The Politics of Foreign AI Dependence

By
Sajal Shahid

Published: November 27, 2026

In September 2025, artificial intelligence (AI) once again demonstrated its rapidly increasing potential for misuse. According to a 13-page report published by Anthropic, a group referred to as GTG-1002 used Claude Code in a cyber-espionage campaign that targeted approximately thirty different private and governmental organizations. The attackers convinced the AI agent that it was conducting authorized security testing, after which Claude conducted reconnaissance, identified vulnerabilities, harvested credentials, and conducted other stages of the operation with little human intervention. According to Anthropic, Claude conducted 80 to 90% of the tactical operations.

The significance of this incident was not simply that AI had been used for cybercrime, as similar forms of misuse have occurred before. Rather, it highlighted existing concerns about increasingly capable AI systems and reinforced the need for effective global AI governance frameworks. As the world begins to develop rules for applying this technology, an important question is raised: who decides what the rules are and what will that mean for countries that are not developing AI systems themselves?

The states that are at the forefront of AI development have valid reasons to promote its use, as the technology can generate substantial economic returns and extend their technological influence. At the same time, they have incentives to protect their technological advantage. This tension is already visible in the controls placed on advanced computing and efforts to expand domestic AI infrastructure and policies aimed at maintaining technological leadership. For example, the US has continued to place restrictions on the export of high-performance GPUs and accelerators, which enable large-scale AI training, based on national security grounds.

For states that do not develop advanced AI themselves, the implications are different. While developing nations may wish to adopt AI for healthcare, education, agriculture, and public services; they depend on foreign companies for the models, chips and computing infrastructure needed to do so. This gives the exporting countries significant control over important government functions such as who can access these technologies and on what terms, leaving some governments highly vulnerable to changes in pricing, licensing, and access.

This dependence not only creates security risks but can make it difficult for local firms to compete when regulations that were developed in major AI markets become applicable worldwide. Safety testing, transparency, and auditing standards that are manageable for large corporations can be costly endeavors for smaller firms operating in low-resource countries. If entering a market requires expensive certification, companies with limited resources may be excluded even if their systems meet the underlying safety standards. Thus, the ability to comply with regulations can become another advantage that is concentrated among states with greater technical and financial resources.

There is also a difference between accessing AI and being able to benefit from it. A country may have access to a leading model yet find that it performs poorly in local languages or fails to fulfil the needs of its domestic institutions. Research has already documented significant performance impacts when AI tools trained on Western data are used in different contexts. For instance, AI systems used for agricultural assistance in East Africa have repeatedly failed in basic tasks such as recognizing indigenous crops like cassava or maize. As a result, institutions including the World Bank have stressed the need for AI to be adapted to local contexts.

The capacity to train AI is also unevenly distributed. Adapting AI requires technical expertise, computing infrastructure, data, and investment that many developing countries lack. Where countries cannot adapt systems themselves and have few alternative providers, their dependence on foreign companies becomes greater. This also weakens their bargaining power: if a provider raises prices, changes licensing terms, or restricts access. States are left with a limited ability to negotiate or switch to another system due to few alternatives.

The 2025 US AI Diffusion Rule highlighted how these imbalances can play out in practice. While the rule was introduced to limit China's ability to obtain advanced AI capabilities, it also proposed different conditions for access to advanced computing across other countries. Although it was rescinded before taking effect, the episode showed geopolitical decisions can have consequences far beyond the countries they directly target. On the other hand, states without their own domestic computing infrastructure are left with limited ability to influence such decisions or find alternatives when politics change.

However, the solution is not necessarily for every country to build its own advanced AI model. For many states, its cost would outweigh the benefits. Instead, a more realistic goal is to develop enough technical and institutional capacity to evaluate foreign systems, adapt them to local needs and maintain more than one option for accessing AI technologies. This is where global AI governance can play a role. Rather than focusing solely on the safety of advanced systems, international frameworks may also address unequal access and capacity. Common principles on transparency around technology restrictions, investment in computing and technical expertise, support for local data and language resources, and competition among more providers could give countries with fewer technological resources more room to determine how AI is used in their own economies.

The goal is therefore not just to achieve technological self-sufficiency, but to obtain greater capacity and bargaining power. Countries that do not develop advanced AI should still be able to evaluate the systems that they use, adapt them to their own needs, and have meaningful input into the rules that shape their access to the technology.

Sajal Shahid is a Research Assistant at the Centre for Aerospace & Security Studies (CASS) Islamabad, conducting research on South Asian security. Her work has been published on national and international platforms, including Green Network Asia, The Independent Singapore, and Fair Observer. She can be reached at cassthinkers@casstt.com. Views expressed in this article are the author's own.