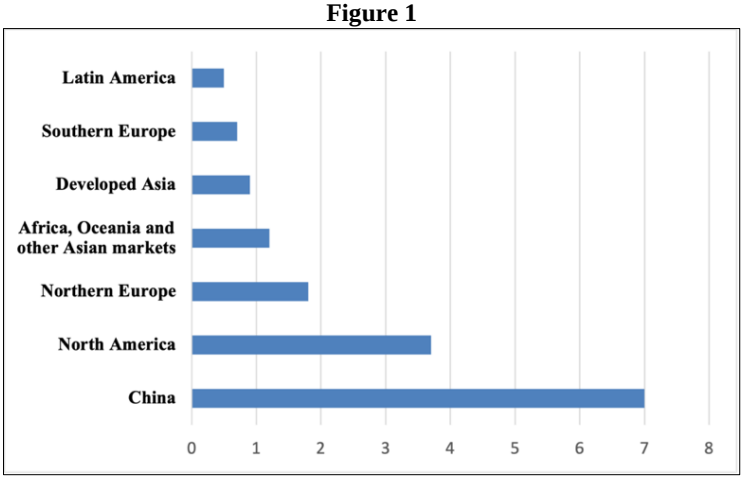
As a General-Purpose Technology, AI has the potential to deeply enhance key aspects of national power, contributing directly to a country's geopolitical influence through socioeconomic, technological, and strategic advancements.

The pivotal role of Artificial Intelligence in the geopolitical arena is best understood through its economic impact, as it confers significant competitive advantages in productivity, innovation, and market efficiency – translating directly into economic power that strengthens a nation's global influence. Multiple studies converge on AI's potential as a key driver of GDP growth in the years ahead. According to McKinsey & Company (2023), the cumulative global economic impact of artificial intelligence – AI and generative AI combined – could reach up to $25.7 trillion. Indeed:

a. AI significantly enhances productivity by automating repetitive and routine tasks, reducing human error, and enabling workers to focus on higher-value activities. It also allows for the automation of complex workflows, optimisation of resource allocation, and improved operational efficiency across capital-intensive industries such as manufacturing, logistics, and energy. According to estimates, global AI-related productivity gains could reach $6.6 trillion by 2030 (PwC, 2017), or add approximately 3.5 percentage points to global productivity over ten years (ECB, 2025)
b. AI acts as a powerful driver of innovation by accelerating product development, scientific discovery (e.g., molecule and materials design), and the emergence of entirely new business models – such as autonomous systems, adaptive supply chains, and personalised content engines. AI, particularly generative AI, is increasingly recognised as a method of invention, reshaping the boundaries of creativity and R&D (OECD, 2024).
c. AI stimulates consumption through deeper product personalisation and real-time responsiveness to consumer preferences, ultimately boosting demand (PwC 2017, McKinsey 2023)
d. AI also offers significant social spillovers. In healthcare, AI enables earlier diagnosis, personalised treatments, and better resource allocation. In education, it supports adaptive learning tools and accessibility for underserved communities. For governments, AI enhances policy design, tax compliance, public service delivery, and crisis response (e.g., during pandemics or natural disasters). These applications contribute to greater equity, inclusion, and institutional efficiency,
e. Finally, AI has a growing military and strategic impact; from autonomous weapon systems and intelligence to cyberwarfare capabilities and surveillance infrastructure, AI is becoming a key enabler of strategic superiority.

AI is a force multiplier and the most important asset in this era due to its wide and deep spillover effects: winning the AI race means gaining economic, technological, and strategic power. The United States and China, as the leading contenders, are competing across multiple domains – including research, infrastructure, standard-setting, and global influence – to achieve this goal. Figure 1 showcases PwC's (2017) forecast for how the expected $15.7 trillion growth in global GDP by 2030 will be distributed across regions.

Figure 1



Source: PwC (2017)

2.2 WHY IS IT GLOBAL?

Inputs and supply chains needed for AI systems development are globally distributed, involving data sourced from multiple regions, computing hardware manufactured across wide international networks, and talent pools spread across continents. From chip design in the United States, to semiconductor fabrication in Taiwan and South Korea, to cloud infrastructure hosted in Europe and Asia, AI development depends on a deeply interconnected global ecosystem. For instance, the production of an AI chip involves raw materials extracted in China, a design developed in the United States by companies like NVIDIA or AMD, manufacturing carried out in Asia, particularly in Taiwan and South Korea, and finally, assembly, testing, and packaging conducted in countries like Malaysia or Vietnam.

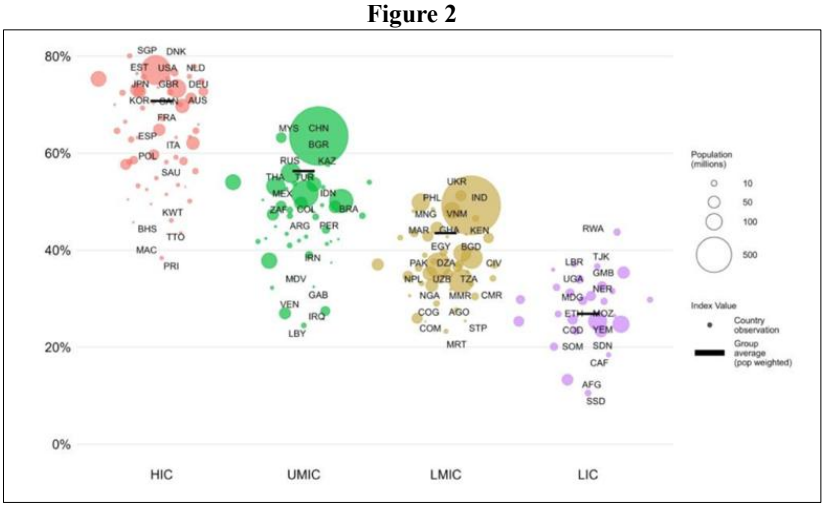
Outputs and effects are global too. Once developed, AI systems are accessed worldwide and deployed through global cloud infrastructures. Machine learning models often continue collecting user data in real time, generating ongoing cross-border information flows. This raises concerns for national security: Gartner (2025) predicts that by 2027, 40% of AI-related data breaches will arise from the misuse of cross-border generative AI, highlighting the growing risk of flow-breaking exploits leading to sensitive data leak.

AI also affects global financial stability. As reported by the Bank of England (2025), the use of AI in high-frequency trading is encouraging herd behaviour among traders, increasing the risk of market volatility and systemic shocks.

Environmental impacts are global too. Although AI can help optimise energy efficiency, training and deploying LLM require massive amounts of electricity and water, particularly for cooling data centers. This rising environmental footprint adds further complexity to the global management of AI technologies.

A main global effect of AI it's that expected economic benefits will not be evenly distributed across countries. Those with an elevated stock of assets such as talents, infrastructure, data, computing power etc., like High Income Countries and wealthier Developing countries (see figure 2, showing the AI preparedness Index by Country Income Group 2024), hold an elevated advantage in capturing AI-related economic value.

Figure 2



Source: IMF AIPI Index

This will lead to the potential breakthrough of three main consequence in the years ahead.

1) Due to their leadership position in the AI race, the United States and China are projected to consolidate their roles as superpowers in the geopolitical and economic landscape, capturing the largest GDP gains from artificial intelligence. On the other hand, thanks to strong education systems and innovation ecosystems, middle or secondary powers – such as Canada, France and the UK – can harness AI to amplify their global influence (Lazard, 2023)
2) AI may widen global inequality; the Global South has structural limitations in AI adoption due to the lack of the strategic assets previously cited. Moreover, in advanced economies the adoption of AI – particularly generative AI – is expected to foster complementarity through augmentation and to generate new roles through reinstatement. In contrast, in developing countries, AI is more likely to act as a force of substitution, increasing the risk of job displacement. Automation may devalue the comparative advantage of developing countries and worsen their terms of trade. However, despite of this pessimistic scenario, some authors argue that AI represent a double-edged sword; it also "has the potential to integrate a nexus of technologies enabling digitizing developing nations to leapfrog into a data-centric, knowledge-driven, sustainable growth." (Manning, 2020). AI can, in fact, be applied to a wide range of sectors in developing economies: from precision agriculture and accessible healthcare to personalised education and financial inclusion. In Kenya, AI-powered platforms like M-Pesa are being applied to optimise financial inclusion and improve healthcare access in rural areas. In Rwanda, digital health assistants and AI-enabled diagnostics are filling critical gaps in the national healthcare system.
3) Some emerging markets, well equipped with only few of the necessary inputs, may still have the opportunity to grow rapidly by strategically leveraging those assets. India, for example, can capitalise on its vast pool of talent and rich data resources to position itself as a global hub for AI services. Indonesia, on the other hand, possesses abundant energy resources – crucial for powering the data center infrastructure required for AI training – as well as a rapidly expanding digital population generating massive amounts of data.

3 MAIN ACTORS

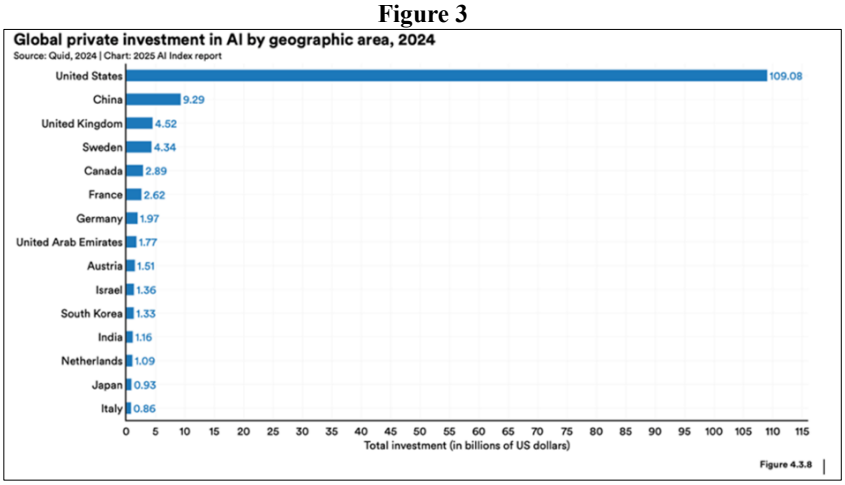
3.1 USA

As AI continues to reshape industries, economies, and governance frameworks, the U.S. maintains a position of clear dominance which is reinforced year after year by its unmatched capacity for innovation, investment, and talent attraction. The Stargate project, announced by President Donald Trump in January 2025, clearly illustrates the country's power and the record-breaking

investment amounts allocated to artificial intelligence, positioning the AI sector as a true strategic priority for the nation. This $500 billion investment plan is a joint venture between OpenAI, SoftBank, Oracle, and MGX. The aim of this initiative is the construction of 10 data centers in the U.S. by 2029 to face the growing competition from other powers, including China. President Donald Trump even described it as "the largest AI infrastructure project by far in history (BBC, 2025)." Stargate aims to bolster American technological sovereignty and foster the creation of more than 100,000 jobs. In a tense international context, the need to regain technological sovereignty through national technological partnerships (Microsoft, Nvidia, Oracle, etc.) is imperative, with semiconductor dependency at the centre of the debate. While the Stargate project perfectly illustrates the global importance placed on AI, the United States is in fact already a leader in many branches of this field.

According to the Stanford 2024 Global AI Vibrancy Ranking, a well-known ranking covering 36 countries and based on 42 indicators such as R&D, Responsible AI, Economy, or Education, the US ranks first globally, outperforming all other countries across nearly every key indicator used to assess national AI ecosystems. This leadership position is not accidental but the result of a powerful convergence of factors: a thriving academic research base, unparalleled private sector investment, a robust culture of entrepreneurship, and access to high-performance computing infrastructure. In 2024, the U.S. reached a total of $109.08 billion (figure 3) in private investments, which 11.7 times greater than the investment of China, its closest competitor. American tech companies – such as OpenAI, Google DeepMind, Meta, Microsoft, and Amazon – are at the forefront of developing and deploying large language models (LLMs) and other frontier AI systems that are shaping global standards and expectations.

Figure 3

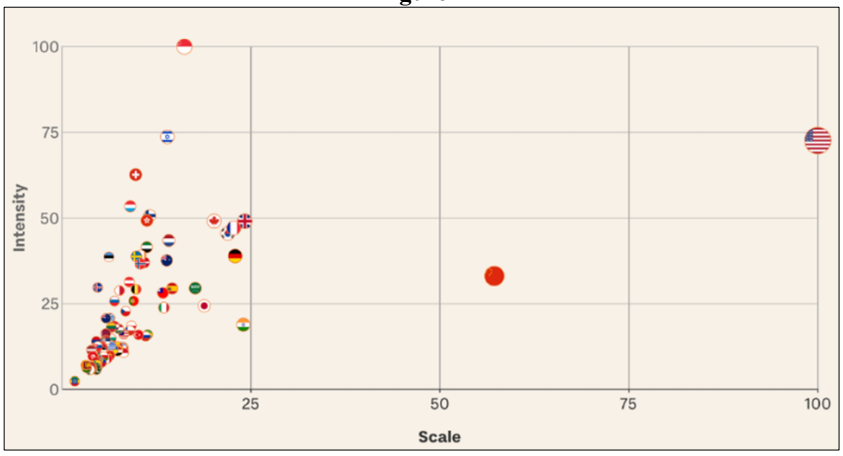


Source: Stanford (2025)

This surge in investment is closely tied to the generative AI boom, which alone attracted $29.04 billion in global private capital. The United States continues to dominate here as well, accounting for the vast majority of generative AI investment (China, at the second place attracted $2.11 billion the same year).

