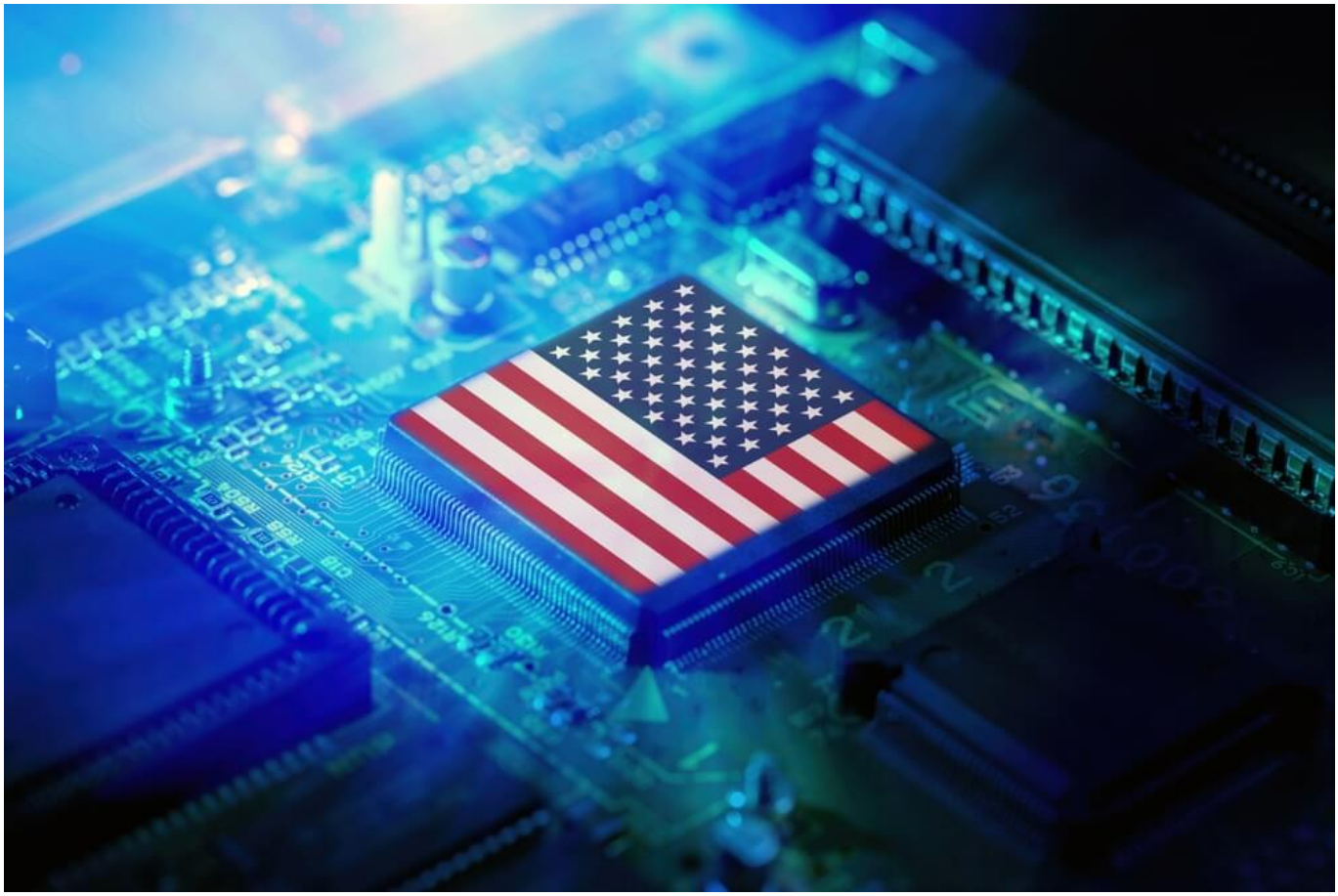
Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: The Editorial Board

The end of open access to the most powerful AI models



In early July, the US government entered the final phase of negotiations with leading artificial intelligence companies on rules for releasing the most advanced models.

These negotiations are not a technical discussion of industry standards, but an attempt to establish a system of state control over today's most powerful technology before it becomes widely available.

Washington no longer regards frontier models as merely products of technology companies. They are treated as a capability that can affect banking, energy, critical infrastructure, cyber defence, intelligence and military advantage.

