Issue Brief

August 2025
No : 457

NVIDIA's H20 Chips & China: The Backdoor Controversy Truth, Rumour, or Something in Between?

Govind Nelika

NVIDIA's H20 Chips and China: The Backdoor Controversy Truth, Rumour, or Something in Between?

Govind Nelika

Abstract

This paper examines the policy and security implications of the U.S. decision to allow Nvidia's H20 AI chip exports to China after an initial ban. The reversal, following direct engagement between Nvidia and U.S. leadership, reflects the tension between economic interests and strategic risk. China's Cyberspace Administration has raised concerns about potential "backdoors" in the chips, allegations denied by Nvidia. At the same time, U.S. lawmakers are advancing proposals such as the Chip Security Act, which would require export-controlled AI chips to include tracking or deactivation features. These developments underscore the challenges of managing trust in technology supply chains, balancing innovation with national security, and navigating the risks of deeper U.S.–China technological separation.

Keywords: Nvidia H20 chips, U.S.–China, H20 backdoor, Chip Security Act, AI export controls, technology supply chains.

Introduction

In April 2025, the U.S. Department of Commerce blocked the export of Nvidia's H20 AI chips to China, citing national security concerns. That decision was reversed last month, when the Nvidia was granted the license for sale of H20 chips to China. The policy reversal coincided after a meeting (Freifeld, 2025) between Nvidia CEO Jensen Huang and President Trump, suggesting a shift in U.S. policy that balances economic opportunities with strategic risks.

This paper examines the implications of that reversal, especially as China's Cyberspace Administration claims which stated that the H20 chips may contain "backdoors" allowing remote access or shutdown. Nvidia has firmly denied these allegations, saying its products meet strict security standards.

The debate comes at a time when U.S. lawmakers are discussing new rules, such as the proposed Chip Security Act,(Rep. Huizenga, 2025) that could require export-controlled AI chips to include tracking or deactivation features. These measures raise important questions about trust in global technology supply chains, the balance between innovation and security, and the risk of deeper U.S. - China technology separation.

Backdrop

Beijing and Washington have been at odds in recent years, and the introduction of Artificial Intelligence (AI) into the mix has only complicated things further. U.S which predominantly holds monopoly over high end processing chips, imposed a ban on China citing national security, Beijing in response played a similar card, by imposing their own restrictions on rare earth minerals, owing to U.S reliance on Chinas rare earth minerals exports.

Although the situation may appear to be a stalemate, the United States remains heavily dependent on rare earth minerals, which are a critical component of its economy and defence ecosystem. While Washington has invested in $439 million in 2020, to reduce this dependence and increase domestic production, demand remains substantial (Todd, 2024). These minerals are essential in the manufacture of advanced weapons systems. For example, an F-35 fighter jet requires more than 900 pounds of rare earth elements; an Arleigh Burke–class DDG-51 destroyer requires approximately 5,200 pounds; and a Virginia-class submarine consumes around 9,200 pounds.

Forgoing this the current approach of U.S is steadfast as seen by Laura Taylor-Kale, assistant secretary of defence for industrial base policy, remark in 2024 “Resilient supply chains are essential to this goal. The U.S. can no longer afford to rely on overseas, single-points-of-failure for critical components,” Even now the U.S is still reliant on Chinese exports to meet demand.

