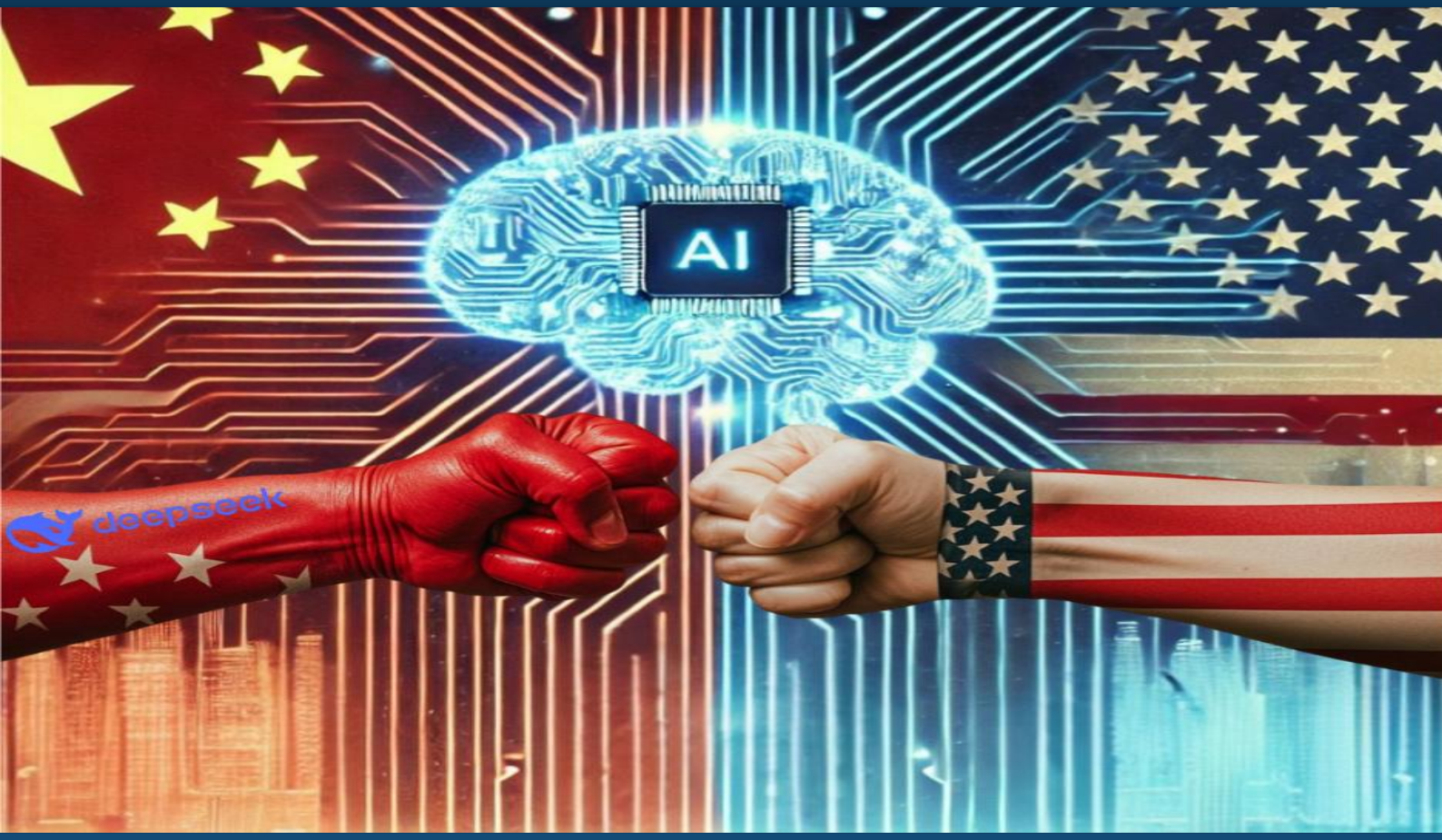
ΙΝΣΤΙΤΟΥΤΟ ΜΕΛΕΤΩΝ
ΠΟΛΙΤΙΚΗΣ και ΔΗΜΟΚΡΑΤΙΑΣ



Battle of Giants in Artificial Intelligence:

