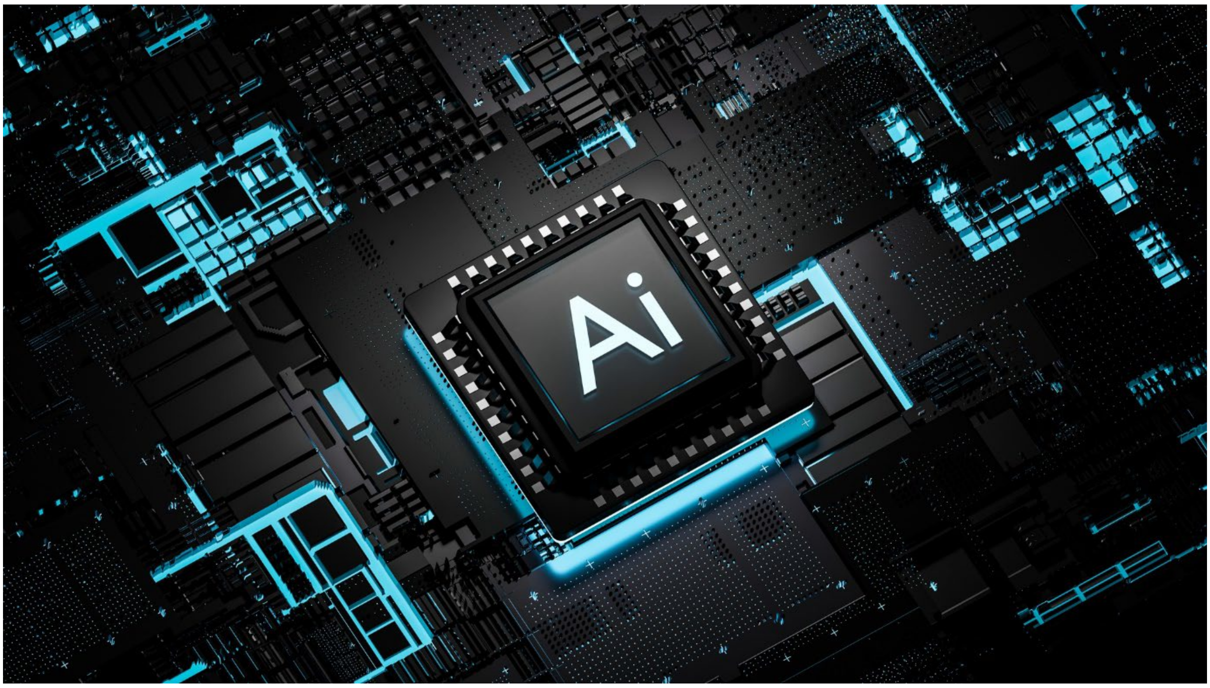
Note: Below are extracts from significant technology articles with global reach, published by The Financial Times (9th November 2023) and Medium (medium.com 13th November 2023) as referenced below.

New AI product development at Nvidia amidst ongoing chip war between US and China, plus what now for global supply chains with the latest cyber security breach at key Australian shipping ports? .



Nvidia to Release Three New AI Chips for China.

In their recent Financial Times report, Liu, Olcott, and Bradshaw (2023) reveal that Nvidia Corp will release three new artificial intelligence chips for China after the US further restricted the Asian nation's access to advanced semiconductors last month:

Nvidia has developed three new chips tailored for China that aim to meet the region's growing demand for artificial intelligence technology while complying with US export controls, according to leaked documents and four people familiar with the situation. The latest effort marks the second time in little more than a year that Silicon Valley-based Nvidia has been forced by new US regulations to reconfigure its products for Chinese customers, as it strives to maintain its foothold in one of its most important markets. Nvidia is preparing to launch the new chips just weeks after the US restricted sales to China of high-performance chips that can be used to create AI systems, in the Biden administration's latest salvo in a tit-for-tat tech war between the two superpowers.

> The three new Nvidia chips are named the H20, L20 and L2, according to a document distributed by the company to prospective customers that was obtained by the Financial Times. The overall performance of these chips has been moderated compared with those that Nvidia had previously sold in China. Nonetheless, the new graphics processing units were expected to remain competitive in the Chinese market, said the people familiar with the situation. "Nvidia is perfectly straddling the line on peak performance and performance density with these new chips to get them through the new US regulations," wrote analysts at Semi Analysis, a chip consultancy, in a note to clients on Thursday. Nvidia did not immediately respond to a request for comment.
>
> Liu, Olcott, and Bradshaw (2023)

According to Liu, Olcott, and Bradshaw (2023), the products which the US targeted last month include Nvidia's A800 and H800 series. They were tailored for Chinese firms after American officials first introduced restrictions on artificial intelligence accelerators for China in 2022, out of concern that it could assist the Chinese in modernizing their military capability.

