INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב
Policy Paper

The Battle over Access to Artificial Intelligence: Israel's Next Strategic Challenge

Hadas Lorber | July 1, 2026

Key Points

The restrictions recently imposed on Anthropic — including the U.S. administration's directive to limit access to certain models for users and entities outside the United States on national security grounds[1] — constitute a significant milestone in the evolving relationship between technology, national security, and foreign policy. Whereas over the past decade, the discourse surrounding digital sovereignty has focused on issues such as privacy, data localization, regulation, and cloud infrastructure, recent developments point to a transition to a new phase in which access to advanced artificial intelligence capabilities is becoming a strategic asset in itself. In this reality, not only data or chips are becoming objects of government policy, but also the models themselves.

This article argues that the Anthropic case is not an isolated incident but rather a manifestation of a broader trend, in which artificial intelligence is becoming a central component of national power. As a result, access to advanced models may in the future become a policy tool, a mechanism of geopolitical influence, and a means of advancing strategic interests. For Israel, this development necessitates a reassessment of its approach to technological sovereignty and its policies in the fields of artificial

[1] The directive conveyed to Anthropic on June 12 by the Trump administration required the company to terminate access to its Fable 5 and Mythos 5 models for all foreign users, including the company's foreign employees, users outside the United States, and international clients. According to reports, the company was given a very short timeline to implement the directive, under the threat of civil and criminal sanctions in the event of non-compliance. At a later stage, a limited exemption was granted, allowing the use of Mythos 5 for a small number of critical infrastructure organizations within the United States, while Fable 5 remained restricted.

intelligence, computing, and infrastructure, as well as a rethinking of its broader security paradigm.

****

In recent years, artificial intelligence has emerged as one of the central areas of competition in the international area. States, companies, and organizations are investing unprecedented resources in the development of advanced models, the establishment of computing infrastructure, and the creation of innovative AI-based ecosystems. This process is accompanied by a profound shift in how governments perceive technology. Whereas in the past most AI applications were viewed as commercial products developed by private companies and operating within the global market, there is now growing recognition that artificial intelligence constitutes strategic infrastructure, with direct implications for economic power, technological superiority, scientific innovation, and national security.

Against this backdrop, recent developments surrounding Anthropic and its Mythos 5 and Fable 5 models represent an event whose significance extends far beyond the specific case of this company. For the first time, access to an advanced AI model has become an issue perceived by the U.S. administration as having national security implications. The Anthropic case began on June 12, when the U.S. administration instructed the company to restrict access to its advanced AI models — including Mythos 5 and Fable 5 — for users and organizations outside the United States. According to reports, the directive was issued on national security grounds, as part of a broader policy aimed at preserving the United States' technological advantage in artificial intelligence.

Although the decision sparked public and legal controversy, the very fact that the administration had intervened in the availability of commercial AI models marked a significant shift: for the first time, AI models were treated not merely as software products, but as strategic assets whose access may be subject to geopolitical considerations and export controls.

Developments did not end with Anthropic. A few days later, it was reported that OpenAI was also asked by the U.S. administration to limit the initial release of its new flagship model, GPT-5.6, making it available first to a limited group of government-approved partners for security review and assessment before broader public access. Although OpenAI cooperated with the request and emphasized that it was a temporary measure, the very fact of the request illustrates that government intervention is not confined to a single company, but reflects an emerging policy under which advanced AI models are regarded as strategic assets subject to national security considerations and governmental oversight.

From a legal perspective, the move raises complex questions. At this stage, no federal law explicitly regulates restrictions on access to advanced AI models for foreign users. Some of the measures rely on existing executive powers in the areas of national security, export controls, and critical infrastructure protection, alongside a presidential order issued in June 2026 that

established a mechanism for the prior review of frontier AI models before their public release.[2] However, legal and technology policy experts have noted that the legal basis for direct intervention in the availability of commercial models remains unclear, and that the scope of governmental power is likely to face both public and judicial scrutiny. This very uncertainty reinforces the strategic message: even in the absence of explicit legislation, government decisions can have an immediate impact on access to advanced AI technologies.