A country with access to such systems can detect vulnerabilities more quickly, protect networks, process data and build an industrial edge. A country that is restricted remains dependent on another country's permission.

This shift will shape relations between states far more profoundly than public debates about algorithm regulation, copyright, or data protection.

Artificial intelligence is no longer merely an industrial race between American and Chinese companies. It is becoming a way of choosing allies, a test of political trust and an instrument of pressure in trade disputes.

Washington closes the circle around the most advanced AI models

The first serious shift came on 2 June, when President Donald Trump signed an executive order requiring major US companies to submit their most powerful models to federal agencies for safety checks before wider release.

Agencies could test the models for up to thirty days before they became available to users outside the state system.

Departments responsible for finance, defence, internal security and trade are involved in the process. This shows how Washington views this technology.

A model is no longer just software that a company releases when it judges it ready. It is regarded as a capability that can affect the banking system, critical infrastructure, cyber defence, intelligence and military advantage.

> The US Department of Commerce ordered restrictions on access to the Fable 5 and Mythos 5 models for foreign nationals

Just ten days later, the Anthropic case showed how quickly that logic can turn into a concrete ban. The US Department of Commerce ordered restrictions on access to the Fable 5 and Mythos 5 models for foreign nationals, citing security risks. The company temporarily suspended broader access until it could clarify exactly whom it had to exclude.

It was an important precedent. Until then, American controls had mainly concerned the export of chips, production equipment, and computer infrastructure.

Now the focus of control has shifted to the AI model itself. Chips were the entry point to the race; models have become the ultimate capability.

Washington then partially eased the restrictions, but not by opening the system to everyone. Access is shifting towards a model centred on selected users, vetted institutions and trusted partners. This is the core of the new American policy. The aim is not only to stop opponents, but also to determine who is in the inner circle.

Alliance no longer means automatic access

At the G7 summit in Évian in mid-June, a plan was discussed to grant access to advanced

American models only to selected “trusted partners”. This introduces a new hierarchy among allies: it is no longer enough to belong to the same political bloc or security alliance.

Access to the most powerful models will depend on Washington’s specific assessment, the level of security cooperation, and the belief that the state or company will not transfer that capability.

> American policy on models will no longer remain a purely domestic technological issue

This alters the substance of the alliance. In previous decades, the most sensitive exchanges involved intelligence, military technology and nuclear protection. Artificial intelligence has now been added to that list.

As a result, American policy on models will no longer remain a purely domestic technological issue. It will spill over into relations with Europe, Japan, Canada, Australia, the Gulf states and all the middle powers that want access to the most advanced tools but cannot develop them independently.

Europe between American permission and Chinese pressure

Europe enters this phase with a large market, developed regulation, strong research centres and the ambition to build its own digital policy. However, it lags in key areas.

There are not enough state-of-the-art models, computing infrastructure is insufficient, and there is no unified industrial strategy capable of withstanding simultaneous pressure from Washington and Beijing.

When dealing with the US, Europe faces the prospect that access to the most powerful models will depend on political and security conditions set in Washington. Meanwhile, from China, it faces industrial pressure that long ago ceased to be limited to cheap consumer goods.

China is now displacing European manufacturers in machinery, transport equipment, clean energy, electric vehicles and an expanding range of technology components.

At the end of May, the European Commission concluded that the trade and investment relationship with China is no longer sustainable. Behind that formulation lies a simple fact: Europe’s open market can no longer absorb the impact of China’s industrial policy without serious consequences for its own producers.

The problem is not only cheap imports, but also a combination of government subsidies, soft capital, control over supply chains, and manufacturing capacity that Beijing uses as an instrument of industrial dominance.

Brussels is trying to close the channel through which bulk Chinese exports have for years exploited rules designed for individual small purchases

The data explain why the mood in Brussels has changed. The European Union’s trade deficit with China exceeded one billion euros per day in the first quarter of 2026. Chinese exports to the EU continued to grow, while European exports to China fall behind.

An even more serious problem is the pressure from Chinese manufacturers in third markets, where European companies are losing ground in areas in which they have been dominant for decades.

The EU's decision to introduce a three-euro charge on small consignments from 1 July shows how Europe's response to China is filtering down from major industrial sectors to everyday trade.

