NVIDIA responses, questions for the record - Subcommittee on Communications and Technology on Wednesday, June 4, 2025, "AI in the Everyday: Current Applications and Future Frontiers in Communications and Technology."

The Honorable Russ Fulcher

Can you talk about how NVIDIA's stacking approach and the need to parse large amounts of data being delivered over 5G, and as you note in your testimony, 6G, to ensure there is adequate detection of potential malware trying to infiltrate and undermine controls in everything from power systems, water systems, energy pipeline transfer systems, or even financial networks?

Cybersecurity is critical, and as a full stack accelerated computing company, we are in a strong position to address the risk of malware at every location in the system.

AI will bring many benefits with respect to the security and reliability of critical infrastructure. AI systems are able to process massive data streams to quickly identify and neutralize attacks, whether they are occurring on the device, at the network edge, or in the cloud. This new capability will mean that critical infrastructure, financial markets, and other vital services are better protected from cyber threats. Together, AI and AI-driven cybersecurity will ensure that our hyper-connected world remains resilient, secure, and adaptive.

The Honorable August Pfluger

I am highly concerned about the national security implications of foreign-owned data centers in the United States. Such ownership would provide adversaries with direct access to Americans' sensitive personal data, allow for the disruption of critical infrastructure, or increase the risk of espionage or misuse for malicious purposes. Do you see potential risks posed by foreign adversary-owned or influenced companies from building data centers in the United States?

We are confident that the United States can balance the benefits of investment in the U.S. while mitigating the risks. Data centers in the United States are subject to the jurisdiction and laws of the U.S., allowing the government to track and address risks. Furthermore, we want to ensure that the American infrastructure leads worldwide, promoting American standards and supporting jobs and infrastructure at home. NVIDIA is proud to be an American company driving technological leadership and promoting secure infrastructure both domestically and abroad. In datacenters, telecom networks, and research labs around the world, we're deploying American technology to help advance U.S. leadership. NVIDIA has, and will continue to, supply the most advanced and secure technology solutions for domestic data center buildouts.

From my understanding, the majority of components used in data centers, which AI systems rely on, have complex global supply chains. Many critical parts are manufactured or assembled in foreign countries, sometimes by companies with ties to adversarial governments. This raises additional concerns about the potential for hardware backdoors or hidden vulnerabilities to be intentionally embedded during manufacturing, which could be exploited to compromise U.S. data security or disrupt critical operations. Given these risks, do you have concerns about the national security implications of relying on AI components or hardware sourced from foreign

adversaries, particularly regarding the possibility of supply chain tampering or embedded backdoors?

Cybersecurity is critical to everything we do. We rigorously test our products at every level of the stack to ensure safety and security, and constantly monitor for new and emerging risks. We also work with trusted, long-term partners that understand and share our commitment to security. We have a high degree of confidence in our products and partners and remain vigilant at all times.

Are there regulatory or enforcement gaps that could allow foreign adversaries to gain control or influence over our data infrastructure?

We haven't identified any such gaps, and will continue to make every effort that the U.S. data infrastructure is safe and secure.

Would new legislative measures - such as a ban on foreign adversary control over data centers and critical components - be necessary to close these gaps and ensure robust protection?

We want multinational companies and countries worldwide to use the U.S. technology stack, ensuring that America leads in the AI race. We have robust cybersecurity laws and protections in the U.S. today; to avoid unintended negative consequences, any further measure should be narrowly-tailored to a specific issue. NVIDIA is proud to be an American company driving technological leadership and promoting data center deployments across the country and around the world. We will compete to win everywhere we can—that's the American way.

I also recognize the importance of maintaining U.S. leadership in technology and innovation. What potential economic or innovation impacts should Congress consider when restricting foreign investment and participation in our data center and AI supply chains?

Maintaining U.S. leadership in technology and innovation is an economic and national security imperative. Pursuing policies that allow American companies like NVIDIA to compete worldwide will ensure the U.S. leads in global deployments of AI infrastructure, at every layer of the stack. Multinational companies that invest in the U.S. will also use American infrastructure worldwide, promoting U.S. technical, national security, and economic interests. We can and should encourage investment in America and U.S. technology, while ensuring safety and security.

How can we balance national security with continued technological advancement and global competitiveness?

U.S. technology being the global standard in AI and 6G will support national and economic security. We cannot forfeit leadership to competitors and will compete to win everywhere we can. The surest way for continued U.S. technology leadership is to compete and win at every layer of the AI stack. When we win, we drive the adoption of American technology and standards around the world, promoting national and economic security. This supports continued growth of U.S.-based companies and contributes to reducing trade deficits.

The Honorable Doris Matsui

To meet the increased demand for connectivity, we must use our spectrum resources efficiently. Mr. Vasishta, how can AI maximize the efficiency of a balanced spectrum plan?

As demand for spectrum increases, it is imperative that we develop new strategies for using this limited resource more efficiently. AI plays an essential role in these new strategies. That's why NVIDIA is collaborating with telco and research leaders to develop an AI-native wireless network stack based on the NVIDIA AI Aerial platform, which provides software-defined radio access networks (RANs) on the NVIDIA accelerated computing platform. This effort will help ensure that next generation wireless networks are built with AI from the ground up and capable of utilizing spectrum more efficiently than ever before. Leveraging AI enabled tools like , dynamic spectrum sharing, integrated sensing, real-time beam tracing, dynamic network configuration, digital twins and semantic communications will yield spectral efficiency gains at an unprecedented scale. More spectrally efficient networks enabled by AI-RAN, mean more productivity per megahertz than has ever been possible. It is vital that AI is now integrated into our networks going forward to handle new and increased network traffic.