Another measure of leadership is the production of cutting-edge AI models including some of the most capable open-source and commercial models released by firms like OpenAI, Anthropic, Meta, and Google DeepMind. While the U.S. excels in scale – absolute AI capacity, i.e., a country's overall output – and innovation – national AI capacity relative to the size of a country's population or economy – (see figure 4), the performance gap with Chinese models is narrowing, with models from institutions like Tsinghua University and Alibaba increasingly ranking among the global top performers on multilingual and multimodal benchmarks.

Figure 4



Source: Tortoise Media Global AI Index

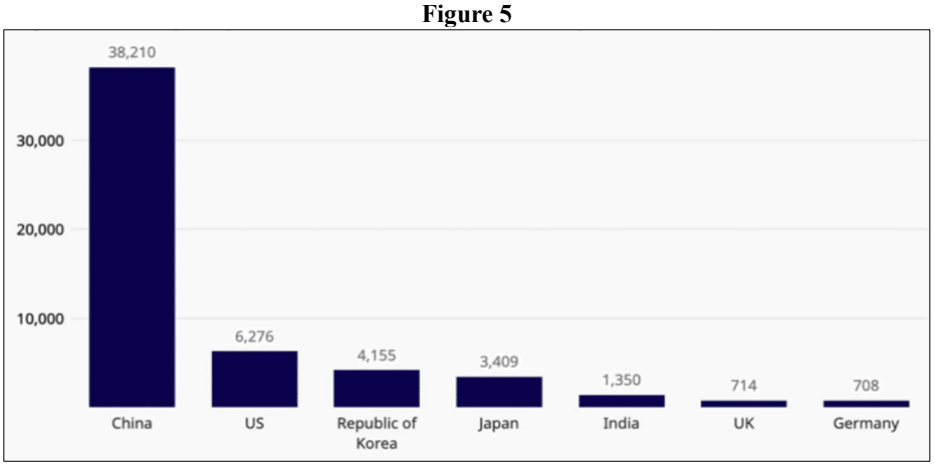
3.2 CHINA

China's AI strategy is primarily guided by two key documents: the New Generation Artificial Intelligence Development Plan (AIDP) released in July 2017 and the Made in China 2025 initiative. Under the umbrella of these policies, the Chinese government has significantly bolstered its AI sector through substantial investments. In 2023 alone, authorities pledged between $40 billion and $50 billion toward AI development. Additionally, over 2,000 state–backed "guidance funds" are actively investing in AI, steering private investments toward strategically important technologies (The Economist, 2024).

In a further move to enhance technological innovation, China has launched a national venture capital guidance fund with the aim of mobilizing approximately 1 trillion yuan (about $138 billion) from social capital (KPMG, 2025). The fund targets cutting–edge sectors, including AI, and aims to boost China's capabilities in next–generation technologies. These efforts emphasise the importance of AI for enhancing national competitiveness and security. The AIDP outlines goals for achieving world–leading levels in AI technology, aiming to reduce dependence on foreign technologies.

China has established itself as a global leader in artificial intelligence (AI) innovation and patent filings. According to the WIPO China–based inventors are filing the highest number of AI patents worldwide. Between 2014 and 2023, China accounted for more than 38,000 generative AI (GenAI) inventions (figure 5), which is six times more than the second–placed United States. However, American AI patents are cited nearly seven times more often than Chinese patents (13.18 vs 1.90 average citations) (Buntz 2024). So, it seems to be a matter of quantity vs quality.

Figure 5



Source: WIPO

The arrival of DeepSeek-R1 in January 2024 sent shock waves through the US tech industry and stock market. The company claimed to have built its model using a fraction of the computing power used by US rivals. DeepSeek's debut was also a surprise because the US government has continuously sought to limit China's access to the computer chips needed to build the most advanced AI models.

China is progressively introducing a growing number of AI applications into the consumer market, in some cases more rapidly than the United States. This widespread adoption enables the collection of vast amounts of user data and allows companies to refine their models at scale. Combined with the size of the domestic market, this dynamic could strengthen China's position as a commercial power in AI, particularly in consumer–facing technologies.

3.3 EUROPE

If the United States is unquestionably the global leader in AI, both in technological capability and strategic influence, Europe is also progressively asserting its role in this increasingly multipolar AI landscape. Indeed, Europe is nowadays an indisputable player in the field, especially with its role of regulatory pioneer. As the AI Index 2025 report by Stanford's Institute for Human–Centered Artificial Intelligence (HAI) illustrates, Europe promotes responsible, inclusive, and sustainable AI while also scaling up its innovation capacity and national strategies to compete technologically. The European Union has taken a different path from the United States, one rooted in strategic sovereignty, regulatory leadership, and long–term industrial planning. According to the same report, several European countries continue to invest significantly in AI at the national level, with France, Germany, and the United Kingdom consistently appearing in the global top 10 for AI publications and model releases.

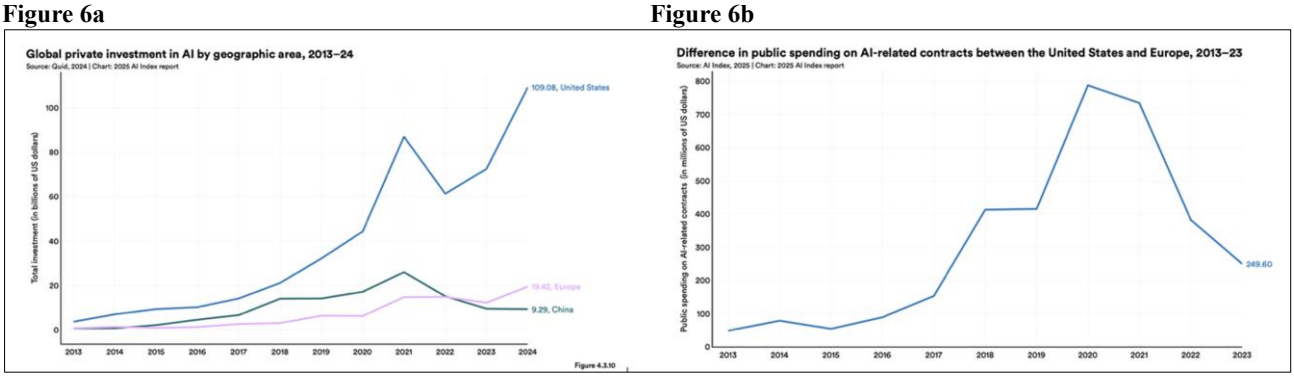
For instance, France has moved from the 13th place in 2023 to the 5th in 2024 in the Global Index and, in 2025, the country has more than 1,000 AI startups, including gems like Mistral AI, H Company or Poolside. In a major announcement at the AI Action Summit in Paris in February 2025, President Emmanuel Macron unveiled an ambitious €109 billion national AI investment plan. This initiative aims to make France a European hub for AI excellence by developing high–performance computing infrastructure (e.g. cloud, supercomputing capacity, essential to training next–generation AI models).

While Europe may not yet rival the United States in terms of private funding or the scale of commercial development, it is steadily building a distinctive approach to AI cantered on three core pillars: responsible governance, excellence in research, and sovereign innovation. According to the Stanford AI Index 2025, Europe is transitioning from a role of regulatory frontrunner to a more balanced model that combines ethical oversight with technological capability.

First, Europe shows strong performance in AI research and academic output. Germany and the United Kingdom rank among the top contributors to AI publications globally. With strong research ecosystems cantered around institutions such as the University of Oxford, ETH Zurich, and the Max Planck Institute. Furthermore, the EU's research programs such as Horizon Europe and the European Laboratory for Learning and Intelligent Systems (ELLIS) also continue to strengthen continental academic cooperation and talent development.

Then, while the gap remains wide in private investment, the trajectory is changing especially with China (figure 6a). In 2024, France, Germany, and the UK each attracted between $2 and $3.6 billion in private AI investment, placing them among the top 10 globally (Figure 3). More importantly, private investments have decreased in China in 2023 (-1,9%) compared to a significant augmentation for Europe in the same period (+60%); not to mention the investment plan launched by France in February 2025, which we have already discussed. Concerning public investment, the difference between the US and EU has narrowed over the past three years with a strong effort from Europe to close the gap which is now of about $250 billion against almost $800 billion three years ago (figure 6b).

Figure 6a **Figure 6b**



Source: Stanford (2025)

Moreover, Europe is the undisputed leader in regulation and ethical AI governance. For instance, in March 2024, the European Parliament adopted the EU AI Act. It is the world's first regulatory framework on AI and emphases on transparency, fundamental rights, human oversight, and risk classification. Furthermore, according to the Stanford AI Index 2025, 17 out of the 36 new AI laws passed globally in 2024 were adopted in European countries. This is evidence that the EU is shaping the regulation framework on AI. Europe's governance-first approach makes it not only a normative power but also a standard-setter in global digital policy.

Finally, in terms of frontier model development, Europe still lags behind the U.S. and China in terms of scale. Most state-of-the-art foundation models continue to be released by U.S.-based companies. However, companies such as France's Mistral or Germany's Aleph Alpha are among the few non-U.S. organisations making significant contributions to open-source model development. For example, Mistral's open-source models have been widely adopted and integrated to improve other models. This ideology, which we could name "openness", reflects a deeper European philosophy around AI innovation that highlights interoperability, academic reproducibility, and digital sovereignty.

In this rapidly evolving technological landscape, a coalition between the United States and Europe is imperative to face other threats especially China but also emerging countries such as India, UAE or Israel. This collaboration should focus on building shared norms around transparency, safety, accountability, and open science to lead to a more democratic AI future.

3.4 INDIA

Under strong government stewardship, India is rapidly emerging as one of the leading global players in the field of artificial intelligence. It ranks third worldwide in the 2024 Stanford AI Index in terms of AI activity volume, behind only the United States and China. This rise is supported by two key strategic assets: on one hand, a massive talent base, with over 4 million IT professionals and an AI talent pool expected to grow from around 600,000-650,000 to more than 1.25 million by 2027 (IndiaAi, 2024); on the other hand, an enormous volume of internal data, fuelled by a population of over 1.4 billion people who are increasingly connected thanks to rapid digitalisation and the expansion of Digital Public Infrastructure (DPI).

This transformation is guided by the visionary framework #AIForAll, a programmatic manifesto launched in 2018 by NITI Aayog, the Indian government's official policy think tank. The initiative promotes an ethical and inclusive AI approach focused on key sectors such as agriculture, healthcare, education, and smart mobility. Building on this vision, the Indian government introduced the National Program on AI**,** also coordinated by NITI Aayog, which laid out the initial strategic roadmap for AI research, talent development, and public sector applications. This foundational strategy has since evolved into the IndiaAI Mission, launched in 2024 by the Ministry of Electronics and IT (MeitY), as the concrete operational arm of India's AI

ambitions. Backed by over $1.2 billion in public investment, the Mission aims to strengthen the national AI ecosystem through support for startups, language-specific AI models, the development of skilled professionals, and the establishment of an AI Safety Center. A flagship of this effort is AIRAWAT, India's public AI supercomputing infrastructure, which was ranked 75th globally in the latest Top500 supercomputer rankings. Underpinning all these efforts is India's robust Digital Public Infrastructure **(**DPI**)** – a suite of open, scalable platforms such as Aadhaar, UPI, DigiLocker, India Stack, and Bhashini – that provides structured, interoperable data and services used to train locally relevant AI systems.

As part of this broader mission, India is also establishing the IndiaAI Innovation Centre, a flagship institution dedicated to developing and deploying indigenous Large Multimodal Models (LMMs) and domain-specific foundational models tailored to critical sectors such as healthcare, agriculture, law, and education. This effort aims to strengthen India's technological sovereignty by creating cutting-edge AI systems that are culturally and linguistically aligned with its population. Complementing this is the forthcoming IndiaAI Datasets Platform, designed to enhance the accessibility, quality, and utility of public sector datasets, thereby enabling data-driven governance and catalysing AI-based research and innovation across both public and private domains. To support the human capital necessary for this ecosystem, the IndiaAI FutureSkills initiative will provide large-scale training and certification programmes in AI, machine learning, data science, and related fields.

India's vast linguistic diversity, with 122 major languages and hundreds of dialects, has become a strategic asset in its national AI agenda. Recognising this potential, the government has launched Bhashini, a Digital Public Infrastructure aimed at providing linguistic data to start-ups and developers for building AI tools in vernacular languages – an enormous yet largely untapped market. In parallel, the government-backed AI4Bharat initiative has developed open-source language models such as IndicBART and IndicBERT.

