Security Concerns due to China's DeepSeek Artificial Intelligence Model

DeepSeek, a Chinese company, launched its Artificial Intelligence (AI)-powered large language models—DeepSeek-V3 and DeepSeek-R1 in Dec 2024 and Jan 2025, respectively. The development grabbed a lot of attention due to the models' cheaper developmental costs and efficient performance as compared to the United States' (US) ChatGPT and Meta AI models. It's being claimed that DeepSeek uses 50,000 Nvidia H100 chips. The company's co-founder Liang Wenfang stated in 2022 that DeepSeek will explore artificial general intelligence, which is defined as autonomous systems that surpass humans in most economically valuable tasks.[1]

DeepSeek models has sparked hope for a new wave of innovation in AI because it is currently reliant on huge investments in microchips, datacentres, and new power source, often dominated by the US tech companies.[2] While the rise of AI models is not a threat in itself, the fact that DeepSeek originates from China and its co-founders have often been found to be close to Chinese Communist Party (CCP) raises the concerns regarding the use of DeepSeek by the CCP to pursue its goal of threatening the global order. Thus, it is important to understand the possible ramifications via proliferation of such AI models.

DeepSeek AI Model's Characteristics

DeepSeek utilises a mix of experts' architecture and various engineering efficiencies for algorithmic efficiency and resource optimisation. The first feature—Reasoning—aims to improve reasoning and mathematical capabilities using pure reinforcement learning. The other feature is 'Replication', which provides strong results for complex mathematical reasoning with a long chain-of-thought and self-reflection.[3] This methodology is deliberately different from the hybrid training strategies employed by the US-based AI chatbot models like ChatGPT.[4] AI experts think that DeepSeek may probably be using model distillation based on OpenAI's technology to train its models. However, that's unproven because the final model developed by DeepSeek is public and not its training data.[5]

The US think tanks estimate that while DeepSeek's chatbot models could have been trained on Nvidia H800 chips, its AI app might be running on Huawei-made Ascend 910C chips. Also, DeepSeek is employing researchers and developers from Chinese universities which could signal China's prowess in developing homegrown futuristic tech.[6] DeepSeek is estimated to have utilised 2,048 Nvidia H800 Graphics Processor Units (GPUs) for a total of 2.788 million GPU hours to complete the training stages, which involve pre-training, context extension, and post-training of 671 billion parameters.[7] The US-based Rand corporation has acknowledged DeepSeek's achievements as genuine and significant while dismissing the US' claims of DeepSeek being a copied version of ChatGPT as a mere propaganda.[8]

Security Threats Regarding DeepSeek's AI Models

DeepSeek can be used by malicious actors without restrictions in various ways, for instance, to understand how to launch phishing attacks or fill internet with AI slops, etc. Next concern is regarding the user data synthesis, where sensitive datas like keystroke patterns, Internet Protocol (IP) addresses, and user personal details could be stored in secure servers located in China. Third concern is respecting the ability of DeepSeek to influence thoughts and ideologies of its global users and feed authoritarian narratives on cultural and political topics as it censors/manipulates topics which are sensitive to the CCP. These include the issue of Taiwan or the reality of the Tiananmen square massacre.[9] When asked about the origins of Kimchi in Chinese, which is originally a Korean dish, the response falsely claims its Chinese origins.[10] Concerns over data storage in China led the US lawmakers to pursue a ban of TikTok in the past.[11] DeepSeek could also help in impersonation using deepfakes and for profiling and surveillance campaigns by creating detailed profiles of individuals, corporations, and governments.[12]

DeepSeek can gather service-related, diagnostic, and performance information such as crash reports and performance logs.[13] Feroot Security, a Canadian cybersecurity firm, has discovered a code in DeepSeek's web login page which has connections to China Mobile, a Chinese state-owned company which has direct links to the People's Liberation Army, as per the US Federal Communications Commission. Feroot also found that DeepSeek's login system incorporates fingerprinting techniques, which track a user's devices.[14] DeepSeek can also be used to steal intellectual property from western organisations, as China is a champion in mining datas which run into terabytes.[15] Australia already considers DeepSeek's threat to be similar to Huawei, which was banned in 2018.[16] Studies indicate that DeepSeek-R1 is 11 times more vulnerable to generate harmful and toxic content like chemical, biological, radiological, and nuclear materials and agents outputs compared to its peers. It can bypass safety protocols and generate criminal planning guides, illegal weapons information, and extremist propaganda. In a concerning development, it was found to be producing recruitment blog for terrorist organisations.[17]