The Geopolitical Chessboard of DeepSeek

Dr.Eleni Kapsokoli

Opinion Article

February 2025
No.3

INSTITYTE OF STUDIES FOR POLITICS AND DEMOCRACY

Address: Andrea Zakou 2, Office 301, 2404 Engomi, Nicosia, Cyprus

Telephone: +357 22 664470 ■ Email: info@ispd.org.cy ■ www.ispd.org.cy

Dr. Eleni Kapsokoli

Research Fellow

About the Author

Eleni Kapsokoli is a Post-doctoral candidate at the Department of International and European Studies at the University of Piraeus. She earned her Ph.D. from the same department, focusing on cyberterrorism. She holds a degree in Political Science and Public Administration from the National and Kapodistrian University of Athens and a master's degree in International Relations and Strategic Studies from Panteion University of Social and Political Sciences. Her main research interests include International Relations, International Security, Strategy, Terrorism, Cyberspace, American and European Governance, and Digital Democracy. She has published and participated in conferences and research programs related to these fields. She is also a graduate of the European Doctoral School on Common Security and Defence Policy. Additionally, she is a researcher at the Information and Cybersecurity Laboratory of the Department of International & European Studies at the University of Piraeus, the Foreign Affairs Institute, and the Institute for National and International Security in Serbia. Regarding her teaching experience, she is a lecturer at the Police Academy - National Security School, specializing in cyberterrorism and cybersecurity. She also teaches at the Department of History, International Relations & Political Science at Webster University, Athens Campus, focusing on American politics. Furthermore, she is an accredited Lecturer at the Mediterranean College and the University of Derby, specializing in cybersecurity and data protection.

Battle of Giants in Artificial Intelligence:

The Geopolitical Chessboard of DeepSeek

Introduction

Artificial Intelligence (AI) is one of the most defining technological factors of our time, significantly impacting all areas of human activity. It has brought about radical changes in social structures. In recent years, AI has been at the center of public, academic, and political discussions, often regarded as a 'revolution' due to its exceptional capabilities and the rapid increase in its user base. Major technology companies act as independent actors, controlling computing power, big data, and human resources in the market.

The geopolitical dimension of AI is shaped by the competition between states, such as the United States (US) and China, for economic, political, and military dominance, as well as for influence over global technological standards and norms.

While the US relies on private tech giants and top research institutions, China invests in state-led initiatives and exploits data in order to gain a competitive edge.

The above-mentioned countries follow opposing strategic approaches in AI development. While the US relies on private tech giants and top research institutions, China invests in state-led initiatives and exploits data in order to gain a competitive edge. Both nations are engaged in an 'AI race', raising concerns about global stability. At the same time, a new chapter in geopolitical competition appears to be unfolding with the emergence of the Chinese AI company DeepSeek, which is striving to position itself among the industry's most established competitors.

This article examines the geopolitical competition in the field of AI, focusing on the power struggle between the US and China. It further analyzes the rise of the new Chinese model, DeepSeek, and its impact on the global market while highlighting the digital security challenges of our era. The discussion concludes with an overview of government and private sector responses to these developments.

The Geopolitical Competition in the Field of Artificial Intelligence

The geopolitical dimension of Artificial Intelligence (AI) is inextricably linked to the strategic moves of states seeking to dominate technological development. The US is focusing on disconnecting its technological ecosystem from that of China, implementing strict policies restricting exports, financial flows, and technology transfers to Chinese AI companies.

At the center of technological supremacy is Silicon Valley, home to the largest technology companies such as OpenAI, Google, Meta, and Anthropic, which operate globally and collaborate with various foreign governments. The US holds a clear advantage in computing power, which strengthens the development of advanced semiconductor technology and cloud computing programs.

In particular, NVIDIA stands out as a leading semiconductor designer, offering a strategic advantage to the American AI industry. The Trump administration abolished certain previous policies and assigned officials the task of developing an AI action plan within six months to ensure that systems are 'free from ideological bias or manufactured social agendas'. The US President also established the Presidential Council of Advisors on Science and Technology (PCAST), a 24-member group that will guide U.S. leadership in AI and other emerging technologies. Additionally, he proposed the "Stargate" project, a $500 billion AI consortium in collaboration with OpenAI, Oracle, and SoftBank to build data centers in Texas. This initiative is also expected to involve Microsoft, ARM, Meta, and Nvidia[1]. These companies have established their dominance through extremely costly training processes and computational power. OpenAI and Anthropic have invested over $100 billion in training a single AI model. On the contrary, Meta's training costs for 2025 are projected at $65 billion, while Microsoft's investment is expected to reach $80 billion[2].