The private sector has developed its own vernacular AI models: Sarvam AI launched OpenHathi, the first Hindi LLM based on Meta's architecture. CoRover.ai, in partnership with Bhashini, released BharatGPT, supporting over a dozen Indian languages. Tech Mahindra plans to launch Indus, an open-source LLM focused on Hindi dialects, while Zoho has announced a suite of generative AI features and future domain-specific models built atop ChatGPT (Kak and West 2024). These efforts are bolstered by India's globally influential legacy IT industry, including giants like Tata, Infosys, Wipro, Zoho, Fractal Analytics, and Sarvam AI itself. These firms are not only integrating AI into enterprise solutions at scale – developing platforms such as TCS's ignio, Infosys's Topaz, and Wipro Holmes – but are also increasingly engaged in building proprietary and open AI tools for global markets.

Despite an ambitious policy framework and a mature IT services ecosystem, India's role in the global AI landscape remains peripheral when it comes to foundational research and frontier model development. India's AI ecosystem is notably robust on the domestic front – particularly in vernacular AI and data-driven governance – but its global footprint in steering the direction of AI innovation remains marginal. Even emerging start-ups like Sarvam AI, while promising, still build upon core architectures developed by Western tech giants such as Meta and Microsoft.

Finally, India has also positioned itself as a promoter for trustworthy, inclusive, and human-centric AI on the global stage. Through international forums and its domestic initiatives, it emphasises the need for ethical AI. Framing itself as an "AI garage for the Global South", India aspires to become a hub for developing scalable, low-cost, and context-sensitive AI solutions that can be adapted across other emerging economies.

3.5 SAUDI ARABIA AND THE UAE

Saudi Arabia and the UAE are each making significant investments to diversify their economies and contribute to the region's broader technological acceleration.

The UAE has launched a $10 billion AI VC fund, more than eight times the total funding received to date by Mistral, for example. Notably, the UAE was also the first country in the world to appoint a Minister of State for Artificial Intelligence, establishing the position in 2017 as part of a national push to lead globally in AI governance and innovation. This ambition is further reflected in the UAE National Strategy for Artificial Intelligence 2031, which sets out a bold vision to position the country as a global leader in AI by 2031. The strategy aims to leverage AI as a transformative force across economic, educational, and governmental sectors, with the objective of generating AED 335 billion (approximately $91 billion) in economic growth (CSIS, 2025).

Saudi Arabia, meanwhile, plans to invest $40 billion in AI development, on top of a recently announced plan to invest $100 billion in data center expansion (Project Transcendence) and its earlier $100 billion tech fund. Saudi Arabia's Aramco has produced what is reportedly the largest industrial GenAI model in the world, and the Saudi Data and AI Authority released the leading Arabic LLM family, ALLaM, the largest versions of which are built on the basis of Meta's Llama-2. Two of the Emirati Technology Innovation Institute's Falcon models continue to be counted among the world's top LLMs, and the UAE's G42 has developed a high-performing Arabic model family, Jais, which speaks to the ability of developers in the region to access a robust corpus of Arabic data for model development.

Finally, Saudi Arabia and the UAE have sustained the AI talent pipeline needed to foster a self-sustaining model-development ecosystem. For all the impressive growth in this regard, with roughly 7,000 and 5,000 AI specialists now residing in the UAE and Saudi Arabia, respectively, the Gulf's talent pool remains small compared to countries such as Germany (55,000 AI specialists) or France (50,000).

4 AI VALUE CHAIN AND GEOPOLITICAL INFLUENCE; FOCUS USA VS CHINA

AI, along with its underlying supply chains and infrastructure, is rapidly becoming a key instrument of geopolitical influence; nations are fiercely competing to secure AI's economic, technological, and strategic advantages, while meaningful cooperation remains distant, and the geopolitical landscape grows increasingly fragmented. Techno-nationalism and digital sovereignty have become the two key concepts driving the strategies of global powers and superpowers. These frameworks reflect a push for full control and strategic exploitation of AI – a dual-use technology with wide-ranging spillover effects – while seeking to safeguard national security and technological autonomy, thus leading to a neo-mercantilist-like approach.

The United States and China, as global superpowers, are the main actors in this competition. The rivalry between these two giants is profoundly reshaping the AI value chain, as well as the development and application of AI technologies – particularly through growing fragmentation and the lack of interoperability between AI systems across geopolitical blocs. Both countries have continuously implemented measures and policies aimed at strengthening their own positions while weakening that of the other. Strategic assets needed to develop AI, like data, cloud infrastructure and chips, have long since been the object of competition between the USA and China, but this dynamic has been exacerbated with the rise of artificial intelligence.

4.1 VALUE CHAIN WEAPONISATION AND DECOUPLING

4.1.1 Chips, Data centers and Critical Materials

Specialised chips (GPUs, ASICs, TPUs) play a critical role in artificial intelligence by providing the computational power required to train and deploy complex models, primarily within high-performance data centers. The strategic importance of advanced semiconductors has fuelled what is often referred to as the "chip war" between the United States and China: the chip industry – and its underlying sub-industries – has become the primary focus of supply chain weaponisation, a trend that was already underway but has been significantly intensified with the rise of artificial intelligence.

In recent years, the United States has imposed severe restrictions on the export of chip technologies to China. As early as 2022, Washington banned the sale to Beijing of the most advanced microchips produced by American companies such as Nvidia – particularly high-end GPUs critical for AI development. These restrictions were further tightened throughout 2022 and 2023, requiring specific licences even to export downgraded versions of AI chips (such as the Nvidia H20, a derivative of the H100) to China. Key non-U.S. companies were also affected. Under pressure from Washington, allied countries such as the Netherlands and Japan introduced export controls on high-end semiconductor manufacturing equipment, effectively preventing China from accessing the tools required to produce advanced chips.

The case of Huawei marked a turning point in the US–China tech rivalry, particularly in the strategic domain of artificial intelligence. In 2019, the United States added Huawei to its Entity List, barring U.S. firms from supplying the company with critical technologies, including AI chips. In 2020, the U.S. Department of Commerce amended the Foreign Direct Product Rule (FDPR), significantly tightening restrictions on Huawei's access to semiconductor technologies. Under the revised rule, any chip or equipment manufactured outside the United States is subject to U.S. export controls if it incorporates American-origin technologies – such as U.S.-developed software or components. This extraterritorial measure impacted key foreign firms: TSMC, a major Taiwanese foundry reliant on U.S. design tools, and ASML, a Dutch manufacturer of advanced lithography systems that integrate U.S. components and software. Both were consequently required to obtain U.S. licences to supply Huawei. As a result, Huawei was effectively cut off from both high-performance chips and the equipment necessary to produce them, severely constraining its capacity to advance in artificial intelligence. In December 2020, SMIC (Semiconductor Manufacturing International Corporation), one of China's largest semiconductor foundries, was also added to the Entity List.

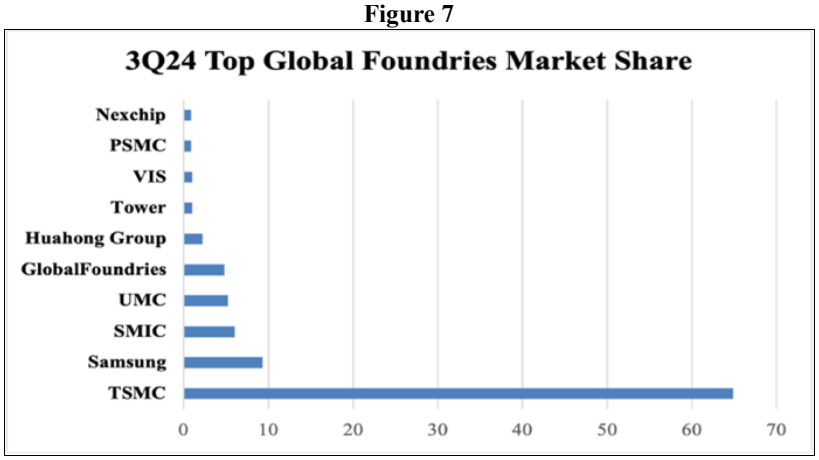
Moreover, starting from 2022, Nvidia and AMD, two U.S. fabless chip designers whose products are the most advanced and widely used to train AI systems in data centers, became the target of continuous and expanding export restrictions. Initially focused on China and Russia, these restrictions were later expanded in 2023 to additional countries including the United Arab Emirates (UAE) and Saudi Arabia, to prevent indirect access.

In this context, Taiwan and South Korea are being increasingly drawn into the US-China clash, as they respectively host the world's first (TSMC, but also UMC) and second (Samsung Foundry) largest semiconductor foundries.

Taiwan represents a crucial geopolitical node, given the persistent threat of Chinese military action – rooted not only in technostrategic interests but also in cultural and political claims under the "One China" principle. Similar concerns apply to South Korea: geopolitical tensions in East Asia – particularly the possibility of a confrontation between China and U.S. allies – could place significant pressure on Seoul. South Korea must balance strategic expectations from the United States while preserving its economic ties with China, the primary market for firms like Samsung and SK Hynix.

Aware of these geopolitical risks, both Taiwan and South Korea have joined multilateral initiatives such as the Chip 4 Alliance (alongside the United States and Japan) to enhance cooperation on semiconductor supply chains, while cautiously avoiding actions that could escalate tensions with Beijing.

Figure 7



Source: Trendforce 2024

In response to U.S. export restrictions, beginning in mid-2023, the Chinese government imposed multiple curbs on the export of certain rare earth elements and critical minerals (such as gallium and germanium) – materials essential to produce AI hardware, including chips and cooling systems for high-performance data centers. China plays a dominant role in the global supply of these resources; the International Energy Agency (2024) estimates that China accounts for about 61% of rare earth production and 92% of their processing.

Because of the chip war, both the United States and China are striving to develop separate, fully controlled semiconductor value chains. What was once a deeply globalised system has been increasingly fragmented due to strategic competition between the two powers.

For example, with the CHIPS and Science Act of 2022, the U.S. government allocated $52 billion in tax credits and subsidies to promote full domestic manufacturing of semiconductors, benefiting both American companies like Intel and foreign firms: TSMC and Samsung are each building fabs in the United States, receiving $6.6 billion and $4.75 billion in government subsidies, respectively. As a result of these initiatives, in 2025, NVIDIA announced the production of a fully U.S.-based AI supercomputer, utilising its Blackwell chips manufactured at TSMC's Arizona facility. NVIDIA's AI supercomputers now serve as the engines of a new generation of data centers, specifically designed for large-scale artificial intelligence processing. In addition, the CHIPS Act allocates $200 billion to support research across several fields; while part of this funding is specifically dedicated to AI initiatives, a significant share indirectly benefits AI development by advancing semiconductor technologies and computing infrastructure critical for training and deploying AI systems. Regarding critical minerals, the United States is pursuing a similar strategy, aiming to reduce global interdependence on China through several initiatives. These include "friendshoring" efforts – such as the creation of the Mineral Security Partnership, a coalition with countries like Australia, Canada, Japan, and several European nations – to secure alternative supply chains, as well as investments to boost domestic production capacity.

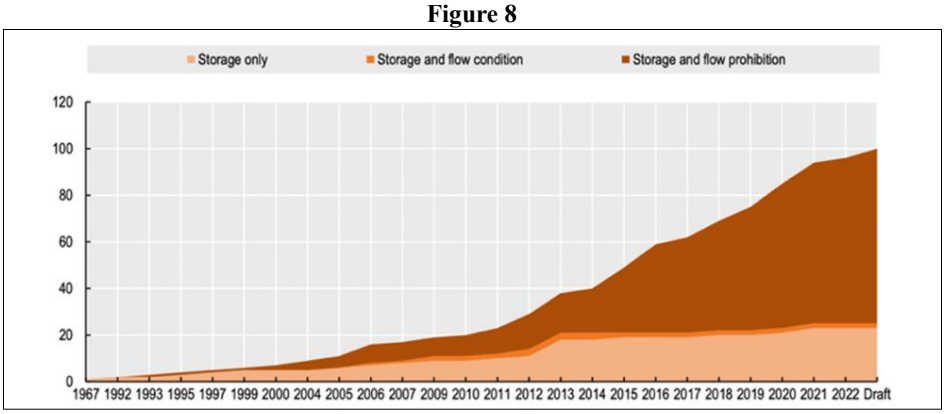
On the other hand, China is aggressively pursuing self-sufficiency across the entire semiconductor value chain to reduce its reliance on foreign technologies. Through its state-backed Big Fund – whose third phase is capitalised at $47.5 billion – China is providing strategic support to national champions such as SMIC and chip designer HiSilicon. The goal is to reduce dependence on Taiwanese foundries and U.S. design firms, also fostering the development of domestic alternatives for critical tools and technologies. Between 2021 and 2022, the Chinese state reportedly spent nearly $300 billion to recreate the chip supply chain at home, helping firms like Huawei and SMIC design an advanced GPU (The Economist, 2024). Furthermore, in pursuit of full self-sufficiency, Beijing is intensifying its efforts in the data center sector, where the United States currently hosts 5,426 facilities compared to China's 449 (Statista, 2024). In 2021, China's Ministry of Industry and Information Technology (MIIT) launched a Three-Year Action Plan to promote the nationwide development of new data centers. In late 2022, AI infrastructure was elevated to a national priority, prompting local governments to accelerate the construction of AI-focused facilities, known as "smart computing centres." By the end of 2024, more than 150 new centres had been completed, supported by state-owned enterprises, public funds, and local initiatives.