Even as the debate over the specifics of the case continues to evolve, the fact that an AI model is being treated as a strategic asset whose access may be restricted, marks a profound conceptual shift. Advanced models are no longer merely software products; they are becoming infrastructures of power.

This development necessitates a reassessment of the concept of technological sovereignty. Whereas in the past the discourse focused on data sovereignty — that is, where data is stored, who controls it, and under which legal and regulatory frameworks it operates — an emerging reality is taking shape in which the central question is one of Access Sovereignty — the ability of states, companies, and organizations to maintain reliable and continuous access to the world's most advanced AI capabilities.

From the Anthropic Case to the Era of Strategic Artificial Intelligence

For years, the prevailing perception in both the public and private sectors rested on the assumption that artificial intelligence models are commercial products that can be purchased or accessed, much like other software services. This perception was grounded in the logic of the internet economy, according to which technological innovation spreads rapidly and enables the broadest possible access to markets and users.

However, next-generation models are challenging this assumption. Unlike earlier generations of software systems, advanced models are increasingly evolving into general cognitive systems capable of performing tasks of growing complexity. Their capabilities span software

---

[2] There is currently no explicit U.S. law that directly authorizes the blocking of access to an AI model. What exists instead is a combination of the following mechanisms:

1. **Export Administration Regulations (EAR)** – export control regulations administered by the Bureau of Industry and Security (BIS) within the U.S. Department of Commerce. These regulations grant the administration powers to restrict the export of sensitive technologies on national security grounds. In the Anthropic case, it has been argued that the directive was issued under these powers, although the directive itself has not been made public.
2. **Executive Order 14409 (June 2, 2026), "Promoting Advanced Artificial Intelligence Innovation and Security"** – which establishes a framework for the review of frontier AI models and the assessment of national security risks. However, it does not explicitly create a new mechanism for restricting the export of AI models.
3. **General national security powers of the executive branch** – under which it is argued that exceptional directives may be issued when a technology is perceived as having strategic significance.

development, scientific research, intelligence analysis, complex systems planning, cyber vulnerability discovery, content generation, translation, simulation, data analysis, and decision-making.

The implication is that advanced models are no longer merely tools, but cross-cutting force multipliers. Their potential impact on productivity, research and development, security capabilities, and economic competitiveness renders them assets of strategic value.

From a U.S. perspective, this development necessitates a new conceptual framework. Just as governments impose export controls on advanced chips, encryption systems, supercomputing, and other dual-use technologies, there is a growing inclination to apply similar considerations to advanced AI models. In other words, artificial intelligence is beginning to undergo a process of "strategic classification," whereby access to certain capabilities may be shaped by security considerations rather than purely commercial ones.[3]

AI Models as a New Instrument in U.S. National Security and Foreign Policy

The broader significance of the Anthropic case is not technological but geopolitical. For decades, the United States has relied on a range of mechanisms to preserve its strategic advantage: control over the international financial system, export controls, privileged access to advanced technologies, and dominance over key chokepoints in global supply chains. In recent years, advanced AI chips have been added to this list. It now appears that AI models themselves may also become part of this framework.

This trend stems from the recognition that advanced models generate significant advantages not only for private companies but also for states. A model capable of accelerating scientific research, shortening development cycles, enhancing cyber capabilities, or supporting complex decision-making processes constitutes a strategic asset. This perception is also shaped by the intensifying competition between the United States and China for leadership in artificial intelligence. From the perspective of the U.S. administration, maintaining technological superiority requires not only investment in infrastructure and models, but also control over access to them, in order to prevent the diffusion of capabilities that could strengthen strategic rivals. In this context, control over access to models may, in the future, become a tool of influence over other states and a central instrument of foreign and security policy.[4]

---

[3] From a legal perspective, the directives relied on existing executive powers in the areas of national security and export controls, alongside the presidential order on frontier AI. However, the legal basis for direct intervention in the availability of commercial AI models remains contested and is already subject to both public and judicial scrutiny.