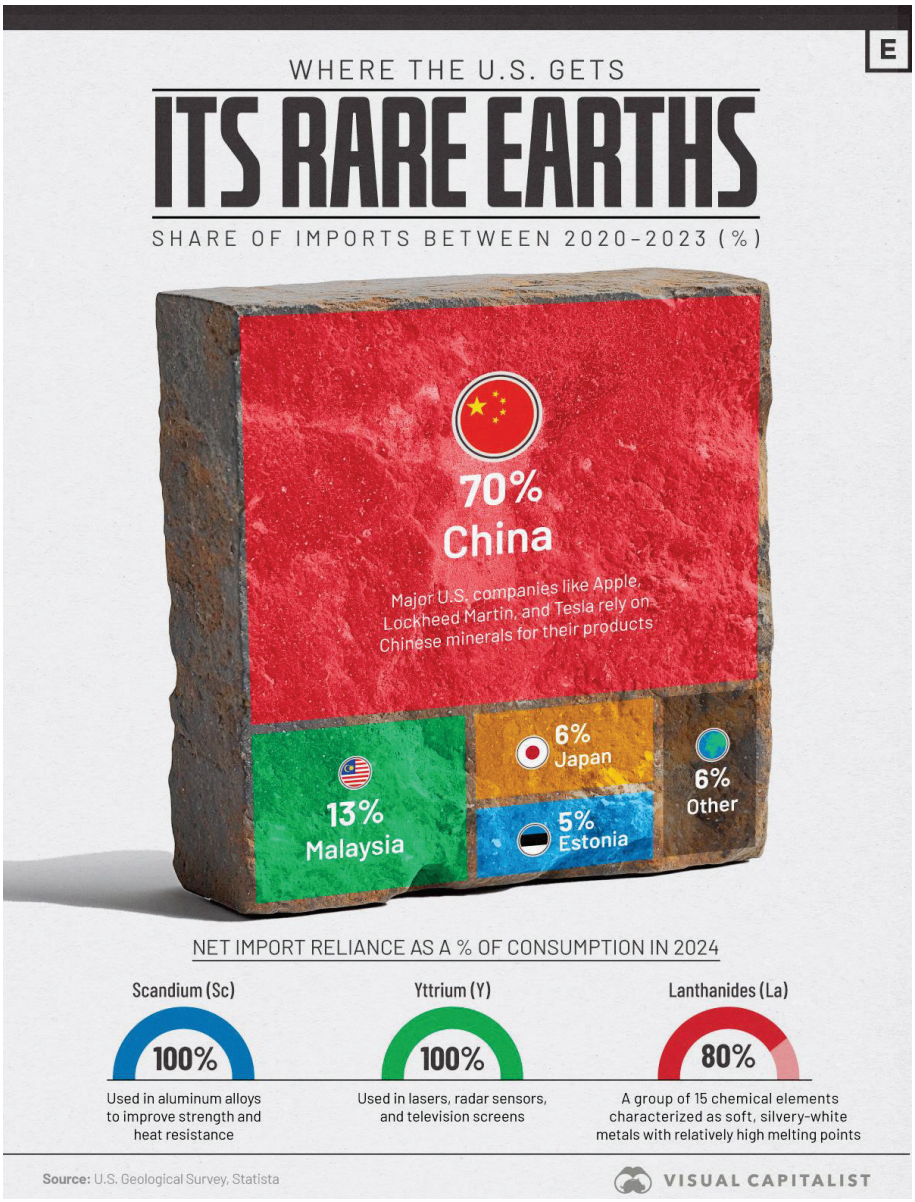

Figure 0.1(Venditti & Parker, 2025)

If one follows the trail of the recent lift of export control of Chips, a mutual deal might as well have gone down between Beijing and Washington, as evidence in June of 2025, when China's MOFCOM Spokesperson He Yadong made the remarks at a press briefing, "We have stressed many times before that rare earth-related items have dual-use attributes, and that imposing export controls on them is in line with international practice," (GT Staff, 2025). He also added in the briefing that China is prepared to strengthen communication and dialogue with relevant countries on export controls. This may well be a hint at China's interest in having a beneficial agreement. Following this the high-level delegations of both countries met in London in Jun 2025, following which Trump made the following statement

"Full magnets, and any necessary rare earths, will be supplied, up front, by China. Likewise, we will provide to China what was agreed to, including Chinese students using our colleges and universities (which has always been good with me!)"(Pfister, 2025).

When probed on China's stance on the matter, to understand whether statement held any water, Chinese Foreign Ministry spokesperson Lin Jian responded that the China-US trade meeting was held under the strategic guidance of the two heads and stressed "China always honor its commitments with concrete actions. Now that a consensus has been reached, both sides should abide by it" (GT, 2025).

Restrictions Lifted on Nvidia Chip Sales to China

While mutual agreement and purported discussions between the United States and China eased tensions over trade restrictions, Nvidia was able to able to get licenses to be approved for sale of H20 chips to China. As the reversal itself was already raising eyebrows among China hawks across the globe, what followed was even more controversial, it started with the Cyberspace Administration of China (CAC) summoning NVIDIA for a meeting regarding security risks associated with backdoors in the H20 computing chip.

Figure 0.2 (CAC, 2025)
(Qwen Model Use for Translation)

The official statement of the the Cyberspace Administration of China (CAC) via their Official Weixin (WeChat) Handle only further raised eyebrows, not to mention the recent the proposed Chips security act, as to what transpired between Nvidia officials and CAC is not well known, however Nvidia later on released an article in their blog specifically titled no backdoor no kill switches spyware, in the article NVIDIA's Chief Security Officer David Reber Jr. addressed concerns and rumours that its GPUs might contain built-in remote shutdown mechanisms, hidden access points, or surveillance features, the following statements in itself in the article explains the stance of Nvidia,

"To mitigate the risk of misuse, some pundits and policymakers propose requiring hardware "kill switches" or built-in controls that can remotely disable GPUs without user knowledge and consent. Some suspect they might already exist.