4.1.2 Data and Cloud Computing

The AI supply chain decoupling concerns not only hardware but also the digital dimension. The first essential input for the development of AI systems is data, used to train, fine-tune, and operate models. Consequently, controlling access to data and cloud infrastructures has become a strategic priority, with initiatives such as data localisation laws, national cloud policies, and restrictions on cross-border data flows playing a critical role in the fragmentation of the global AI ecosystem.

Starting from initiatives like the Great Firewall of China, aimed at blocking foreign platforms and tightly controlling the flow of information, a fragmented internet – also known as the "splinternet" – has gradually emerged. This fragmentation has been fuelled by a growing number of national policies designed to restrict, channel, and exert sovereignty over data flows (Aaronson, 2024).

Figure 8



Source: OECD (2023)

According to OECD (2023), data localisation measures are evolving in scope and complexity (figure 8) and could have significant implications for international trade and data flows. As of early 2023, there were 100 such measures in place across 40 countries, and over two-thirds of them combined local storage requirements with prohibitions on international data transfers – the most restrictive form of data localisation. A significant shift occurred starting in late 2023, when U.S. trade policymakers began to reverse years of advocacy for the free flow of data, reconsidering their long-standing position on digital trade. For example, in January 2025, the U.S. Department of Justice finalised a regulation that limits the cross-border transfer of sensitive personal data to so-called "countries of concern", such as China.

Creating AI systems that can effectively address a wide range of challenges and serve diverse populations depends heavily on access to global datasets. Therefore, policies enforcing data localisation – by restricting the international flow of data – can significantly weaken the ability to develop AI models that are customised and relevant to specific user groups. These types of restrictions are particularly challenging for smaller or developing nations. While countries like the United States and China benefit from large, digitally connected domestic populations providing a rich data stock, smaller countries often lack this advantage. In addition, artificial intelligence is deeply intertwined with other foundational digital technologies such as cloud computing, big data analytics, and the Internet of Things (IoT). All of these rely on the seamless exchange of information across borders. Therefore, data localisation regimes affect AI not only directly – by limiting data availability – but also indirectly – by destabilising the underlying technological architecture upon which AI innovation relies.

Alongside data, cloud computing plays a vital role in artificial intelligence by providing scalable data storage, high-performance computing for training and inference, and a global infrastructure for deploying AI solutions. This fundamental input is also being weaponised and targeted by decoupling strategies in several countries, particularly by the United States – the clear global leader in cloud service provision – followed at a considerable distance by China. Cloud access restrictions complement chip export controls, as cloud services provide remote access to U.S.-based GPUs – allowing Chinese firms to bypass hardware bans and train advanced AI models.

Figure 9

Cloud Services Leadership by Region

Rank	Worldwide	US	China	Rest of APAC	Europe	Rest of World
Leader	Amazon	Amazon	Alibaba	Amazon	Amazon	Amazon
#2	Microsoft	Microsoft	Tencent	Microsoft	Microsoft	Microsoft
#3	Google	Google	China Telecom	Google	Google	Google
#4	Alibaba	Oracle	Huawei	NTT	Oracle	Salesforce
#5	Oracle	Salesforce	China Unicom	Alibaba	Salesforce	Oracle
#6	Salesforce	IBM	China Mobile	Fujitsu	IBM	IBM

Based on IaaS, PaaS and hosted private cloud revenues in Q2 2024

Source: Synergy Research Group

Consequently, the Biden administration has moved to close regulatory loopholes in its export control regime. This includes proposals by the Department of Commerce that would require U.S.-based cloud providers to implement "know-your-customer" (KYC) frameworks, aimed at identifying and restricting foreign entities – particularly Chinese – from accessing U.S.-based GPUs via the cloud. In parallel, the U.S. government has expanded its Entity List to include Chinese firms such as Inspur Group. As one of China's oldest technology brands, Inspur maintains deep partnerships with Western tech companies, including major hyperscale cloud providers. Moreover, U.S. cloud providers have begun rolling out "sovereign cloud" solutions, such as Microsoft's 2022 offering designed to meet government demands for data localisation and privacy (Lazard, 2023).

In response, China is intensifying its efforts to develop a sovereign and self-sufficient cloud infrastructure. Companies like Alibaba Cloud and Tencent Cloud have received both policy support and state-linked investments.

4.2 AI: GEOPOLITICAL INFLUENCE AND DIGITAL COLONIALISM

AI-driven products and services are actively leveraged or deployed by the United States and China to expand their spheres of control, impose digital colonial structures, and create enduring strategic dependencies across the developing world. Moreover, although strategic inputs such as cloud computing, data centers, and critical AI infrastructure are fiercely guarded within their domestic blocs amid the intensifying US-China technological decoupling and techno-nationalist competition, they are also strategically exported to emerging and developing nations as instruments of influence and dependency-building. Through these targeted deployments, major powers seek to consolidate regional footholds, reshape global digital ecosystems, and extend their geopolitical reach.

Less developed countries, unable to develop internal AI ecosystems, are increasingly compelled to trade access to their population's data and domestic markets in exchange for essential AI services and infrastructures. In doing so, they expose themselves to new forms of digital dependency, effectively transitioning into digital vassal states that sacrifice elements of their economic autonomy and information sovereignty in pursuit of technological advancement.

AI infrastructures and products have become powerful instruments of geopolitical influence across multiple dimensions. On the cultural front, large language models shape linguistic frameworks, ideological narratives, and cognitive environments, enabling major powers to extend their soft power by embedding their values and worldviews into everyday digital interactions. LLMs have thus become another means of cultural hegemony. (Carnegie Endowment for International Peace, 2025)

Simultaneously, AI surveillance systems – particularly those exported by authoritarian regimes such as China – serve as vectors for spreading governance models based on centralised control, facilitating the replication of autocratic practices and consolidating political alignments in recipient countries. Economically and technologically, the export of AI infrastructures such as cloud-based services entrenches long-term dependencies, as countries adopting these technologies cede control over data flows, regulatory standards, and critical digital assets. Through this combination of cultural projection, political influence, and infrastructural entrenchment, AI fuels a new wave of digital colonialism, binding emerging economies into asymmetric technological relationships that reshape the global order in favour of the AI race-leading superpowers.

However, exporting advanced AI technologies presents a fundamental trade-off for leading powers: broad diffusion can expand geopolitical influence and shape global standards, but it also risks empowering competitors and undermining long-term technological dominance. This challenge is particularly acute for the United States, due to their current leadership in AI. In early 2025, Washington responded by introducing the AI Diffusion Framework, a policy designed to regulate the international flow of critical AI technologies. Covering advanced semiconductors, computing resources more broadly, and powerful frontier AI models, the framework aims to balance the global diffusion necessary for maintaining influence with the technological containment essential for preserving U.S. strategic supremacy. The Framework divides the world into three tiers, modulating the diffusion of U.S. AI capabilities according to the strategic alignment of each group.

4.2.1 United States

Beyond the AI Diffusion Framework, the United States' global influence in the AI domain remains strong, driven by the dominant presence of its major technology companies and hyperscalers across both AI products and cloud infrastructure. The U.S. approach is therefore primarily based on its technological and cultural supremacy. The widespread adoption of American large language models – including OpenAI's GPT series, Google's Gemini, and Anthropic's Claude – enables the projection of cultural soft power on an unprecedented scale. By 2023, 61 notable AI models had originated from U.S.-based institutions, further cementing America's leadership in frontier AI development. Moreover, the United States leads the global open-source ecosystem, leveraging platforms such as GitHub and promoting freely accessible AI tools and frameworks. This open-source leadership extends American influence by embedding U.S.-based standards, practices, and values into the foundational layers of emerging digital ecosystems. (Pannier, 2024)

In parallel, the United States exerts strong influence within international standard-setting organisations such as the OECD and the G7, helping to shape the global governance principles for AI. Moreover, the broad diffusion of technical standards developed by U.S. agencies like the National Institute of Standards and Technology (NIST), combined with the massive international adoption of American LLMs, has effectively established de facto U.S. standards at a global level, further amplifying America's geopolitical influence.

Moreover, the United States consolidates its influence through the strategic dominance of AI infrastructures. Major American cloud providers – Amazon Web Services, Microsoft Azure, and Google Cloud – control a substantial majority of the global cloud computing market, providing the computational backbone necessary for AI deployment and scaling. The widespread adoption of U.S.-based cloud infrastructures binds client nations into technical ecosystems controlled by American firms, creating durable dependencies.

4.2.2 China

In the domain of large language models (LLMs), China currently lags several steps behind the United States, as models developed in America dominate global usage. However, through major government-backed initiatives, China has promoted the development of sovereign large language models such as WuDao 2.0, PanGu-α, and Ernie Bot, aiming to build independent capabilities and challenging the cognitive and cultural soft power projected globally by U.S.-origin LLMs. In parallel, China is

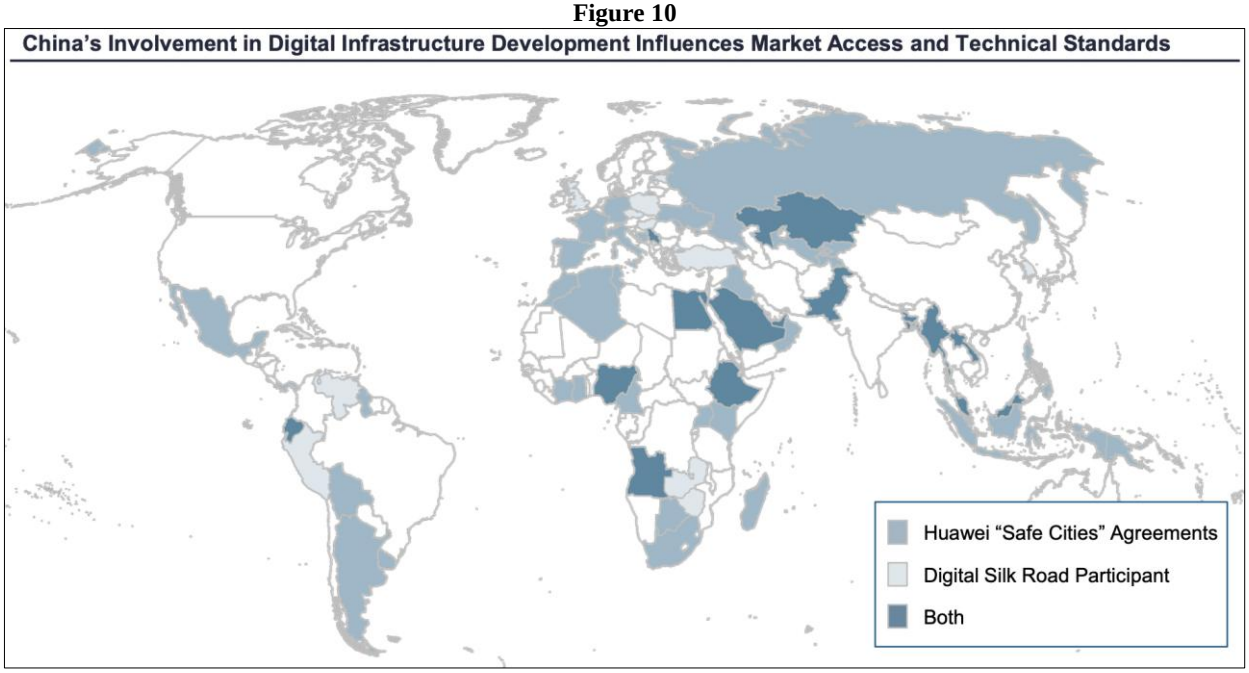
fostering its own open-source ecosystem, with projects like DeepSeek releasing competitive open-source LLMs, and the expansion of platforms such as Gitee, developed as a domestic alternative to GitHub. These efforts reflect Beijing's broader strategy to embed Chinese technological standards, practices, and governance models into the digital infrastructures of emerging economies, positioning itself as a central player in the contest for global AI influence.

Beyond the development of sovereign AI models, China's approach to shaping its geopolitical influence through artificial intelligence is more overtly colonialist compared to that of the United States. The Digital Silk Road (DSR) has emerged as a central pillar of China's broader strategy to expand its geopolitical influence through digital means. The DSR focuses on building critical digital infrastructures – including cloud computing platforms, and AI – across emerging and developing economies. Beijing has concentrated its DSR efforts in regions such as Southeast Asia, sub-Saharan Africa, the Middle East, and Latin America. Through this initiative, China has aggressively expanded the export of AI-powered surveillance technologies as a core instrument of geopolitical influence. Through initiatives such as Huawei's Safe City projects and the international expansion of companies like Hikvision, SenseTime, and CloudWalk, Beijing has equipped dozens of emerging and developing countries with advanced surveillance infrastructures. For example, 59% of Huawei's agreements are concentrated in Asia and sub-Saharan Africa, and 71% are with lower-middle-income and upper-middle-income countries. China is also promoting more advanced integrated systems such as "City Brain" platforms – notably powered by Alibaba Cloud – which combine real-time data from surveillance cameras, IoT devices, and digital transactions to enable predictive monitoring and management of urban activities.