[4] See also: Sobelman Ariel and Genkin Michael, **"Does Israel Need a National Language Model?"**, INSS Insight, No. 2047, Institute for National Security Studies, October 20, 2025.

This development aligns with a broader shift from a focus on data to a focus on capabilities. Whereas in the past the debate revolved around the question "where is the data located?", it now centers on the question "who has access to the most advanced capabilities?".

The implications of this shift are not limited to the economy or industry; they extend directly to national security. In recent years, leading militaries — foremost among them the U.S. military — have begun adopting an AI-first approach.[5] Within this framework, artificial intelligence is integrated into the core of intelligence, decision-making, and operations. Advanced models enable the processing of information at unprecedented scale, the identification of patterns, the construction of real-time situational awareness, and enhanced support for commanders.

As models become more advanced, their influence is likely to extend across all domains of warfare. The ability to secure access to the most advanced models may, in the future, become a key differentiator among militaries and states. Accordingly, access to AI models is no longer merely an economic or technological issue, but also one of operational superiority.

Implications for Israel

For Israel, this development carries significant strategic importance. Israel currently benefits from close cooperation with the United States and broad access to American technologies. The Anthropic case, however, illustrates that even close allies may find themselves dependent on regulatory, security, or political decisions made beyond their borders.

This dependence is not limited to the models themselves. It also extends to computing, cloud infrastructure, semiconductors, and broader AI infrastructure. As the Israeli economy, the defense establishment, and advanced industries increasingly rely on AI, the importance of ensuring continuous and reliable access to these capabilities grows accordingly.

The implications are not confined to the civilian-economic sphere. While security bodies operate in secure environments and use dedicated models when handling sensitive information, the defense establishment and defense industries are also increasingly reliant on advanced AI models for research and development, software engineering, simulations, engineering processes, data analysis, and the acceleration of innovation. Restrictions on access to the most advanced models could undermine the pace of technological development in the defense sector and erode the qualitative edge which Israel relies on.

At the same time, the civilian sphere is also likely to be significantly affected. Israel's high-tech ecosystem, startups, research and development centers, academic institutions, and business organizations increasingly depend on advanced AI models for software development, research, and innovation. A slowdown in the economy's innovative capacity is not merely an economic issue; over time, it may also affect Israel's national power, the knowledge and technological

---

[5] For further discussion, see: Lorber Hadas, *"The Pentagon's AI-First Doctrine and Its Implications for Modern Warfare: Lessons from the Conflict with Iran,"* INSS Insight, No. 2116, Institute for National Security Studies, March 19, 2026.

base underpinning its defense industries, and the economic resources available for investment in security.

In this sense, the Anthropic case serves as a warning sign. It does not necessarily indicate an American intention to harm its allies, but rather reflects a structural shift in the international system. From the U.S. perspective, the concern stems not only from the potential misuse of advanced models for cyber operations, weapons development, or the acceleration of military research, but also from the desire to preserve the technological advantage of the United States and its allies in an era in which artificial intelligence is perceived as strategic infrastructure. In this context, restricting access is seen not only as a risk mitigation tool but also as a means of maintaining geo-technological advantage. In a world where AI is treated as a strategic asset, the key question is no longer only who develops the technology, but who can guarantee access to it — and under what conditions.

Accordingly, Israel's challenge is not to achieve complete independence in this domain — an unrealistic and undesirable goal — but rather to build strategic resilience based on diversification of suppliers, partnerships with allies, and investment in domestic computing infrastructure.

Policy Recommendations for Israel

In light of recent developments, Israel must adopt a broader conception of technological sovereignty — one that relates not only to data but also to capabilities. This does not mean striving for full independence from American models, but rather ensuring that Israel's status as a strategic ally is translated into long-term access to the most advanced capabilities. Alongside investments in domestic computing infrastructure and complementary capabilities, a strategic dialogue is required with the U.S. administration and leading AI companies, aimed at establishing trust, security, and oversight mechanisms that will ensure continued access to models even in an era of export restrictions. Just as Israel currently benefits from special arrangements in the security domain, it should work to establish a dedicated framework for cooperation in AI.