On the other hand, China has made significant investments in strengthening its digital autonomy, emphasizing the development of its AI industry and national critical infrastructure. Since 2017, AI has been one of China's national strategic priorities under the 'New Generation Artificial Intelligence Development Plan' and the 'Made in China 2025' initiative[3]. Between 2022 and 2023, China managed to attract $95 billion in private

[1] Li, C. (6 February 2025). 'DeepSeek shakes up AI sector – and other digital tech stories you need to know'. *World Economic Forum.* https://www.weforum.org/stories/2025/02/china-deepseek-shakes-up-ai-tech-stories/

[2] Streets, M. (20 February 2025). 'Stargate AI explained: What's in the $500 billion project'. *TechTarget.* https://www.techtarget.com/whatis/feature/Stargate-AI-explained-Whats-in-the-project

[3] China Embassy. (2017). *'Next Generation Artificial Intelligence Development Plan'.* http://fi.china-embassy.gov.cn/eng/kxjs/201710/P020210628714286134479.pdf

investments, while the semiconductor fund 'Circuit Industry Investment Fund' (Big Fund III) allocated $47 billion for AI product manufacturing[4]. Despite challenges such as dependency on Western technological equipment, China is making substantial progress. Companies like the Semiconductor Manufacturing International Corporation (SMIC) have developed a new semiconductor (7nm), while continuing to plan the production of new proprietary technologies[5].

OpenAI suspended ByteDance, the Chinese owner of TikTok, from accessing its platform in December 2023 over similar allegations. These claims were further reinforced by a statement from the Beijing Academy of Artificial Intelligence in March 2024, confirming that several Chinese companies have successfully developed software and applications based on OpenAI's models.

As of January 2024, China had approved over 40 AI models for public use, all domestically developed, aiming for strict control and local storage of big data. Companies such as Baidu, Huawei, and iFlytek continue to develop their 'fully proprietary' AI models. However, Chinese companies have faced accusations of developing software and applications based on American AI models. For example, in November 2023, the Chinese AI unicorn 01.AI—founded by former Google executive Lee Kai-fu—was accused of using technology similar to Meta's Llama in its Yi-34B model. Similarly, OpenAI suspended ByteDance, the Chinese owner of TikTok, from accessing its platform in December 2023 over similar allegations. These claims were further reinforced by a statement from the Beijing Academy of Artificial Intelligence in March 2024, confirming that several Chinese companies have successfully developed software and applications based on OpenAI's models.

The geopolitical competition extends to countries such as the United Kingdom, Russia, Canada, France, Singapore, India, Iran, South Korea, and Israel, which are strengthening their technological autonomy. These nations are implementing development strategies to bridge the technological gap by creating domestic large language models (LLMs), funding national AI companies, establishing research centers, and enhancing their digital infrastructure.

[4] Shilov, A. (8 January 2025). 'China starts Big Fund III spending: $47 billion for ecosystem and fab tools'. *Tom's Hardware.* https://www.tomshardware.com/tech-industry/china-starts-big-fund-iii-spending-usd47-billion-for-ecosystem-and-fab-tools

[5] He, A. (18 September 2024). 'In the Global AI Chips Race, China Is Playing Catch-Up'. *CIGI.* https://www.cigionline.org/articles/in-the-global-ai-chips-race-china-is-playing-catch-up/

The EU aims to establish itself as a global regulatory authority for AI and other emerging technologies, influencing other nations to adopt similar regulations and policies—a phenomenon known as the 'Brussels Effect'.

Meanwhile, other countries, including Taiwan, South Korea, the Netherlands, and Japan, play a critical role in the global semiconductor supply chain, which is the 'central pillar' of modern technological and economic development. Investments in this sector are primarily driven by the US ($53 billion), China ($48 billion), South Korea ($19 billion), and the European Union ($100 billion) to boost their production capabilities[6].

French President Emmanuel Macron has emphasized the political significance of AI, stressing that this technology concerns sovereignty and strategic dependency. The European Union (EU), while not matching the scale of American tech giants, is focusing on responsible AI governance aligned with its democratic values. The EU aims to establish itself as a global regulatory authority for AI and other emerging technologies, influencing other nations to adopt similar regulations and policies—a phenomenon known as the 'Brussels Effect'. The 'AI Act' is one of the most ambitious attempts to govern AI, though critics argue that the rapid evolution of technology could outpace it before its implementation in 2026. Additionally, the EU has announced the 'AI Innovation Package' and 'InvestAI' to strengthen a resilient digital ecosystem. Concerns over 'digital dependency' on American AI technologies may intensify, reigniting discussions on 'digital sovereignty and autonomy'

From the perspectives of Washington and Beijing, the fear that the opposing power might gain an AI advantage outweighs any theoretical risks that this technology may pose to their societies.