In parallel, Chinese cloud providers such as Alibaba Cloud, Huawei Cloud, and Tencent Cloud are rapidly expanding their global presence. Notable examples include Alibaba Cloud's joint ventures in Saudi Arabia to deliver sovereign cloud services supporting local digital transformation, and Huawei Cloud's deployment of data centers and AI platforms across Southeast Asia and Africa.

These projects do not merely offer technological modernisation; they strategically embed Chinese firms into the digital backbones of client states, creating long-term infrastructural dependencies. By exporting such data-centric governance models and critical infrastructures, Beijing seeks to export and normalise authoritarian practices across emerging economies, reinforcing China's political influence and entrenching a new form of digital authoritarianism. In doing so, China consolidates political alignments, entrenches structural technological dependencies, and gains privileged access to vast amounts of data, further enhancing its informational and geopolitical leverage over recipient countries.

Figure 10



Source: Lazard Geopolitical Advisory (2023)

5 POWERING THE FUTURE: AI, ENERGY & INFRASTRUCTURE

Artificial intelligence is emerging as a key element in optimising energy consumption and managing smart grids. It makes possible the analysis of huge amounts of data from sensors and smart meters, allowing accurate predictions of electricity demand and grid status. AI systems already help utilities balance generation and consumption in real-time, mitigating peak demand and better integrating intermittent renewable sources (wind, solar). The U.S. Department of Energy has highlighted how AI can significantly improve grid planning and operations, increasing resilience and efficiency on the path to a clean economy. In sum, AI acts as the "digital brain" of energy infrastructure, enabling data-driven management that reduces costs and environmental impact while improving the reliability of supply.

Here lies the paradox: while AI can be used to optimise smart grids, forecast renewable energy output, and improve efficiency across sectors – thus reducing environmental impact on a global scale – it simultaneously relies on energy-hungry data centers that consume vast amounts of electricity and water for cooling, making it, in effect, a polluting technology. Indeed, training and running large-scale AI algorithms requires thousands of specialised servers operating 24/7, generating a significant energy footprint. According to a special report by the International Energy Agency (IEA), worldwide data center electricity demand is set to more than double by 2030, reaching about 945 TWh (a value greater than Japan's entire electricity consumption today). AI will be the main driver of this growth, with electricity consumption related to AI workloads alone likely to quadruple over the same period. In the United States, nearly half of the increase in electricity demand between now and 2030 will come from data centers themselves: by the end of the decade, the country will consume more electricity for data processing (cloud, AI, etc.) than for the entire manufacturing of energy-intensive goods (aluminium, steel, cement, chemicals).

This trend has put data centers in the spotlight for their sustainability. On the one hand, large tech companies have pledged to mitigate their impact, for example, with a stated goal of powering their data centers with 100 percent renewable energy. On the other hand, governments are beginning to demand "green" standards. According to the IEA, much of the new data center's electricity needs will be met by renewables but also by natural gas-fired power plants, which could hinder climate goals if no action is taken on offsets and efficiency.

The use of AI in infrastructures also raises security concerns and geopolitical risks, particularly regarding AI-enhanced cyberattacks against critical infrastructure. Power grids, water distribution systems, transportation, and communications have become highly dependent on software and automation; as a result, hostile actors (criminal groups or state sponsors) could exploit AI to plan and launch more effective and targeted attacks. A 2024 report called cyber-attacks on critical infrastructure "the new geopolitical weapon," noting that power grids, oil pipelines, ports, and industrial facilities are increasingly the target of campaigns traceable to foreign powers. Such scenarios are taken very seriously by security agencies: in 2023, the U.S. NSA established an Artificial Intelligence Security Center dedicated to protecting AI systems and studying how AI could be used in attacks on national infrastructure.

The hope is that AI itself can also provide countermeasures (e.g., simulating attacks to test the robustness of systems or automatically isolating portions of the network at the first serious anomaly), but the fact remains that the increase in the digital attack surface amplifies the risks. Ultimately, the reliability of basic infrastructure – energy, water, transportation, communications – is now an integral part of geopolitical confrontation in the digital age: protecting this infrastructure from AI-enhanced attacks has become a national security priority for many governments.

6 BETWEEN HARD AND SHARP POWER: RISKS OF ARTIFICIAL INTELLIGENCE

The application of artificial intelligence in the military domain is accelerating the development of autonomous weapons systems, reaching the point of systems that require no human intervention in the decision-making process – so-called “human-out-of-the-loop” systems. This evolution marks a radical shift in the conduct of warfare, but it also opens the door to highly destabilising scenarios. The opacity of the chain of responsibility, the difficulty of attributing attacks, and the high speed of action of these systems increase the risk of unintended clashes and uncontrolled escalation.

In this context, AI emerges as a fundamentally dual-use technology, with far-reaching implications across the military, security, and intelligence domains. One of its most critical areas of application is Intelligence, Surveillance, and Reconnaissance (ISR), where AI capabilities are rapidly transforming how information is gathered and processed. AI algorithms are being used by intelligence and law enforcement agencies to collect and analyse huge amounts of data. Computer vision systems can scour satellite images in search of military installations or specific vehicles. Nations like China are investing heavily in AI for internal and external surveillance, building ubiquitous systems of cameras, drones, and sensors supplemented by facial recognition, license plate reading, and even predictive behavioural analysis. In parallel, intelligence agencies in the United States (NSA, CIA, NGA, etc.) are using AI to filter the huge flow of information collected to extract only anomalous or relevant signals.

Artificial intelligence represents an unmatched vehicle for the projection of sharp power in the digital age. Since late 2022, with the public dissemination of generative models (ChatGPT for text, tools such as Midjourney for images, advanced speech synthesizers, etc.), we have seen a proliferation of deepfakes, and synthetic content used to deceive the public. In May 2023, an AI-generated fake image of an explosion at the Pentagon sowed panic on social media and caused a brief stock market drop before being debunked. In the same months, deepfakes of various kinds have gone viral online, demonstrating how AI can fuel increasingly convincing disinformation campaigns, with concrete examples in several countries: a wave of election-related deepfakes in Europe and Asia swept through social media in 2023, serving as a wake-up call for more than 50 nations expected at the polls in 2024. In the United States, a political activist revealed that he was hired (in January 2024) to use AI software capable of imitating President Joe Biden's voice and making phone calls to Democratic voters in New Hampshire to dissuade them from voting in the primaries.

Faced with such threats, institutions have begun to react. For example, the Federal Election Commission (FEC) in the U.S. discusses imposing disclosure requirements for AI-generated political content, while the EU (through the Digital Services Act and Code of Conduct on Disinformation) calls on digital platforms to explicitly label synthetic media and to enhance systems for detecting fakes.

7 THE GLOBAL AI GOVERNANCE: INTERNATIONAL REGULATIONS AND TECHNICAL STANDARDS

Given the global nature of AI, the development of an international regulatory framework has become increasingly urgent. Interstate coordination is necessary to avoid legal fragmentation and normative dumping, where countries lower safety or ethical standards to attract greater investments. Thus, in the current geopolitical landscape, growing tensions exist between the need for international cooperation on AI governance and the major powers' drive to compete, each promoting innovation and AI adoption through distinct domestic legal frameworks. The main initiatives to develop global AI governance are as follows.

1. **2024 AI Act**: The European Union is widely recognised as a normative superpower and, as with the GDPR, it plays this role for AI, leveraging the Brussels Effect to compensate for the lack of major tech giants like the USA or China that can set global standards. The AI Act is the first comprehensive AI law in the world and is expected to exert significant extraterritorial influence, shaping AI governance well beyond the EU's borders. It could encourage companies and even third countries to voluntarily align with its provisions to access the European market or to benefit from regulatory certainty. This dynamic is particularly impactful in developing regions, where adopting EU-aligned frameworks may attract investment, enhance trade opportunities, or facilitate technical cooperation. As such, the AI Act functions not only as a legal instrument within the EU, but also as a strategic tool of soft power, exporting European values into the global AI ecosystem.
2. **Council of Europe Framework Convention**: In May 2024, the Council of Europe adopted the Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law, the first binding international treaty establishing clear principles for AI governance, including human dignity, equality, privacy, transparency, accountability, reliability, and safe innovation. The Convention applies to both public and private actors and adopts a risk-based approach, which calibrates requirements based on risk, allowing states to choose between direct obligations or alternative measures to regulate the private sector. Signature and ratification are voluntary, and membership is open not only to Council of Europe states but also to third countries worldwide, reinforcing its global ambition. Implementation will be monitored by a Conference of the Parties to ensure compliance and facilitate international cooperation.
3. **G7 Initiatives**: Within the G7 framework, several initiatives have been launched to address the opportunities and challenges posed by artificial intelligence. Among these, the Hiroshima AI Process Comprehensive Policy Framework, introduced in May 2023, represents a key effort to promote the development of safe, secure, and trustworthy AI, aimed at establishing a set of international rules for an inclusive global governance of AI, with the dual objective of maximising innovation opportunities while mitigating the risks associated with advanced AI systems. It is currently structured around two main instruments: the "Hiroshima Process International Guiding Principles for Organisations Developing Advanced AI Systems," addressed to all relevant actors throughout the AI lifecycle, and the "Hiroshima Process International Code of Conduct for Organisations Developing Advanced AI Systems," specifically targeting AI developers. The Apulia G7 Leaders' Communiqué, adopted in 2024, reaffirms the commitment to advancing a safe, secure, and trustworthy development of artificial intelligence, while promoting a digital transformation that is inclusive, human-centred, and supportive of economic growth and sustainable development. The G7 leaders emphasised that AI should serve as a catalyst for increasing productivity, creating quality employment, and ensuring decent work standards. Moreover, under the 2024 Italian presidency, the G7 promoted the creation of the AI for Sustainable Development Hub, implemented in collaboration with the UNDP. This initiative specifically focuses on leveraging artificial intelligence to advance the United Nations Sustainable Development Goals (SDGs), with particular attention to fostering digital inclusion and sustainable innovation in Africa and other developing regions.
4. **Global Partnership on Artificial Intelligence (GPAI)**: The GPAI is an international initiative dedicated to promoting the responsible, human-centric, and trustworthy development and use of artificial intelligence. First announced at the 2018 G7 Summit by Canadian Prime Minister Justin Trudeau and French President Emmanuel Macron, the partnership was officially launched in 2020 with fifteen founding members. Today, GPAI integrates OECD members through an integrated partnership, bringing together a total of 44 nations across six continents. GPAI operates through a multi-stakeholder approach, engaging governments, industry, academia, and civil society to ensure that its activities are informed by a broad range of perspectives and technical expertise. Its governance structure includes a Council, a Plenary, and a Steering Committee, designed to guarantee inclusive participation and evidence-based decision-making at every level.
5. **OECD**: The OECD AI Principles, initially adopted in 2019 and updated in May 2024, provide a global framework to guide AI actors in the development of trustworthy artificial intelligence and to assist policymakers in designing effective AI policies. These Principles emphasise key values such as inclusive growth, sustainable development, human rights, democratic values, transparency, and security. In addition, the OECD also offers concrete recommendations for policymakers on how to invest in AI research and development, foster inclusive AI ecosystems, shape interoperable governance frameworks, build human capacity, and promote international cooperation. Today, the European Union, the Council of Europe, the United States, and the United Nations and other jurisdictions use the OECD's definition of an AI system and lifecycle below in their legislative and regulatory frameworks and guidance.
6. **G20**: The G20 AI Principles, endorsed in 2019 during the Tsukuba meeting, represent a non-binding political commitment to promote trustworthy, inclusive, and human-centred AI. Inspired by the OECD framework, these principles emphasise transparency, fairness, accountability, and sustainable development, serving as a common reference to guide national policies and foster international cooperation on AI governance.
7. **UN:** The United Nations has launched several initiatives related to AI, both directly and through its specialised agencies. Among these, the UNESCO Recommendation on the Ethics of Artificial Intelligence, adopted in 2021, stands

out as a landmark effort. Applicable to all 194 UNESCO member states, the Recommendation places the protection of human rights and dignity at its core, emphasising fundamental principles such as transparency, fairness, and the necessity of maintaining meaningful human oversight of AI systems. What distinguishes the Recommendation is its comprehensive set of Policy Action Areas, which assist policymakers in translating ethical principles into practical measures.

The UN High-Level Advisory Body on Artificial Intelligence, initially proposed in the 2020 Roadmap for Digital Cooperation, was formally established in October 2023. Its mandate is to conduct analysis and deliver recommendations to guide the international governance of AI. To ensure a globally inclusive approach, the UN Secretary-General convened the Advisory Body for a 12-month term starting from 26 October 2023. The Body comprises 39 leading AI experts from 33 countries, representing diverse sectors and regions.
The Global Digital Compact (GDC) is a comprehensive global framework for digital cooperation and the governance of artificial intelligence. Introduced in the United Nations Secretary-General's "Our Common Agenda," the GDC provides a roadmap for strengthening global digital collaboration and addressing digital divides. On 22 September 2024, during the Summit of the Future in New York, world leaders adopted the "Pact for the Future," which formally incorporates the Global Digital Compact. Among its key objectives, the Compact aims to support the development of interoperable national data governance frameworks, establish an international scientific panel on AI, promote a global policy dialogue on AI governance, and foster AI capacity-building partnerships, including the exploration of options for a dedicated Global Fund on AI.