While DeepSeek claims to be an open-access platform, it may not be the case. Its training data, fine-tuning methodologies, and parts of architecture remain largely undisclosed.[18] It is also vulnerable to serious data breaches as Wiz, a New York-based cybersecurity firm, uncovered publicly accessible ClickHouse databases that contained over a million log entries like chat histories, backend details, application programming interface secrets, and sensitive operational information with no authentication mechanisms in place. These unprotected databases granted full administrative control over its contents. Attackers with access could have retrieved proprietary data, extracted plaintext passwords, and accessed local files stored on DeepSeek's servers.[19] DeepSeek has also experienced cyberattacks like targeted Distributed Denial-of-Service (DDoS) attacks, which aims to disrupt the flow of traffic.[20]

Apart from threat at micro level, DeepSeek AI models also pose national security threats at the strategic domains. DeepSeek contains undetected backdoor risks/sleeper agents which, when used by specific organisations or in specific contexts, could lead to insertion of vulnerabilities.[21] China has been known to target companies like SpaceX and Blue Origin, on

whom National Aeronautics and Space Administration and Pentagon increasingly rely upon, to steal the US' space technology.[22]

Global Reactions and Restrictions on DeepSeek

While the US evaluates the national security implications from DeepSeek, they are currently focussed on preventing DeepSeek's threat to global market dominance of the US-based AI apps. The US also suspects that IP threat could have played a major role in development of DeepSeek.[23] DeepSeek may also meet similar fate as TikTok, which was not banned by President Donald Trump even though he rallied against TikTok and labelled it as a national security threat during his first term.[24] Irrespective of President Trump's current lack of concern towards DeepSeek, the US Congress has introduced a bipartisan bill to ban it from being used in the US government's devices.[25] The US navy has also instructed its personnel to refrain from downloading, installing, or using DeepSeek model in any capacity.[26]

Based on the above developments, the US' allies and partners have started banning DeepSeek. Australia has restricted the use of DeepSeek from all government devices and termed it as an unacceptable risk to the government technology.[27] Italy's data protection authority blocked DeepSeek while also initiating an investigation against it.[28] Taiwan's Ministry of Digital Affairs also banned workers in the public sector and at key infrastructure facilities from using DeepSeek.[29] Similarly, South Korea has also restricted the access of DeepSeek on government devices over concerns of user data collection.[30] Many countries like Belgium, Ireland, France, and others are planning to investigate DeepSeek's user data management policies.[31] Several organisations have also started blocking access to DeepSeek.[32]

China, on the other hand, has reacted sharply to the above developments. China's Foreign Ministry has slammed the overstretching of the concept of national security to politicise trade and technology.[33] The country's military has termed the US Navy's ban on DeepSeek as security paranoia. China's ambassador to the UN has requested the US for cooperation on AI and technology, citing mutual benefits.[34] Similarly, China condemned Taiwan's decision to ban DeepSeek and labelled Taiwan's ruling party as anti-China while calling their decision unreasonable and absurd.[35]

Conclusion

Looking at DeepSeek's probable threats, India's Finance Ministry has also banned the use of DeepSeek.[36] This should also be a wake-up call for Indian technology sector that India can't afford to fall behind the US or China in AI-related development. While India is currently developing its own AI model, its dependency on advanced chips and processors is still unknown, whereas China utilised many US-made GPUs for initial development of their AI models. India still lacks considerable research in the AI sector. DeepSeek's debut has rekindled global fears that the US and other western nations will tighten their export control policies for high-end AI chips. India currently is not in a situation to develop its own AI chips fabrication units; however, it is under the process of setting up a unit in near future. President Trump is

already weighing on putting tariffs across the world, including India. If India goes against the US tariffs and retaliates in future, there are chances that President Trump could selectively decide to act against former US President Joe Biden's flagship CHIPS Act to safeguard the country's interests, which can act as a blow to India's efforts to establish itself as a major AI chips and semiconductor manufacturer. Therefore, India needs to realise this reality early and start building partnerships with trusted nations while focussing more on domestic AI research.

Endnotes

---

[1] Eduardo Baptista, 'What Is DeepSeek and Why Is It Disrupting the AI Sector?', *Reuters*, 28 Jan 2025 https://www.reuters.com/technology/artificial-intelligence/what-is-deepseek-why-is-it-disrupting-ai-sector-2025-01-27/

[2] Dan Milmo and Robert Booth, 'Experts Urge Caution over Use of Chinese AI DeepSeek', *The Guardian*, 28 Jan 2025 https://www.theguardian.com/technology/2025/jan/28/experts-urge-caution-over-use-of-chinese-ai-deepseek

[3] Sarah Mercer, Samuel Spillard, and Daniel Martin, 'China's AI Evolution: DeepSeek and National Security', *Centre for Emerging Technology and Security,* 7 Feb 2025 https://cetas.turing.ac.uk/publications/chinas-ai-evolution-deepseek-and-national-security