NVIDIA GPUs do not and should not have kill switches and backdoors."

The article also went on to detail the clipper chip initiative of NSA during 1993, whereby creating such backdoors only allowed malicious threat actors to take advantage of them, and would only result to further security breaches. The article concluded with Nvidia committing itself to never build backdoors, kill switches, or spyware into its chips.

Although this came well after the meeting between Nvidia and Cyberspace Administration of China, a commentary that followed questioned whether Nvidia Chips were safe to use by Chinese consumers, the commentary did not appear on print form but on Official Weixin (WeChat), the images are as under, the Commentary came from the official handles of Peoples Daily

Figure 0.3 (People's Daily China, 2025)
(Qwen Model Use for Translation)

As per the above translation the People's Daily article stresses that cybersecurity is vital to daily life, business continuity, and national security, citing recent global cyber incidents as warnings. It called for strict compliance with Chinese laws and security requirements as a prerequisite for foreign companies operating in China, it called for the company to given convincing assurances as to the supposed backdoor. The post ends with the author stating he is a commentator of the People's Daily and is people are welcome to share their thoughts on the matter. One should note People's Daily is the official newspaper of the Central Committee of the Chinese Communist Party (CCP). It is considered the most authoritative and influential newspaper in China, serving as the official voice of the party and the central government.

Now the approval of the sale and China's question of tampered chips wasn't raising enough eyebrows. The statement made by Rush Doshi, Director of the CFR China Strategy Initiative, tweet only further worked to stir the pot.

Figure 0.4 (Doshi, 2025)

Since the Ministry of Commerce, confirmed that it was infact U.S that had proactively approved the sale of Nvidia H20 chips to China. The notion of a of a mutually beneficial agreement seems unlikely, it would have to do with both Nvidia and AMD agreeing to give the U.S. government 15% of revenue (Freifeld et al., 2025) from sales of chips to China, and which would be the logical explanation of the Trump administration lifting the ban. It also sheds light on why Beijing is so cautious about chips that might contain backdoors especially since Nvidia's H20 chips are custom-made for China, and the U.S. has a long history of leveraging technology for surveillance.

Technicality of backdoor

While Nvidia has undoubtedly declared that their Chips have no remote shutdown features or built in backdoor to them, the probability of backdoor doesn't necessarily have to be built in to be misused, even an existing flaw unknown can be exploited by anyone who knows of its existence. The U.S government over the years has repeatedly tried to leverage

technology for surveillance, some well-known instance would be the **Clipper Chip** introduced during the Cliton Administration.

The Clipper Chip was a programme by the NSA which only lasted from 1993 – 1996, the Chip had an inbuilt backdoor, it basically contained an 80-bit key burned in during fabrication, with a copy of the key held in escrow to used with proper clearance. Although the programme was snuffed because of the obvious, any built-in backdoor can eventually be broken into, and that backdoor itself would pose a very serious security, flaw not to mention even then such an idea was an extreme invasion of privacy (Shaun, 2020). Another recent example would be the PRISM program which was known to the world once Edward Snowden leaked information of its existence.

In an age of Artificial Intelligence and automation, even the notion of a backdoor built in would lead to alarms, especially when the processors which makes all of it possible can be shut down. Even more so when any internal flaw of Chipset alone is sufficient for attackers to take advantage of it. A very recent example can be the vulnerability **CVE-2024-36347** identified in 27th June 2025, which would essentially allow attackers with local administrator rights, to load harmful code into the CPU, which would let them tamper with how the computer runs instructions and steal or change private data, and take over special protected parts of the system (National Vulnerability Database, 2025).

Conclusion

In conclusion even though in the eye's China watchers' Washington's decision to lift the trade ban may have been prompted further profit, but China's concern seems to hold water, since U.S has had a long history of tech backed surveillance. While any company would never allow to install such a backdoor to begin with which would hamper their product, most corporations would undoubtably pursue the courts such as Apple which went to court against U.K government for asking them to install a backdoor, into their encrypted system's.