8. **The AI Safety Summit**, held in the United Kingdom in 2023, resulted in the signing of the Bletchley Declaration on AI Safety by 28 countries, marking the first global agreement focused on the safe development and deployment of artificial intelligence. The Declaration recognises the collective need to understand and manage the potential risks associated with advanced AI technologies, ensuring that AI is developed and used safely, responsibly, and for the benefit of the global community. As of today, 29 countries, including the United States, the United Kingdom, China, India, Brazil, Australia, and the European Union, have joined and endorsed the Bletchley Declaration.

Finally, data itself – the fuel of AI and the digital economy – is at the centre of intense geopolitical and regulatory competition. The ability to collect and exploit massive amounts of information (big data) is now seen as a source of national power, to the point where data is now considered a strategic resource of the 21st century. Countries and regional blocs increasingly claim data sovereignty – that is, control over how their citizens' data is stored, processed, and transferred across borders.

The European Union, a pioneer in regulation with the GDPR, has laboriously negotiated with the United States to ensure adequate protections when European personal data are stored on U.S. soil. In July 2023, the EU Commission launched a new EU-US pact for data flows (EU-US Data Privacy Framework) aimed at ending the legal uncertainty that followed the cancellation of the previous Safe Harbor and Privacy Shield agreements. Meanwhile, other jurisdictions are taking even stronger paths on data control: China, for example, has enacted data security and privacy laws that require companies (including foreign ones) to store sensitive data on local servers and provide it to the government upon request, while blocking the unauthorised flow of information abroad.

The 2023-2025 biennium will likely be remembered as the period in which data emerged explicitly as a geopolitical battleground, with AI acting as the catalyst: indeed, the quality and quantity of data available to a nation will directly influence its ability to train the most advanced AI and thus to compete technologically. In short, in the age of AI, data is a primary productive factor.

Beyond the efforts to regulate and govern AI globally through ethical guidelines and legal frameworks, significant attention is also being directed towards the development of technical standards, aimed at bridging gaps between policy principles and practical implementation.

The International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) are the two leading global bodies responsible for developing international standards across a wide range of industries and technologies. In the context of AI, ISO and IEC work together, primarily through the Joint Technical Committee 1, Subcommittee 42 (ISO/IEC JTC 1/SC 42), to develop International Standards that address critical areas such as privacy, bias mitigation, transparency, accountability, and risk management. These standards are crucial for ensuring the interoperability and compatibility of AI systems, making it possible for different technologies to work together and exchange data efficiently across borders and industries. This interoperability is vital for building a cohesive and scalable AI ecosystem globally.

Key ISO/IEC Standards for AI are:

- ISO/IEC 42001:2023. *AI Management Systems*: specifies requirements for establishing, implementing, maintaining, and continually improving an Artificial Intelligence Management System (AIMS) within organisations. It is designed for entities providing or utilizing AI-based products or services, ensuring responsible development and use of AI systems.
- ISO/IEC 23894:2023. *AI Risk Management Guidance*: provides methods for identifying, analyzing, and mitigating risks associated with AI systems, promoting auditable and understandable AI.
- ISO/IEC 23053:2022. *Framework for AI Systems Using Machine Learning*: establishes an Artificial Intelligence (AI) and Machine Learning (ML) framework for describing a generic AI system using ML technology. The framework describes the system components and their functions in the AI ecosystem.

8 CASE STUDIES

8.1 AI SURVEILLANCE AND DEMOCRATIC RISK: THE CASE OF HUAWEI'S SAFE CITY PROJECT IN SERBIA

Introduction

This case study examines the deployment of AI-powered surveillance infrastructure in Serbia to explore how artificial intelligence intersects with geopolitical strategy in non-Western, transitional democracies. Serbia offers a particularly relevant context due to its unique positioning between competing global powers – aspiring to join the European Union while maintaining strong political and technological ties with China. In this environment, AI is not merely a tool for efficiency or modernisation but a strategic instrument with significant geopolitical implications.

China has emerged as a leading exporter of AI surveillance technologies, supplying states with tools for biometric monitoring, facial recognition, and data analytics, often through opaque agreements and with limited regard for democratic safeguards. Such exports are increasingly interpreted as part of a broader effort to project influence, standardise authoritarian-compatible digital infrastructure, and expand China's normative reach through its Digital Silk Road initiative. For countries like Serbia, the adoption of these technologies can deepen asymmetrical dependencies, introduce legal and ethical tensions with Western norms, and complicate their path toward Euro-Atlantic integration.

As recent policy research highlights, the global proliferation of Chinese AI technologies challenges not only individual privacy and civil liberties, but also the sovereignty and strategic alignment of recipient states. In this light, AI infrastructure becomes a geopolitical battleground – one where the choice of technological partner signals deeper political and ideological affiliations in the emerging global order

Background and Context

The deployment of Huawei's Safe City surveillance system in Serbia must be understood within the broader context of the country's strategic positioning between East and West.

While Serbia formally aspires to join the European Union, it has simultaneously cultivated a close political and economic relationship with China. This dual alignment allows Serbia to benefit from EU funding and political legitimacy, while also receiving unconditional Chinese investment and support, particularly in the area of digital infrastructure.

Cooperation between the two countries on internal security began in 2009 and deepened in 2017 with the signing of a strategic partnership agreement under China's Digital Silk Road initiative. This agreement led to the launch of the Safe City project, involving the installation of thousands of AI-enabled surveillance cameras across Belgrade, equipped with facial recognition, behavioral analysis, and license plate tracking capabilities.

The project unfolds in a domestic political environment characterised by growing authoritarian tendencies. Since 2019, Serbia has been rated as "partly free" by Freedom House due to declining media freedom, blurred lines between state and party, and weakening institutional checks.

In such a context, the introduction of mass surveillance technologies raises serious concerns about their potential use not only for public security, but also for political control and the suppression of dissent.

Domestic Implications and Democratic Risk

The implementation of Huawei's Safe City surveillance system in Serbia has raised serious concerns about democratic governance, data protection, and human rights. Although officially justified as a tool for improving public safety, the project has proceeded in a legal and institutional vacuum, raising alarm among civil society organisations, legal experts, and international observers.

Since 2019, when the Serbian Ministry of Interior confirmed the acquisition of facial recognition-enabled surveillance cameras from Huawei, the project has advanced with limited transparency. The initial public announcement stated that 1,000 cameras would be installed across Belgrade, yet independent investigations led by the SHARE Foundation estimate that as many as 8,000 cameras may be active, including models capable of real-time facial recognition and behavioral analysis. These cameras were acquired under a 2017 strategic partnership agreement between Serbia and Huawei, signed without public debate or parliamentary scrutiny. The Serbian government has consistently refused to disclose key details such as the location of cameras, technical specifications, data storage practices, or data access rights.

Although Serbian authorities claim that the facial recognition function has not been activated, there are indications that surveillance tools have already been used to monitor political activity. During the 2020 COVID-19 lockdown and the 2021 environmental protests in Belgrade, citizens reported receiving fines despite not being physically stopped or identified by law enforcement, suggesting that video footage and possibly biometric data may have been used to identify participants. In both cases, police denied the use of facial recognition, but failed to provide alternative explanations for how protestors' identities were confirmed.

Legal safeguards around biometric surveillance remain inadequate. The Law on Personal Data Protection, which aligns broadly with the EU's General Data Protection Regulation (GDPR), does not explicitly regulate the processing of biometric data in public spaces. Attempts by the Ministry of Interior to introduce a legal framework have been rejected twice – first in 2021 and again in 2022 – following strong opposition from NGOs, legal experts, and Serbia's Commissioner for Information of Public Importance and Personal Data Protection.
The Commissioner declined the Ministry's Data Protection Impact Assessments (DPIAs) on both occasions, stating that they failed to meet legal standards and lacked the necessary justification for such intrusive measures.

Civil society has played a critical role in resisting the normalisation of mass surveillance. The SHARE Foundation launched the initiative *"Thousand Cameras"* in 2020, an open-source mapping project to document the locations of Huawei surveillance devices across Belgrade. Still, these efforts have largely been ignored by government institutions, and their impact on national policy remains limited.
Public awareness remains low. Surveys suggest that most Serbian citizens either support the use of surveillance technologies as a means of fighting crime or remain unaware of the risks posed by biometric data collection.

This disconnect enables political leaders to present surveillance technologies as signs of progress and modernisation, even as they contribute to the gradual erosion of democratic safeguards and accelerate democratic backsliding.

International Responses

The partnership between Huawei and Serbia, particularly through the implementation of AI-driven surveillance systems under the Safe City project, has sparked significant international concern and geopolitical ramifications. For the United States, Huawei's growing presence in Serbia is viewed as a direct extension of China's global surveillance ambitions and a serious threat to democratic values, cybersecurity, and Western influence in the Balkans. In response, the **Washington Agreement**, signed in September 2020 under U.S. mediation, included a specific clause obligating Serbia to exclude untrusted vendors from its 5G infrastructure, a move clearly aimed at curbing Huawei's influence. Though this clause targeted 5G networks, its implications extended to broader technological cooperation, including surveillance systems. Despite this formal commitment, Serbia has continued expanding Huawei's AI surveillance infrastructure, revealing the limited enforceability of the agreement and Belgrade's ongoing strategic balancing act between East and West.

The European Union has also reacted critically, especially given Serbia's status as an EU candidate country. EU officials and parliamentarians have raised alarms over the lack of transparency in the Huawei deal and its potential to erode democratic standards. Several reports have warned that outsourcing core surveillance capabilities to a Chinese tech company risks compromising data privacy, human rights, and rule of law in Serbia. The project has even been described by some EU figures as effectively "outsourcing policing functions to Beijing", further complicating Serbia's EU accession path. Brussels is also concerned that Serbia's deepening technological ties with China contradict its obligations to gradually align with EU norms on data protection and democratic governance.

Conclusion

The growing integration of AI-powered surveillance infrastructure in Serbia is part of a broader global phenomenon: the export of Chinese digital technologies to both democratic and illiberal states under the guise of urban efficiency and security. As Belgrade becomes one of the first European capitals to embed Chinese-made facial recognition systems into its public spaces, the city also becomes a symbolic front in the geopolitical contest between liberal democracies and digital authoritarianism. The risks posed by such systems are not theoretical. Experts warn of potential state overreach, mass surveillance without oversight, and the risk of foreign interference through embedded software vulnerabilities.
These concerns show that decisions about AI infrastructure are not just technical; they carry political significance, as they influence both how cities operate, and which values underpin their development.

8.2 THE DEEPSEEK EFFECT: SHOCKING THE WORLD, RESHAPING THE RULES

Introduction

In January 2025, the Chinese startup DeepSeek unveiled its language model R1, which achieved performance levels comparable to OpenAI's GPT-4, but at a development cost of approximately $5.6 million only a fraction of the estimated $100 million to $1 billion typically required for similar models in the United States. This accomplishment sent shockwaves through the tech industry, challenging Western dominance in the field of artificial intelligence.

Founded in 2023 by Liang Wenfeng, a former executive at the High-Flyer hedge fund, DeepSeek quickly established itself as a key player in the field of artificial intelligence by adopting an open-source strategy that stands in stark contrast to the proprietary models favoured by many Western companies. Its rapid rise reflects deeper shifts in the global technological landscape. DeepSeek's ability to compete with long-established industry leaders calls into question the longstanding dominance of the United States in AI development and points to a broader redistribution of innovation capacity across new centers of influence. At the same time, the increasing availability of high-Performing, low-cost models raises serious concerns about digital infrastructure security and data protection. A growing divide is also emerging between regulatory models: liberal democracies continue to emphasise transparency and privacy, while authoritarian regimes place greater emphasis on control and performance.

This case study examines the implications of DeepSeek's success for democratic nations, focusing on challenges related to AI regulation, the effectiveness of export control regimes, and the direction of industrial strategy. It advocates for a coordinated and adaptive response that strikes a balance between openness and resilience, technological leadership and normative alignment.

Context and Technological Profile of DeepSeek

Artificial intelligence has become a critical strategic issue, extending beyond innovation to serve as a vector of power and legitimacy. DeepSeek's high-profile entry into this domain demonstrates how algorithmic efficiency can surpass hardware superiority, enabling new players to challenge established leaders.
DeepSeek's R1 model, launched in January 2025, is based on an innovative Mixture-of-Experts (MoE) architecture, combined with advanced tokenisation techniques. This approach allows for the dynamic activation of specialised model subsets depending on the task, thereby optimizing both resource usage and performance. With 671 billion parameters of which only 37 billion are activated per token R1 achieves remarkable efficiency (source: Kamau, I. (2025, January 23). *A simple guide to Deepseek R1: Architecture, training, local deployment, and hardware requirements*. Medium). In parallel, DeepSeek has developed the DeepSeek-Coder series, a suite of open-source code generation models trained on a dataset of 2 trillion tokens, consisting of 87% code and 13% natural language in both English and Chinese. These models, available in various sizes (ranging from 1 to 33 billion parameters), are designed for code completion and generation tasks at the project scale.