[4] Patrick Tucker, 'How DeepSeek Changed the Future of AI—and What That Means for National Security', *Defense One*, 29 Jan 2025 https://www.defenseone.com/technology/2025/01/how-deepseek-changed-future-aiand-what-means-national-security/402594/

[5] Lele Sang, 'Unpacking DeepSeek: Distillation, Ethics and National Security', *University of Michigan News*, 31 Jan 2025 https://news.umich.edu/unpacking-deepseek-distillation-ethics-and-national-security/

[6] Jessie Yin, 'Is DeepSeek a Proof of Concept?', *Atlantic Council*, 29 Jan 2025 https://www.atlanticcouncil.org/blogs/econographics/sinographs/is-deepseek-a-proof-of-concept/

[7] Charles Mok, 'Taking Stock of the DeepSeek Shock', *Cyber Policy Center*, Freeman Spogli Institute for International Studies, Stanford University, 5 Feb 2025 https://cyber.fsi.stanford.edu/publication/taking-stock-deepseek-shock

[8] Lennart Heim, 'The Rise of DeepSeek: What the Headlines Miss', *RAND Corporation*, 28 Jan 2025 https://www.rand.org/pubs/commentary/2025/01/the-rise-of-deepseek-what-the-headlines-miss.html

[9] Andrew R Chow, 'Why DeepSeek Is Sparking Debates over National Security, just like TikTok', *Time Magazine*, 29 Jan 2025 https://time.com/7210875/deepseek-national-security-threat-tiktok/

[10] Jonathan Easton, 'South Korean Intelligence Agency Warns of Security Risks in China's DeepSeek', *National Technology News*, 10 Feb 2025 https://nationaltechnology.co.uk/South_Korean_Intelligence_Agency_Warns_Of_Security_Risks_In_Chinas_DeepSeek.php

[11] Thomas Barrabi, 'DeepSeek AI Collects, Stores US User Data in China – Sparking Eerily Similar National Security Concerns That Forced TikTok Crackdown', *New York Post*, 28 Jan 2025 https://nypost.com/2025/01/28/business/deepseek-app-stores-user-data-in-china-sparking-us-security-concerns-experts/

[12] Stu Sjouwerman, 'Six Ways Threat Actors Will Weaponize DeepSeek', *SC Media*, 31 Jan 2025 https://www.scworld.com/perspective/six-ways-threat-actors-will-weaponize-deepseek

[13] Emmet Lyons, 'DeepSeek AI Raises National Security Concerns, U.S. Officials Say', *CBS News*, 29 Jan 2025 https://www.cbsnews.com/news/deepseek-ai-raises-national-security-concerns-trump/

[14] Govind Choudhary, 'Is DeepSeek a National Security Threat? New Research Highlights Ties with Chinese Telecom Raising Data Security Concerns', *The Mint*, 5 Feb 2025 https://www.livemint.com/ai/artificial-intelligence/is-deepseek-a-national-security-threat-new-research-highlights-ties-with-chinese-telecom-raising-data-security-concerns-11738760340568.html

[15] Alexei Alexis, 'DeepSeek Surge Hits Companies, Posing Security Risks', *Cybersecurity Dive*, 5 Feb 2025 https://www.cybersecuritydive.com/news/deepseek-companies-security-risks/739308/

[16] Andrew Tillett and Tom Mellroy, 'DeepSeek: National Security Experts Urge Albanese Government to Consider Strict Controls for Deepseek and Chinese-Controlled AI', *Australian Financial Review*, 28 Jan 2025 https://www.afr.com/politics/federal/deepseek-poses-security-risk-like-huawei-and-tiktok-labor-warned-20250128-p5l7ru

[17] Pascale Davies, 'Why DeepSeek's 'Major Security and Safety Gaps' Are Causing Concern', *Euronews*, 31 Jan 2025 https://www.euronews.com/next/2025/01/31/harmful-and-toxic-output-deepseek-has-major-security-and-safety-gaps-study-warns

[18] Alicia García-Herrero and Michal Krystyanczuk, 'The Geopolitics of Artificial Intelligence after DeepSeek', *Bruegel*, 4 Jan 2025 https://www.bruegel.org/first-glance/geopolitics-artificial-intelligence-after-deepseek

[19] Gyana Swain, 'DeepSeek Leaks One Million Sensitive Records in a Major Data Breach', *CSO Online*, 30 Jan 2025 https://www.csoonline.com/article/3813224/deepseek-leaks-one-million-sensitive-records-in-a-major-data-breach.html

[20] Eduard Kovacs, 'DeepSeek Blames Disruption on Cyberattack as Vulnerabilities Emerge', *Security Week*, 28 Jan 2025 https://www.securityweek.com/deepseek-blames-disruption-on-cyberattack-as-vulnerabilities-emerge/