The number of low-value imports entering the EU rose from 1.4 billion in 2022 to 5.8 billion in 2025, mostly via platforms such as Shein, Temu and AliExpress.

Brussels is trying to close the channel through which bulk Chinese exports have for years exploited rules designed for individual small purchases.

This measure will not solve Europe's problem with China, but it does signal a shift in attitude. Europe can no longer claim to want industrial independence while leaving its market completely open to competition from a system with far stronger state support.

The digital tax opens up conflict among allies

The dispute with the United States is unfolding in another arena. On 26 June, Donald Trump threatened a 100 per cent tariff on goods from countries that introduce a digital tax on American companies. The digital tax has thus ceased to be a matter of budget policy and has become a tool of trade pressure.

France already levies a three per cent tax on the revenues of large digital platforms. The UK has imposed a similar two per cent tax since 2020. European governments claim they want to tax the value created in their markets, while Washington argues that such taxes are directed against American companies.

This dispute illustrates how much the scope for European independence has narrowed. When Europe attempts to limit Chinese pressure, it relies on American models, American cloud services, American chips and American security guarantees.

When it tries to tax American platforms, it faces the threat of tariffs. When it seeks to pursue its own technological policy, it is confronted with the fact that it does not control the most important tools.

> Europe must finance its own computing infrastructure, energy capacity, models, and a market in which European companies can grow

For Europe, this is a question of its industrial base, not just its trade regime. While the most powerful models, cloud infrastructure and largest platforms are predominantly American, and a large part of the production chains and cheap digital hardware is under strong Chinese influence, Brussels can set the rules but does not control the key capabilities. It is a weak position for a continent that speaks of digital independence.

If it wants to change this, Europe must finance its own computing infrastructure, energy capacity, models, and a market in which European companies can grow. Otherwise, its policy will remain limited to taxing and penalising other people's platforms, while the most important decisions about technology are made in Washington, Beijing, and the boardrooms of big companies.

A security concern is not an excuse

The cause of the American acceleration can be seen in the Five Eyes warning of 22 June. The United States, Great Britain, Canada, Australia and New Zealand have concluded that the most advanced AI models can shift the balance of power in cyberspace in the short term.

Such systems can accelerate the discovery of software vulnerabilities, link the different stages of an attack, and enable less trained actors to carry out operations that until recently required specialised teams.

The United Nations warned that the development of artificial intelligence is now beyond the ability of states to understand and control

For defence, they are just as important, but only when institutions with sufficient expertise use them to verify model outputs, limit access to sensitive data, and prevent a tool intended for protection from becoming a source of new risk.

On 1 July, the United Nations warned that the development of artificial intelligence is now beyond the ability of states to understand and control.

Countries that lack their own experts, infrastructure and capacity to audit the systems they use in banking, energy, health, administration and security are particularly vulnerable. They can buy access, but not control.

It marks a new division of the world. It is no longer enough to have the Internet, data centres or digitalised administration.

The key question is whether the state understands the model it uses, whether it can verify its behaviour, whether it has an alternative if its access is limited, and whether it is dependent on the political decisions of another power.

Dependence on other countries' models

By the end of 2026, access to the most advanced AI models will begin to influence companies' credit ratings, insurers' valuations and security due diligence procedures.

Banks, energy groups and telecoms will have to prove not only that they use AI, but also that they know whom they depend on if their access is restricted.

Europe will initially try to address the problem through regulation, but very soon it will have to decide on funding, energy and data centres, because without these it does not have an independent AI policy

The first serious test will come from cyberspace, because an incident in a major financial or energy network will immediately raise the question of whether the attacker had a better model than the defence.

After that, governments will no longer be able to allow AI companies to decide for themselves when a model is safe enough for the market.

US standards will formally remain voluntary but will effectively become mandatory for large companies that wish to do business with government, defence, banks, and critical infrastructure.

Europe will initially try to address the problem through regulation, but very soon it will have to decide on funding, energy and data centres, because without these it does not have an independent AI policy.

China will not need to convince the world that it has the best model, but rather that its models do not carry an American political barrier.

That is why many middle powers will choose affordability over top performance.

Therein lies the greatest risk for the West: access control can protect the most sensitive technology, but it can also accelerate the creation of an alternative market beyond US influence.

The new division will not be between states that use AI and those that do not, but between those that can maintain access in a crisis and those that only then realise how dependent they are.