Regulatory Responses in Europe and Australia

A – GDPR Precedent in Italy
In January 2025, the Italian Data Protection Authority (Garante) banned DeepSeek, citing violations of the General Data Protection Regulation (GDPR), including a lack of transparency regarding data collection and inadequate purpose limitation. Although DeepSeek denied operating in Italy, investigations revealed that data from Italian users had been collected.
Despite DeepSeek's claims that its services were not available in Italy, the Garante found that the web version of the application was accessible to Italian users, thereby triggering the applicability of the GDPR.
This marked the first exclusion of a foreign AI provider under the GDPR, prompting similar investigations in France, Belgium, and Ireland.

B – Australian Ban on National Security Grounds
In February 2025, Australia banned DeepSeek across all federal networks including electoral and meteorological systems on grounds of national security, citing risks related to data exfiltration, algorithmic opacity, and links to state entities.
This reflects a convergence between European data protection regulation and Australian national security measures, revealing an emerging consensus among liberal democracies: AI is a dual-use technology that requires anticipatory governance.

Export Controls and Semiconductor Strategy

DeepSeek's success calls into question the effectiveness of current export restrictions:
Performance thresholds: Despite controls aimed at restricting the export of high-performance chips, DeepSeek achieved results comparable to leading Western models using Nvidia H800 chips designed specifically for the Chinese market in compliance with U.S. export restrictions. Although less powerful than the H100, the H800 enabled DeepSeek to develop its R1 model with remarkable efficiency, demonstrating that algorithmic optimisation can offset hardware limitations.
Training-focused controls: Existing regulations primarily target the training phase of AI models, overlooking the deployment phase, which is becoming increasingly resource-intensive. DeepSeek has optimised this phase by designing more efficient models, thereby reducing its dependence on costly and restricted hardware infrastructure.
Supply chain leakages: Investigations have revealed that DeepSeek may have acquired restricted chips via third-party countries, notably Singapore. Servers potentially containing Nvidia chips were shipped to China, effectively bypassing export restrictions. Three individuals, including a Chinese national, have been indicted in Singapore in connection with this case.
Think tanks such as RAND are calling for a revision of export control regimes to account for the growing significance of software-driven innovation.

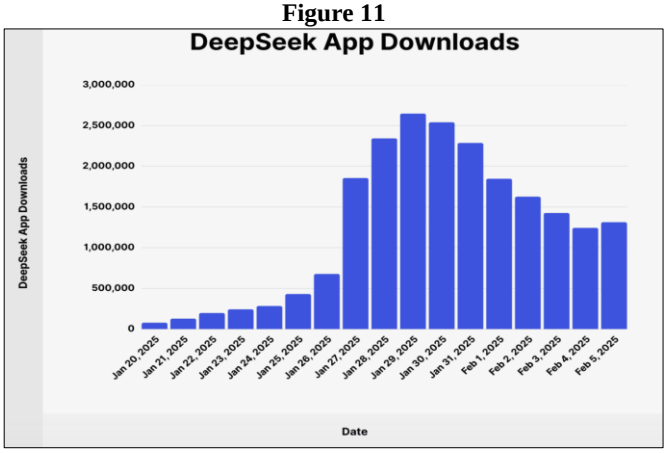
Impact on Global AI Governance

A – Fragmentation of Technological Standards
The meteoric rise of DeepSeek highlights a growing fracture in international standards for the governance of artificial intelligence. On one side, the European Union and its democratic partners rely on principles such as algorithmic transparency, personal data protection (e.g., GDPR), and legal accountability. On the other, China advances a strategy centered on technological performance, rapid dissemination, and state integration absent comparable normative safeguards.

This divergence is not merely theoretical; it is concretely reflected in how AI models are distributed. DeepSeek has opted to release its models under highly permissive open-source licenses (MIT), allowing anyone worldwide to use, modify, or redeploy its systems. This strategic decision stands in stark contrast to the closed models of companies such as OpenAI, Google, or Anthropic, which impose access restrictions due to concerns over security, ethics, or regulatory compliance.
The immediate impact of this open-access approach is evidenced by the surge in downloads of the DeepSeek application.

Between January 20 and January 30, 2025, the number of DeepSeek downloads surged from fewer than 100,000 to nearly 2.7million in a single day just prior to Italy's formal ban on January 30. This trend illustrates the speed at which an uncontrolled AI model can proliferate, made possible by global, rapid, and unrestricted dissemination.

Figure 11



Source: Backlinko (2025)

Analysis of this trajectory highlights two major concerns. First, the absence of pre-emptive regulation at the time of a model's release can lead to massive adoption in unprepared environments, including jurisdictions lacking robust regulatory frameworks. Second, once such a model has been released, national bans tend to come too late to contain its impact. Even after the initial restrictions (Italy, followed by Australia on February 4), daily downloads remained high exceeding 1.5 million per day in early February. This situation perfectly illustrates the challenge of reconciling open innovation with sovereign regulation in a globalised digital space. It also underscores the risk of a regulatory "splinternet," where rival technological blocs impose their own standards without global convergence. DeepSeek thus becomes a symbol of normative fragmentation and a wake-up call for the construction of a coherent international AI governance framework.

B – Shifting R&D Dynamics

DeepSeek's success has prompted major players like Meta and Google to adapt their research and development strategies. Meta launched the LLaMA API to encourage developer integration of its AI models, promoting an open-source approach to foster innovation. Google, meanwhile, introduced multimodal models such as Gemini Pro to match DeepSeek's performance. However, DeepSeek's open-access model raises concerns about the uncontrolled proliferation of AI systems. The ease of access and modifiability increases the risk of malicious use, particularly in regions with weak or non-existent regulatory safeguards. This highlights the pressing need for coordinated global governance to balance technological innovation with security.

Conclusion: DeepSeek as a Geopolitical Catalyst and Strategic Indicator of Global Technological Governance Fractures

The rapid and disruptive emergence of DeepSeek represents far more than a technological breakthrough; it is deeply embedded in a broader geopolitical context where artificial intelligence is becoming both a lever of influence and a cornerstone of digital sovereignty. As a catalyst for strategic realignment, DeepSeek has demonstrated the ability to deliver world-class AI performance with significantly lower resource investments, directly challenging the foundations of Western technological dominance. This development signals a fundamental redistribution of technological power. By minimising dependence on high-end hardware through advanced algorithmic optimisation, DeepSeek enables wider access to cutting-edge AI capabilities across both state and private actors, even in resource-constrained settings. While this may appear to democratise technological leadership, it simultaneously raises the risk of normative fragmentation and increasing regulatory volatility.

The company's choice to open source its models under permissive licenses such as MIT highlights a central tension in contemporary AI governance: the trade-off between fostering innovation through openness and ensuring collective security. In a landscape where AI is increasingly understood as a dual-use technology, existing regulatory structures struggle to keep pace with the speed, scale, and opacity of modern diffusion mechanisms. The open and decentralised nature of these technologies' challenges conventional approaches to accountability, control, and risk mitigation.

At the same time, the DeepSeek case underscores the growing obsolescence of traditional export control instruments, which remain predominantly focused on hardware. As software optimisation, indirect technology transfer, and the fragmentation of global value chains become more prominent, a purely material-based regulatory framework appears insufficient. There is a pressing need to rethink these mechanisms to include more sophisticated oversight of expertise, source code dissemination, and the enforcement of extraterritorial safeguards. Ultimately, DeepSeek embodies a new paradigm – one that tests the capacity of democratic societies to craft a model of AI governance that is both competitive and resilient, while remaining anchored in shared ethical and political values. The challenge today is not only to regulate the use of artificial intelligence but also to actively shape a global digital order capable of responding to its asymmetric, geopolitical, and rapidly evolving nature.

9 POLICY RECOMMENDATIONS

Artificial intelligence is changing the way governments, companies, and people operate, and its development is moving faster than most policy systems can keep up with. Because of this, policy responses need to be flexible, easy to update, and based on clear goals rather than detailed rules that may quickly become outdated. Governments should focus on the results they want to achieve—like fairness, transparency, safety, and respect for human rights—without being too specific on how exactly those results should be reached. This allows space for innovation while still protecting the public. Rules should be based on the level of risk each AI system brings, depending on how and where it is used. For example, the same AI technology might be low-risk when recommending music, but high-risk if used in healthcare or law enforcement. Policymakers should also consider the positive impact AI can have, like improving public services, predicting diseases, or reducing traffic accidents. Ignoring these benefits could lead to missed opportunities, especially in countries that are still developing.

To create safer and fairer AI, it is important to build on existing laws and standards rather than starting from scratch. Many areas where AI is used—like finance, health, or transportation—already have regulations. These can be adjusted to fit the new challenges AI brings. At the same time, governments should create new rules to fill any gaps, especially when existing laws do not address how AI works. Alongside legal rules, soft tools like codes of conduct, ethical guidelines, and certification systems can help companies stay responsible and transparent. All of this should happen in collaboration with the people building and using AI technologies, to make sure the rules are realistic and useful in practice.

Governments should also lead by example. They can use AI to improve their own operations, like detecting tax fraud, predicting economic trends, or evaluating public programs more effectively. But this should be done with care, ensuring data is used responsibly and citizens' rights are respected. AI systems used by public agencies must be clear in how they work, secure, and auditable in case of failure. To achieve this, administrations need strong internal teams of experts who understand AI and its risks. This internal knowledge will help them create better policies and adapt as the technology evolves.

Another important recommendation is to strengthen cooperation across borders. AI is a global issue. What happens in one country can affect many others, especially when it comes to data, trade, or cybersecurity. Countries should work together to create shared standards and to make sure that different national rules do not clash. International principles, like those from the OECD, the G7, or UNESCO, provide a strong starting point. These guidelines focus on human rights, safety, and fairness, and they can help align national approaches. Ensuring interoperability—the ability for rules and practices to work across countries—is especially important for smaller countries that lack the power to shape global standards.

In addition, it is necessary to make sure that AI does not increase inequality between countries or between groups within society. Richer countries and companies often have more data, money, and skilled workers, giving them a major advantage. To reduce this gap, policies should support education, training, and digital infrastructure in places that are currently left behind. There should be public investment in AI tools that solve social problems—like improving farming, healthcare, or education in poorer areas. International bodies like the G20 or the UN could help lead projects that support this kind of inclusive growth.

Another issue is the environmental impact of AI. Large models require huge amounts of energy and water to operate. Policymakers should set clear goals for making AI more sustainable, such as using green energy to power data centers or developing more efficient algorithms. Developers should also be required to share information about how much energy their systems use. This would help create more environmentally responsible innovation and allow governments to compare the impact of different systems.

Finally, to earn the public's trust, AI systems need to be clear, understandable, and open to review. People should know when they are interacting with AI, have access to explanations for AI-driven decisions, and be able to challenge unfair outcomes. Companies and governments alike should be held responsible for how AI systems are used and for any harm they may cause. At the same time, rules about who is legally responsible for problems caused by AI should be carefully written, focusing responsibility on the developers or users that have the most control over the system.

In short, AI can be a powerful tool for good, but only if guided with smart, fair, and flexible rules. The goal should be to support innovation while protecting people and making sure no one is left behind. Governments, companies, and civil society all have a role to play in building a future where AI works for the benefit of all.0

10 CONCLUSIONS

Artificial intelligence has become one of the main battlegrounds for global power, reshaping socioeconomics and geopolitical dynamics. This shift is clearly reflected in the ongoing competition between the United States and China, which acts both as a catalyst for technological innovation and as a tool for strategic dominance. The U.S. continues to lead in cutting-edge technological solutions, while China excels in large-scale digital expansion initiatives. However, Beijing's push for self-sufficiency and domestic technological development has seen considerable success – evident in its recent advancements in chip manufacturing – and is rapidly undermining the United States' advantage. Although middle powers such as some European countries (e.g. France, UK), India and UAE are emerging as influential actors, the AI competition remains largely bipolar.

The strategic relevance of AI is underscored by the intensifying weaponisation of its value chain – from semiconductors to data governance. Coupled with the rise of techno-nationalist policies, this trend has significantly accelerated movements toward digital sovereignty and technological autonomy. The tightening control over strategic bottlenecks in the AI value chain is expected to intensify, further exacerbating geopolitical competition and potentially slowing the pace of AI developments. Moreover, despite the clash over the AI value chain being primarily cantered on the United States-China axis, a wide range of other countries (e.g. Netherlands, Taiwan, South Korea) are directly or indirectly entangled in its implications, highlighting the far-reaching geopolitical impacts of this technology.

Although multiple attempts to build a global governance framework for AI, meaningful international collaboration, crucial for interoperability, fairness, and safety, remains a distant goal in today's polarised environment. Countries worldwide should consider the long-term benefits of a fully integrated global AI ecosystem – for example, the ability to train more accurate and generalizable models through access to diverse and abundant datasets, a goal achievable only in the absence of restrictive barriers to data flows and collaboration, as well as the possibility to build data centers based on energy efficiency and sustainability, such as locating them where they can be powered by renewable sources, without being constrained by geopolitical considerations.