[21] Konstantin F. Pilz and Lennart Heim, 'What DeepSeek Really Changes about AI Competition', *RAND Corporation*, 4 Feb 2025 https://www.rand.org/pubs/commentary/2025/02/what-deepseek-really-changes-about-ai-competition.html

[22] Erin C. Conaton, 'Preventing China's DeepSeek in Space', *Defense News*, 5 Feb 2025 https://www.defensenews.com/opinion/2025/02/05/preventing-chinas-deepseek-in-space/

[23] Andrea Shalal, David Shepardson, and Kanishka Singh, 'White House Evaluates Effect of China AI App DeepSeek on National Security', *Reuters*, 29 Jan 2025 https://www.reuters.com/technology/artificial-intelligence/white-house-evaluates-china-ai-app-deepseeks-affect-national-security-official-2025-01-28/

[24] Philip Elliott, 'Future of DeepSeek, like TikTok, May Come down to Trump's Whims', *Time Magazine*, 28 Jan 2025 https://time.com/7210569/deepseek-ai-trump/

[25] Rob Wile, 'US Lawmakers Move to Ban China's DeepSeek from Government Devices', *NBC News*, 6 Feb 2025 https://www.nbcnews.com/business/business-news/us-lawmakers-move-ban-deepseek-government-devices-chinese-surveillance-rcna190965

[26] Hayden Field, 'US Navy Bans Use of DeepSeek due to 'Security and Ethical Concerns', *CNBC*, 28 Jan 2025 https://www.cnbc.com/2025/01/28/us-navy-restricts-use-of-deepseek-ai-imperative-to-avoid-using.html

[27] Kristy Needham, 'Australia Bans DeepSeek on Government Devices Citing Security Concerns', *Reuters*, 5 Feb 2025 https://www.reuters.com/technology/australia-bans-deepseek-government-devices-citing-security-concerns-2025-02-04/

[28] Sam Clark and Laurens Cerulus, 'Italy Blocks China's DeepSeek over Privacy Concerns', *Politico*, 31 Jan 2025 https://www.politico.eu/article/italy-blocks-chinas-deepseek-over-privacy-concerns/

[29] France 24, 'Taiwan Bans Government Agencies from Using DeepSeek', 1 Feb 2025 https://www.france24.com/en/live-news/20250201-taiwan-bans-government-agencies-from-using-deepseek

[30] Lionel Lim, 'South Korea's Government Is the Latest to Block China's DeepSeek on Official Devices, Following Australia and Taiwan', *Fortune*, 6 Feb 2025 https://fortune.com/asia/2025/02/06/south-korea-blocks-deepseek-government-devices-china-ai-taiwan-australia/

[31] Pascale Davies, 'Which Countries Have Restricted DeepSeek and Why?', *Euronews*, 3 Feb 2025 https://www.euronews.com/next/2025/02/03/deepseek-which-countries-have-restricted-the-chinese-ai-company-or-are-questioning-it

[32] 'DeepSeek's AI Restricted by 'Hundreds' of Companies and Govt Agencies in Days', *The Straits Times*, 31 Jan 2025 https://www.straitstimes.com/business/companies-markets/deepseeks-ai-restricted-by-hundreds-of-companies-in-days

[33] Aamir Latif and Berk Kutay Gokmen, 'China Slams 'Overstretching' National Security amid Ban on DeepSeek in S. Korea, Australia', *Anadolu Ajansi*, 6 Feb 2025 https://www.aa.com.tr/en/asia-pacific/china-slams-overstretching-national-security-amid-ban-on-deepseek-in-skorea-australia/3473425

[34] William Zheng, 'Security Paranoia': China's Military Mouthpiece Says DeepSeek Bans in US Benefit No One', *South China Morning Post*, 4 Feb 2025 https://www.scmp.com/news/china-

future-tech/ai/article/3297298/security-paranoia-chinas-military-mouthpiece-says-deepseek-bans-us-benefit-no-one

[35] Xinlu Liang, 'Beijing Slams Taiwan's 'Absurd' DeepSeek Ban, Dismisses Security Fears', *South China Morning Post*, 12 Feb 2025 https://www.scmp.com/news/china/politics/article/3298357/beijing-slams-taiwans-absurd-deepseek-ban-dismisses-security-fears

[36] HT News Desk, 'Which Countries Have Banned DeepSeek AI, the Chinese Answer to ChatGPT?', *Hindustan Times*, 6 Feb 2025 https://www.hindustantimes.com/world-news/which-countries-have-banned-deepseek-ai-the-chinese-answer-to-chatgpt-101738807121584.html

Ajay Kumar Das, Independent Researcher and Analyst of International Affairs and Security Studies.

Article uploaded on 17-02-2025