However, Nvidia has acted quickly in overcoming these latest restrictions:

> Nvidia was co-founded by Jensen Huang, who is also its chief executive. The company's market value soared to more than $1tn this year driven by investor enthusiasm about its dominant role in the processors needed to develop AI systems. Its A100 and H100 chips have become the most sought-after components for AI companies around the world that want to create large language models, the technology that underpins chatbots such as OpenAI's breakthrough ChatGPT. As the US sought to constrain China's AI development, the Biden administration blocked sales of the A100 and H100 GPUs in October 2022. In response, Nvidia developed two alternative models for China, the A800 and H800, which fell below the performance threshold set by US sanctions. But the US last month tightened its restrictions so that they also caught the A800 and H800. The latest export restrictions took effect immediately as the US government speeded up the deadline, leaving Chinese tech groups dependent on outdated and stockpiled chips to pursue their AI ambitions. The rules were seen as forcing Chinese groups to turn to six-year-old technology to develop AI systems. But Nvidia, which has held a dominant share of China's AI chip market, is moving quickly too. The manufacturing process of its latest chips for China was less complex than the development of the A800 and H800, said a person familiar with the situation. Nvidia has already sent samples of the chips for customers to test, suggesting it expects mass production to begin very soon, according to two people close to the company.
> Liu, Olcott, and Bradshaw (2023)

Chinese chip manufacturers are also looking at alternative sources domestically which is challenging, given the dominance of Nvidia in the Chinese market and the geo-political restrictions placed on them both at home and internationally:

> In the interim, Chinese companies have redoubled their efforts to source AI chips from domestic suppliers, reducing the risk of relying on Nvidia and accommodating the escalating AI chip ban. Prominent Chinese Nvidia competitors include Huawei, Cambricon and Biren. The founder of Chinese AI company iFlytek said in August that Huawei's Ascend AI chip could achieve performance comparable to Nvidia's A100. However, Nvidia's Chinese rivals are all constrained by geopolitical conflicts that prevent them from producing chips outside of China, while international sanctions have also sought to limit their access to advanced chipmaking equipment from suppliers such as Netherlands-based ASML.
>
> Liu, Olcott, and Bradshaw (2023)

Cyber attack Paralyzes Australia Ports in Threat to Supply Chains

A cyberattack against one of the world's largest facilitators of global trade has limited access to several ports across Australia, a mass closure that threatens to disrupt supply chains for days. DP World Plc detected a hack on Friday Nov 10th, that forced it to restrict access to four of the nation's largest ports. The government has convened a crisis meeting to coordinate a response. This Finnerty (2023) piece probes further and asks the remaining question: How vulnerable are global supply chains to Cyber Attack as a result?:

> In an unprecedented event, DP World, one of Australia's major port operators, has been hit by a significant cyberattack, leading to widespread disruption of import and export activities across the country. The attack, which targeted the digital infrastructure of the port, has raised alarm bells over the vulnerability of global supply chains to cyber threats.
>
> **The Immediate Impact**
>
> The cyberattack, which occurred early this week, immediately paralyzed operations at DP World's Australian ports. This sudden halt in operations is causing a significant backlog in both imports and exports, which could have far-reaching consequences for Australia's economy and global trade partners. Businesses across the nation, from large-scale manufacturers to small retailers, are bracing for the impact. The shutdown not only affects goods coming into the country but also hampers Australia's ability to export. Key sectors like agriculture, which rely heavily on timely exports, are particularly vulnerable.
>
> **A Wake-Up Call for Cybersecurity**
>
> This incident serves as a stark reminder of the critical importance of cybersecurity in the modern world. With the increasing digitization of supply chains, ports have become hotspots for cyber threats. Experts have long warned about the potential for such attacks, and now those warnings have become a reality. The Australian government, along with cybersecurity experts, is urgently investigating the breach. Preliminary findings suggest a sophisticated level of planning and execution, indicating that this could be the work of an organized group.
>
> Finnerty (2023)

The wider concern as outlined by Finnerty (2023) in his medium.com article, is that this is not just a local issue for Australia, rather a grave concern for global supply chains and is being closely monitored by international trade partners:

> **Ripple Effects on Global Trade**
>
> The disruption at Australian ports has ripple effects on global supply chains. Australia, known for its exports of minerals, agricultural products, and other goods, plays a pivotal role in the international trade ecosystem. The port shutdown is not just a local issue but a global concern, with potential delays and shortages anticipated worldwide. International partners and trade allies are closely monitoring the situation, and there is a concerted effort to provide support and find alternative routes for critical shipments.
>
> **Recovery and Resilience**
>
> As the situation unfolds, the focus is on both immediate response and long-term solutions. The Australian government is working closely with DP World to restore operations and mitigate the impact on businesses and consumers. This includes exploring temporary logistics solutions and providing support to those most affected by the shutdown. In parallel, there is a strong emphasis on bolstering cybersecurity measures across all critical infrastructure, including ports. This incident is likely to accelerate investment in cyber defence technologies and protocols to prevent future attacks.

Finnerty (2023) concludes that the cyberattack on DP World's Australian ports "is more than just a temporary disruption; it is a wake-up call about the fragility of our interconnected global systems. As we move forward, the lessons learned from this incident will be crucial in shaping a more resilient and secure future for global trade and cybersecurity."

References

Liu, Q. , Olcott, E. and Bradshaw, T. (2023) 'Nvidia develops AI chips for China in latest bid to avoid US restrictions'. *Financial Times November 09.* Hong Kong and London. Available at: Nvidia develops AI chips for China in latest bid to avoid US restrictions (ft.com) (Accessed 13 November 2023).

Finnerty, K. (2023) 'Cyber-attack Paralyzes Australia Ports in Threat to Supply Chains'. *Medium.com November 13*. Available at: Cyber-attack Paralyzes Australia Ports in Threat to Supply Chains | by Kevin Finnerty | Nov, 2023 | Medium (Accessed 14 November 2023).