The fundamental issue that arises is the risks associated with the uncontrolled development and use of AI. The lack of trust between major powers accelerates AI development rather than encouraging careful assessment and mitigation of its negative consequences. From the perspectives of Washington and Beijing, the fear that the

[6] Allan, L. (7 October 2024). 'Government Chip Funding Spreads Globally'. Semiconductor Engineering. https://semiengineering.com/global-government-investments-for-semiconductors/

opposing power might gain an AI advantage outweighs any theoretical risks that this technology may pose to their societies.

DeepSeek: Its Role in the Evolution of Artificial Intelligence

The year 2025 began with the release of advanced open-source models, 'DeepSeek-V3' and 'DeepSeek-R1', from the Chinese AI company DeepSeek, founded in 2023 by Liang Wenfeng. These models are highly efficient and cost-effective, which caused concern in Silicon Valley, disrupting market dynamics. Despite ongoing efforts to restrict semiconductor exports from the US to China, DeepSeek managed to develop its models without significant obstacles.

On the other hand, DeepSeek-R1 focuses on applications similar to OpenAI's, offering free access to users. Its creators have given it a distinct advantage: the model provides more detailed and nuanced answers, while allowing for more complex inquiries.

DeepSeek-V3 boasts 671 billion parameters and impressive performance, requiring approximately 95% fewer resources compared to its competitors, OpenAI's ChatGPT 4 and Claude 3.5[7]. While previous AI models operated with 32-bit precision - meaning each number was stored with excessive detail, often unnecessary - DeepSeek challenged this practice by reducing precision to 8-bit. This seemingly simple modification reduces computational load by 75% without noticeably affecting performance, highlighting the power of optimization over brute-force scaling. As a result, the DeepSeek-V3 requires less than $6 million in computational power from Nvidia H800 chips, which coincided with a 17% drop in Nvidia's stock value[8].

On the other hand, DeepSeek-R1 focuses on applications similar to OpenAI's, offering free access to users. Its creators have given it a distinct advantage: the model provides more detailed and nuanced answers, while allowing for more complex inquiries. Interacting with this chatbot gives the sense that the model is more analytical and thoughtful, offering a deeper and more comprehensive experience for the user. Since its release, DeepSeek-R1 has reached over 10 million downloads and became the most popular free app in the U.S. and the UK Apple App Store. Its success is attributed to its ability to deliver

[7] DeepSeek. https://www.deepseek.com/

[8] Rinnovabili. (29 January 2025). *'How energy-efficient is DeepSeek, China's AI disruptor?'*. https://www.rinnovabili.net/business/markets/deepseeks-energy-consumption-ais-75-power-cut/

results comparable to its competitors at significantly lower costs. For instance, ChatGPT attracted 1 million users within the first five days of its release.

Last but not least, the company offers a range of distilled models, DeepSeek-R1-Distill, based on popular open-source programs such as Llama and Qwen. These models offer different levels of performance and efficiency, tailored to various computational demands and hardware configurations. With its ability to deliver high-quality results at lower costs, DeepSeek has already captured the attention of the global technology community and set new strategic goals for future AI advancements.

Unlike other companies that keep their models proprietary, DeepSeek's decision to publicly release its innovations offers transparency and allows anyone to verify its data. Silicon Valley seemed to be divided into two different camps following the release of these new AI models. The first sees this technological advancement as a natural development, despite the challenges it brings. Meanwhile, the second questions the team's identity, the model's performance, the reliability of its data, and the origin of the chips used for training DeepSeek. Even though this model is open-source and its results are reproduced worldwide, doubts remain[9].

The technological competition was further intensified by ByteDance's announcement of a new AI model aiming to surpass OpenAI's o1[10]. On 29 January 2025, the Chinese company Alibaba unveiled the latest version of the Qwen 2.5 models, claiming superiority over DeepSeek[11]. At the same time, the latter proved that revolutionary AI does not require exorbitant costs, focusing on the efficiency of developing such models and reducing the computational power required for their training compared to other systems.

Security Challenges and Gradual Exclusion of DeepSeek

DeepSeek raises serious concerns regarding the collection, processing, distribution, and storage of data, while simultaneously violating user privacy. Many tech companies, such as Google and Microsoft, store data related to browsing history, which may be provided to government agencies upon request. The American company Enkrypt AI published a study, stating that the DeepSeek-R1 has an 11 times higher likelihood of producing harmful content compared to OpenAI's O1.