The question of China's requirement remains the same, unless China is able to produce high level chipsets to cater to its domestic needs for R&D and Technology, it would still be heavily reliant on U.S chipsets, as for the backdoor it seems more unlikely to exist, since companies like Nvidia have already agreed to pay 15% of the revenue earned to U.S government, hence installing any backdoor would only be counterproductive towards that same cause, but the threat of malicious actors taking advantage of undiscovered flaws is a true concern. Even Nivida is anticipating the ongoing market situations and have informed suppliers to halt the production, namely Amkor and Samsung to halt the work on its China-focused H20 AI chip after Chinese regulators raised security concerns and urged firms like Tencent and ByteDance not to buy it. Nvidia insists the chip is secure, non-military, and contains no backdoors, but is adjusting its supply chain accordingly (Reuters, 2025).

References

CAC. (2025, June 31). *The Cyberspace Administration of China (CAC) summoned NVIDIA for a meeting regarding security risks associated with backdoors in the H20 computing chip.* Weixin (Wechat) | Official Handle. https://mp.weixin.qq.com/s/4SfjclOEbZOcus-TXc0KUw

Doshi, R. (2025, July 18). *Beijing embarrasses the Trump team*. X Formerly Twitter. https://x.com/RushDoshi/thread/1946177313344778497

Freifeld, K. (2025, August 9). *US licenses Nvidia to export chips to China, official says*. Reuters. https://www.reuters.com/world/china/us-licenses-nvidia-export-chips-china-official-says-2025-08-08/

Freifeld, K., Bajwa, A., Hunnicutt, T., & Alper, A. (2025, August 12). *Trump opens door to sales of version of Nvidia's next-gen AI chips in China*. Reuters. https://www.reuters.com/world/china/trump-opens-door-sales-version-nvidias-next-gen-ai-chips-china-2025-08-12/

GT. (2025, June 12). *Chinese FM responds to question on Trump's claim that China will supply rare earths magnets to US*. Global Times. https://www.globaltimes.cn/page/202506/1335965.shtml

GT Staff. (2025, June 5). *China affirms rare-earth export controls align with international practices*. Global Times. https://www.globaltimes.cn/page/202506/1335530.shtml

National Vulnerability Database. (2025, June 27). *NVD - CVE-2024-36347*. National Institute of Standards and Technology (NIST). https://nvd.nist.gov/vuln/detail/CVE-2024-36347

People's Daily China. (2025, August 1). *Nvidia How can i Trust You*. Weixin (Wechat) | Official Handle. https://mp.weixin.qq.com/s/biYTJAHYIYuSh57Rc0oKmg

Pfister, A.-K. (2025, June 17). *US-China trade framework agreed and other trade news to know*. World Economic Forum. https://www.weforum.org/stories/2025/06/us-china-deal-and-other-international-trade-stories-to-know-this-month/

Rep. Huizenga, B. [R-M.-4]. (2025, May 15). *Text - H.R.3447 - 119th Congress (2025-2026): Chip Security Act*. 119th Congress (2025-2026). https://www.congress.gov/bill/119th-congress/house-bill/3447/text

Reuters. (2025, August 22). *Nvidia orders suppliers to halt work on China-focussed H20 AI chip, The Information says*. Reuters. https://www.reuters.com/world/china/nvidia-orders-suppliers-halt-work-china-focussed-h20-ai-chip-information-says-2025-08-22/

Shaun, N. (2020, January 27). *Remember the Clipper chip? NSA's botched backdoor-for-Feds from 1993 still influences today's encryption debates*. The Register. https://www.theregister.com/2020/01/27/clipper_lessons_learned/

Todd, L. (2024, March 11). *DOD Looks to Establish "Mine-to-Magnet" Supply Chain for Rare Earth Materials*. U.S. D.O.D News. https://www.defense.gov/News/News-Stories/Article/Article/3700059/dod-looks-to-establish-mine-to-magnet-supply-chain-for-rare-earth-materials/

Venditti, B., & Parker, S. (2025, May 1). *Charted: Where the U.S. Gets Its Rare Earths From*. Visual Capitalist. https://www.visualcapitalist.com/charted-where-the-u-s-gets-its-rare-earths-from/

About the Author

Govind Nelika is the Web Manager/Researcher at the Centre for Land Warfare Studies (CLAWS). He is an alumnus of Pondicherry Central University with a degree in Political Science complemented by a certification in Data Sciences from IBM. His research approach is multidisciplinary in nature, and his focus area at CLAWS is on emerging challenges and trends in the fields of Cybersecurity, OSINT, and the evolving landscape of Strategic Technology, synergized with Generative AI and LLM. In recognition of his contributions, he was awarded the Chief of Army Staff (COAS) Commendation Card on Army Day 2025 for his work with CLAWS.