The following recommendations are proposed:

First, Israel should act to ensure long-term access to the world's most advanced models through a strategic dialogue with the U.S. administration and leading AI companies. Access to advanced models should be treated as a national interest and integrated into the strategic discourse between the countries (including under the U.S.-led *Pax Silica* initiative, according to which the power of states is determined by their ability to secure reliable access to all AI infrastructure, including advanced models).

Second, Israel should accelerate investment in domestic computing infrastructure. This does not imply full independence, but rather the development of baseline capabilities that provide strategic flexibility in the event of changes in the international environment. These include independent access to computing resources, secure cloud infrastructure, the ability to run

advanced models locally when necessary, and the development of complementary capabilities in areas where Israel has a relative advantage, such as cybersecurity, defense, and healthcare.

Third, Israel should promote the development of dedicated models in areas of national importance, particularly in defense, intelligence, the Hebrew language, and government systems. The goal is not to compete with global models, but to reduce gaps and build complementary capabilities.

Fourth, Israel should consider establishing a permanent governmental mechanism to monitor technological dependence in the field of artificial intelligence. This mechanism should map risks, identify strategic bottlenecks, and develop alternatives in cases where access to critical technologies is disrupted.

Fifth, Israel should actively participate in shaping the international rules of the game in artificial intelligence. As in the fields of cybersecurity and innovation, diplomatic and technological engagement is required to ensure that Israeli interests are taken into account.

Beyond these steps, a reassessment of Israel's national AI strategy is required. The government decision approved in June 2026 to advance artificial intelligence through investment in computing infrastructure, human capital, research and development, public services, and innovation is an important and significant step.[6] However, the Anthropic case demonstrates that alongside these components, an additional strategic layer must be added: ensuring continuous and long-term access to advanced AI capabilities.

To date, most national strategies worldwide have focused on developing capabilities, human capital, and infrastructure. Yet the emerging reality requires states to ask how they will have access to the most advanced models in the future, and under what conditions. In other words, national AI policy cannot focus solely on developing domestic supply; it must also address the management of strategic dependence on global providers.

Accordingly, it is recommended to incorporate, as part of the implementation of Israel's national AI strategy, a dedicated component for securing access to artificial intelligence. This component should include mapping Israel's dependence on foreign models, assessing risks stemming from future access restrictions, developing backup and continuity mechanisms, and strengthening strategic partnerships with leading countries and companies in the field. As in energy, cybersecurity, or supply chain policy, the focus must shift from efficiency alone to resilience, technological redundancy, and survivability.

In the long term, one of the key indicators of success for Israel's AI strategy will not be only the number of companies, researchers, or investments in the field, but also Israel's ability to ensure

[6] Government of Israel Decision No. 4255 (June 16, 2026), Accelerating Artificial Intelligence in Israel and Establishing Global Leadership — Strategic Principles, Courses of Action, and Amendment to a Government Decision.

reliable, continuous, and sustainable access to the world's most advanced AI capabilities — even during periods of geopolitical tension or changes in export policies by leading states.

Conclusion

The Anthropic case is not merely an isolated incident involving a single technology company. It is an indication of a deeper transformation in the international system, in which advanced AI models are becoming strategic assets with economic, security, and geopolitical significance.

The shift from data sovereignty to security-driven access constraints marks the emergence of a new dimension in global technological competition. In the future, states will be required not only to protect their data, but also to ensure their ability to access the most advanced cognitive capabilities. For Israel, the central challenge is not only maintaining its security edge, but also preserving the innovation capacity and growth of its economy. In a world where access to advanced AI models becomes a strategic resource, Israel's ability to secure continuous access to these capabilities will play a decisive role in shaping the future of its high-tech sector, scientific research, and overall competitive advantage.