[9] Reuters. (29 January 2025). 'Microsoft probes if DeepSeek-linked group improperly obtained OpenAI data, Bloomberg News reports'. https://www.reuters.com/technology/microsoft-probing-if-deepseek-linked-group-improperly-obtained-openai-data-2025-01-29/

[10] Mo, L. and Goh, B. (22 January 2025). 'TikTok owner ByteDance, DeepSeek lead Chinese push in AI reasoning'. *Reuters.* https://www.reuters.com/technology/artificial-intelligence/tiktok-owner-bytedance-deepseek-lead-chinese-push-ai-reasoning-2025-01-22/

[11] Forbes. (30 January 2025). *'Alibaba Unveils Qwen 2.5: A DeepSeek Rival?'.* https://www.forbes.com/sites/torconstantino/2025/01/29/alibaba-unveils-qwen-25-a-deepseek-rival/

DeepSeek's algorithm is said to apply censorship to sensitive topics related to China. For instance, it claims that Taiwan is an inseparable part of China since ancient times and avoids answering questions about the 1989 Tiananmen Square protests and the Uighurs in the Xinjiang region.

Furthermore, it reports that 83% of bias tests resulted in biased responses, influenced by racial, gender, health, and religious criteria. DeepSeek's algorithm is said to apply censorship to sensitive topics related to China. For instance, it claims that Taiwan is an inseparable part of China since ancient times and avoids answering questions about the 1989 Tiananmen Square protests and the Uighurs in the Xinjiang region. In this way, the program redirects the discussion to other topics far from politically sensitive issues[12].

A study by the American cybersecurity company, Wiz, states that DeepSeek-R1 bypasses security protocols in 45% of relevant tests, allowing it to provide instructions for terrorist actions and the construction and supply of weapons, as well as create extremist propaganda. It also reports that 78% of cybersecurity tests demonstrated that this chatbot could be deceived, leading to the creation of insecure or malicious code. Finally, they found that an exposed database of the platform left sensitive information and chat histories exposed on the internet [13]. Wiz reported that DeepSeek secured the data after being notified about it.

DeepSeek's privacy policy states that users' data is stored 'on secure servers' in China and are used to comply with legal obligations, serve the public interest, and protect users[14] . The company collects all data related to users from text and audio inputs, uploaded files, and comments, as well as chat history to train its corresponding models. However, the national information law of the country requires companies to 'support, assist, and cooperate' with national intelligence agencies, which increases concerns about unchecked access by authorities to user data[15] .

[12] Enkrypt AI. (31 January 2025). *'DeepSeek-R1 AI Model 11x More Likely to Generate Harmful Content, Security Research Finds'.* https://www.enkryptai.com/blog/deepseek-r1-ai-model-11x-more-likely-to-generate-harmful-content-security-research-finds

[13] Nagli, G. (29 January 2025). *'Wiz Research Uncovers Exposed DeepSeek Database Leaking Sensitive Information, Including Chat History'.* https://www.wiz.io/blog/wiz-research-uncovers-exposed-deepseek-database-leak?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axioslogin&stream=top

[14] *DeepSeek Privacy Policy.* (5 December 2024). https://platform.deepseek.com/downloads/DeepSeek%20Privacy%20Policy.html

[15] Network Data Security Management Regulations. (30 September 2024). https://www.gov.cn/zhengce/content/202409/content_6977766.htm

These concerns have led to a 'chain reaction' from governments and organizations, which are examining DeepSeek's privacy controls. Data protection regulatory authorities in Belgium, France, Greece, and Ireland are investigating the company's data management practices, as well as whether its privacy policy complies with GDPR.

These concerns have led to a 'chain reaction' from governments and organizations, which are examining DeepSeek's privacy controls. Data protection regulatory authorities in Belgium, France, Greece, and Ireland are investigating the company's data management practices, as well as whether its privacy policy complies with GDPR. Similarly, the Italian data protection authority, Garante per la protezione dei dati personali, is reviewing the companies Hangzhou DeepSeek Artificial Intelligence and Beijing DeepSeek Artificial Intelligence for potential violations and has requested further clarifications regarding user data management and whether it is stored in China[16] . The app is unavailable on the Apple App Store and Google Play Store in Italy [17], as was the case in 2023 with ChatGPT. The UK government stated that it is up to citizens to decide whether to use the app, while also calling for transparency from AI developers regarding the use of personal data [18]. Nonetheless, other British officials are closely monitoring the situation and have not ruled out taking emergency measures if national security challenges arise.