The dual-use nature of AI extends far beyond the traditional divide between civilian applications and military uses. Even within the civilian sphere, a fundamental ambiguity remains: is AI a tool for socioeconomic progress, or a means to project soft and sharp power in the pursuit of global influence? The future of AI – and, more importantly, of the world in the AI era – will be shaped not only by technical breakthroughs, but by the normative frameworks, political choices, and power structures that govern its use. As the cases of DeepSeek and Huawei-Serbia demonstrate, the global AI race is not merely about innovation – it is about values, governance, and the kind of digital world we are collectively building.

REFERENCES

Aaronson, Susan Ariel. 2024. “Data Governance Is Not Ready for AI.” *Centre for International Governance Innovation (CIGI)*.

Aliyev, Nariman. “Artificial Intelligence in Digital Silk Road: Driving Innovation and Economic Transformation.” *Euroasia Journal of Social Sciences and Humanities* 12, no. 1 (February 1, 2025): 95–102. https://doi.org/10.5281/zenodo.15107135.

Associated Press. 2023. “AI-Created Election Disinformation Is Deceiving the World.” *AP News*, June 20, 2023.

Backlinko. 2025. “DeepSeek AI Usage Stats.” *Backlinko*, March 19, 2025.

Bank of England. 2025. *Financial Stability in Focus*.

Baptista, Eduardo. 2024. “Explainer: After China's Mineral Export Ban, How Else Could It Respond to U.S. Chip Curbs?” *Reuters*, December 3, 2024.

Barath Harithas. “The AI Diffusion Framework: Securing U.S. AI Leadership While Preempting Strategic Drift.” Csis.org, 2025. https://www.csis.org/analysis/ai-diffusion-framework-securing-us-ai-leadership-while-preempting-strategic-drift.

Basford Canales, S. 2025. “DeepSeek Banned from Australian Government Devices amid National Security Concerns.” *The Guardian*, February 4, 2025.

BBC. 2025. “Tech Giants Are Putting $500bn into ‘Stargate’ to Build Up AI in US.” *BBC News*, January 22, 2025.

Beroche, H., A. Chubinidze, and L. Goelzer. 2023. *Geopolitics of Smart Cities: Expression of Soft Power and New Order*.

Buntz, Brian. 2024. Quality vs. Quantity: US and China Chart Different Paths in Global AI Patent Race in 2024. *R&D World*. November 3, 2024.

Carnegie Endowment for International Peace. 2025. *The World According to Generative Artificial Intelligence*.

Cdac.in. “AIRAWAT,” 2025. https://airawat.cdac.in/airawat/.

Center for Strategic and International Studies (CSIS). 2025. *The United Arab Emirates’ AI Ambitions*. Washington, DC.

Chatham House. 2024. *Artificial Intelligence and the Challenge for Global Governance: Nine Essays on Achieving Responsible AI*. London: Chatham House.

Clayton, Abené. 2023. “Fake AI-Generated Image of Explosion near Pentagon Spreads on Social Media.” *The Guardian*, May 23, 2023.

El Kadi, Tin Hinane. “Local Agency Is Shaping China’s Digital Footprint in the Gulf.” Carnegie Endowment for International Peace, 2025. https://carnegieendowment.org/posts/2025/01/local-agency-is-shaping-chinas-digital-footprint-in-the-gulf?lang=en.

Elbashir, Mohamed, and Kishore Balaji Desikachari. “India’s Path to AI Autonomy.” Atlantic Council, March 13, 2025. https://www.atlanticcouncil.org/in%E2%80%93depth-research-reports/issue-brief/indias-path-to-ai-autonomy/.

European Central Bank (ECB). 2025. *AI Can Boost Productivity – If Firms Use It*. March 28, 2025.

Financial Times. 2025. “US House Panel Probes Whether DeepSeek Used Restricted Nvidia Chips.” *Financial Times*, April 17, 2025.

Gartner. 2025. “Gartner Predicts 40% of AI Data Breaches Will Arise from Cross-Border GenAI Misuse by 2027.” *Gartner Newsroom*.

Hayashi, Yuka, and John D McKinnon. “Exclusive | U.S. Looks to Restrict China’s Access to Cloud Computing to Protect Advanced Technology.” WSJ. The Wall Street Journal, July 4, 2023. https://www.wsj.com/tech/cybersecurity/u-s-looks-to-restrict-chinas-access-to-cloud-computing-to-protect-advanced-technology-f771613.

Hermann, K. 2024. *Strategic Partnership of the Republic of Serbia and the People's Republic of China: The Political and Economic Implications of Cooperation from Serbia's Perspective*.

Hillman, Jonathan E., and Maesea McCalpin. "Watching Huawei's 'Safe Cities.'" Csis.org, 2019. https://www.csis.org/analysis/watching-huaweis-safe-cities.

HIMSS. 2025. "DeepSeek Blocked in Italy Due to Privacy Risks – Setting a Significant Precedent." *HIMSS Newsroom*.

INDIAai. 2024. "India's AI Talent Pool to Grow to 1.25 million by 2027: NASSCOM-Deloitte India Report." *IndiaAI*, March 4, 2024.

INDIAai. "The National AI Portal of India" n.d. https://indiaai.gov.in.

Institute, P. S. 2020. *The Sum of All Fears – Chinese AI Surveillance in Serbia*.

International Energy Agency (IEA). 2024. *Global Critical Minerals Outlook 2024*. Paris: IEA.

International Energy Agency (IEA). 2025. "AI Is Set to Drive Surging Electricity Demand from Data centers While Offering the Potential to Transform How the Energy Sector Works." *IEA*, April 10, 2025.

International Monetary Fund. "AI Preparedness Index (AIPI)" www.imf.org, 2023. https://www.imf.org/external/datamapper/datasets/AIPI.

Kak, Amba, and Sarah Myers West, eds. 2024. *AI Nationalism(s): Global Industrial Policy Approaches to AI*. *AI Now Institute*, March 2024.

Kamau, I. 2025. "A Simple Guide to Deepseek R1: Architecture, Training, Local Deployment, and Hardware Requirements." *Medium*, January 23, 2025.

Knight, Will. "The AI Race Has Gotten Crowded—and China Is Closing in on the US." WIRED, April 7, 2025. https://www.wired.com/story/stanford-study-global-artificial-intelligence-index/.

KnowBe4. 2024. *Global Infrastructure Report 2024*.

Kowalski, B. 2021. "What's Next for Huawei's Safe City Project in Belgrade?" *Balkan Insight*

KPMG. 2025. *Venture Pulse Q1 2025: China Highlights*. April 2025.

Kynge, J., V. Hopkins, H. Warrell, and K. Hille. 2021. "Exporting Chinese Surveillance: The Security Risks of 'Smart Cities'." *Financial Times*.

Ladevac, I. 2024. *Serbia and China: From Strategic Partnership to the Community with a Shared Future*.

Lang, Nikolaus, Leonid Zhukov, David Zuluaga Martínez, Marc Gilbert, Meenal Pore, and Etienne Cavin. "How CEOs Can Navigate the New Geopolitics of GenAI." BCG Global, December 9, 2024. https://www.bcg.com/publications/2024/how-ceos-navigate-new-geopolitics-of-genai.

Larsen, Benjamin Cedric . "The Geopolitics of AI and the Rise of Digital Sovereignty." Brookings, December 8, 2022. https://www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/.

Lazard Geopolitical Advisory. 2023. *Geopolitics of Artificial Intelligence*. October 2023.

Mann, M. 2020. *Geopolitics, Jurisdiction and Surveillance*.

Manning, Robert A. 2020. *Will Data & AI Cripple or Leapfrog Developing Nations' Growth?* Washington, DC: Atlantic Council GeoTech Center.

Martens, Bertin. 2025. *How DeepSeek Has Changed Artificial Intelligence and What It Means for Europe*. Bruegel, March 20, 2025.

McKinsey & Company. 2023. *The Economic Potential of Generative AI: The Next Productivity Frontier*. New York: McKinsey & Company.

Meltzer, Joshua. "The Impact of Artificial Intelligence on International Trade." Brookings, December 13, 2018. https://www.brookings.edu/articles/the-impact-of-artificial-intelligence-on-international-trade/.

Mitrović, D. 2023. *The Dynamics of the Republic of Serbia's Cooperation with China via the Belt and Road Initiative and the "Sixteen plus One" Platform*.

OECD (Organisation for Economic Co-operation and Development). 2023. *The Nature, Evolution and Potential Implications of Data Localisation Measures*. OECD Trade Policy Papers, No. 278. Paris: OECD Publishing.

OECD (Organisation for Economic Co-operation and Development). 2024. *The Impact of Artificial Intelligence on Productivity, Distribution and Growth: Key Mechanisms, Initial Evidence and Policy Challenges*. OECD Artificial Intelligence Papers, No. 15. Paris: OECD Publishing.

Packin, N. G. 2025. "A Deep-See on DeepSeek: How Italy's Ban Might Shape AI Oversight." *Forbes*, January 31, 2025.

Pan, R., and K. Verhage. 2025. "DeepSeek Shows the US and EU the Costs of Failing to Govern AI." *Atlantic Council*, April 1, 2025.

Pannier, Alice. 2022. *Software Power: The Economic and Geopolitical Implications of Open Source Software*. Études de l'IFRI. Paris: Institut français des relations internationales (IFRI).

Peterson, D., and S. Hoffman. 2022. *Geopolitical Implications of AI and Digital Surveillance Adoption*. Brookings.

Potkin, Fanny, and Liam Mo. 2025. "Exclusive: Nvidia Kept Some China Customers in the Dark about New US Chip Clampdown, Sources Say." *Reuters*, April 16, 2025.

PwC. 2017. *Sizing the Prize: What's the Real Value of AI for Your Business and How Can You Capitalize?* London: PwC.

Reuters. 2023. "China Export Curbs Choke Off Shipments of Gallium, Germanium for Second Month." *Reuters*, October 20, 2023.

Reuters. 2023. "EU Seals New US Data Transfer Pact, but Challenge Likely." *Reuters*, July 10, 2023.

Reuters. 2025. "Meta Introduces Llama Application Programming Interface to Attract AI Developers." *Reuters*, April 30, 2025.

Reuters. 2025. "Singapore Prosecutors Say US Server Fraud Case Involves $390 Million." *Reuters*, March 13, 2025.

Schneier, Bruce. 2023. "NSA AI Security Center." *Schneier on Security*, October 2, 2023.

Siegmann, Charlotte, and Markus Anderljung. 2022. *The Brussels Effect and Artificial Intelligence: How EU Regulation Will Impact the Global AI Market*. Oxford: Centre for the Governance of AI.

Smart Energy International. 2024. "AI Can Significantly Improve Grid Management, Reports DOE." *Smart Energy International*, May 3, 2024.

Spigarelli, Francesca, and Gianluca Sampaolo. "Lo Stato Del Conflitto Tecnologico Tra Cina E Stati Uniti." ISPI, January 15, 2024. https://www.ispionline.it/it/pubblicazione/lo-stato-del-conflitto-tecnologico-tra-cina-e-stati-uniti-163524.

Stanford Institute for Human-Centered Artificial Intelligence. 2024. *AI Index Report 2024*. Stanford University.

Stanford Institute for Human-Centered Artificial Intelligence. 2025. *AI Index Report 2025*. Stanford University.

Statista. 2024. *Number of Data Centers Worldwide as of January 2024, by Country*.

Sterling, Toby. 2023. "Dutch Curb Chip Equipment Exports, Drawing Chinese Ire." *Reuters*, June 30, 2023.

Synergy Research Group. “Cloud Is a Global Market - apart from China | Synergy Research Group.” Srgresearch.com, 2024. https://www.srgresearch.com/articles/cloud-is-a-global-market-apart-from-china.

The Economist. 2023. “Taiwan’s Dominance of the Chip Industry Makes It More Important.” *The Economist*, March 6, 2023.

The Economist. 2024. “Welcome to the Era of AI Nationalism.” *The Economist*, January 1, 2024.

TrendForce. “Press Center - Advanced Processes and Chinese Policies Drive 3Q24 Global Top 10 Foundry Revenue to Record Highs, Says TrendForce | TrendForce - Market Research, Price Trend of DRAM, NAND Flash, LEDs, TFT-LCD and Green Energy, PV.” TrendForce, 2024. https://www.trendforce.com/presscenter/news/20241205-12398.html.

Weber, V. 2023. *China’s Smart Cities and the Future of Geopolitics*. The London School of Economics and Political Science.

Weber, Valentin. “Data-Centric Authoritarianism: How China’s Development of Frontier Technologies Could Globalize Repression” National Endowment for Democracy, February 11, 2025. https://www.ned.org/data-centric-authoritarianism-how-chinas-development-of-frontier-technologies-could-globalize-repression-2/.

White, Joe, and Serena Cesareo. “The Global AI Index.” Tortoise Media, 2024. https://www.tortoisemedia.com/data/global-ai.

World Intellectual Property Organization. “Patent Landscape Report - Generative Artificial Intelligence (GenAI) - 2 Global Patenting and Research in GenAI.” Patent Landscape Report - Generative Artificial Intelligence (GenAI), 2024. https://www.wipo.int/web-publications/patent-landscape-report-generative-artificial-intelligence-genai/en/2-global-patenting-and-research-in-genai.html.