Chinese legislation concerning personal data was also a significant factor in the case for banning TikTok in the US. Many national security officials have warned that the company provided Beijing with a channel to acquire personal information from American citizens and that it maintains close collaboration with DeepSeek for similar activities

[16] Reuters. (28 January 2025). *'Italy regulator seeks information from DeepSeek on data protection'.* https://www.reuters.com/technology/artificial-intelligence/italy-regulator-seeks-info-deepseek-data-protection-2025-01-28/

[17] Booth R., Krupa J. and Giuffrida A. (29 January 2025). 'DeepSeek blocked from some app stores in Italy amid questions on data use'. *The Guardian.* https://www.theguardian.com/technology/2025/jan/29/deepseek-blocked-some-app-stores-italy-questions-data-use

[18] Department for Science, Innovation & Technology. (31 January 2025). *'Government response on AI cyber security'.* https://www.gov.uk/government/calls-for-evidence/cyber-security-of-ai-a-call-for-views/outcome/government-response-on-the-cyber-security-of-ai

In Taiwan, the Ministry of Digital Affairs has banned the use of DeepSeek's chatbot in government agencies due to the potential threats it could pose to national security [19]. Australia followed a similar approach, banning it on all government devices and information systems due to the 'unacceptable risk' to national security[20] . In South Korea, several ministries and public agencies have blocked access to the platform for security reasons. In February 2025, the National Intelligence Service (NIS) issued an official warning to government agencies, urging them to take proactive measures, as the platform collects 'excessive' personal data. During the same period, the Personal Information Protection Commission (PIPC) reported that users should not enter personal information on the platform to protect their privacy.

Chinese legislation concerning personal data was also a significant factor in the case for banning TikTok in the US. Many national security officials have warned that the company provided Beijing with a channel to acquire personal information from American citizens and that it maintains close collaboration with DeepSeek for similar activities. Senator Josh Hawley introduced a bill in Congress, the 'Decoupling America's Artificial Intelligence Capabilities from China Act', which refers to extensive bans on imports and exports of AI technologies, as well as research, development, and investment in AI between the US and China[21] . Congress, the state of Texas, NASA, and the US Navy have already banned the use of the platform for security and privacy violations. As concerns grow, many countries are taking strict measures to limit or block DeepSeek, intensifying the discussion around security and privacy in the age of AI.

Concluding remarks

DeepSeek marks a technological advancement that could redefine the structure and expansion of AI, making it more accessible to professionals beyond the field of computer science. At the same time, it strengthens the position of startups and smaller tech players, allowing them to compete with established technology giants. Until recently, the prevailing belief was that AI superiority depended on the scale of investments and computing power. However, DeepSeek has challenged this notion, proving that innovation can significantly reduce costs and increase efficiency. This represents a turning point, lowering market entry barriers and creating new opportunities for AI development.

[19] Focus Taiwan. (31 January 2025). 'Taiwan issues DeepSeek AI public sector ban due to security concerns'. https://focustaiwan.tw/politics/202501310008

[20] Gerken, T. (4 February 2025). 'Australia bans DeepSeek on government devices over security risk'. *BBC.* https://www.bbc.com/news/articles/c8d95v0nr1yo

[21] Hawley, J. (29 January 2025). *'Hawley Introduces Legislation to Decouple American AI Development from Communist China'.* https://www.hawley.senate.gov/hawley-introduces-legislation-to-decouple-american-ai-development-from-communist-china/

Striking a balance between innovation and security, as well as ensuring the responsible use of AI, are critical factors for the future. It is technology companies - rather than governments or regulatory authorities - that are steering the course of this revolutionary technology, with significant implications for the global distribution of power.

The global AI dominance race is intensifying, with the US and China leading while other countries strive to keep up. The competition revolves around four key factors: computing power, human capital, big data, and information infrastructure. The US strategy, focused on increased investments in research and innovation, along with stricter control over technology exports, is expected to shape the global balance of power towards China. The geopolitical dimension of AI complicates the establishment of international agreements and regulations, leading to fragmented regulatory approaches at the national level. Striking a balance between innovation and security, as well as ensuring the responsible use of AI, are critical factors for the future. It is technology companies - rather than governments or regulatory authorities - that are steering the course of this revolutionary technology, with significant implications for the global distribution of power.