

Digital Sovereignty: A Conceptual Framework for Israel and Policy Recommendations

Hadas Lorber¹ | December 18, 2025

Digital sovereignty has, in recent years, become one of the central components of national power, economic resilience, and security. Artificial intelligence, cloud computing, data, and capital-intensive computing infrastructure constitute foundational elements for governmental, military, and economic activity. Accordingly, control over digital infrastructure is not merely a technological or economic issue but a strategic concern of the highest order.

Israel, as a powerhouse of technological innovation, currently finds itself in a paradox. It is a leader in the development of advanced technologies and benefits from a highly developed technological ecosystem. At the same time, it is increasingly dependent on digital infrastructures controlled by foreign actors, including global cloud providers, semiconductor supply chains, and a regulatory framework that is not always aligned with the scale of investment, the risks involved, and the unique characteristics of strategic digital infrastructure. This situation presents Israel with a strategic challenge: how to preserve openness and innovation while ensuring control, resilience, and sovereignty over critical digital assets.

This paper aims to present a conceptual framework for digital sovereignty, to identify principal policy challenges, and to propose an infrastructural and regulatory agenda for integrated implementation that balances public, economic, and security interests.

Conceptualization: Digital Sovereignty in the AI Era

Digital sovereignty is defined as a state's ability to control its digital infrastructure, data assets, core technologies, and governance and regulatory frameworks while minimizing dependence on external actors. In an era in which data and computing constitute critical resources, such control is tantamount to national security sovereignty in the fullest sense of the term. Control over cloud infrastructure, server farms, AI algorithms, and semiconductors forms the backbone of the digital economy, the public sector, and the defense establishment. Insufficient control may create systemic vulnerabilities, exposing the state to geopolitical pressures and constraining its freedom of action.

¹ Hadas Lorber is the Director for the US-Israel Project and head of the Technology Partnerships initiative at the Institute for National Security Studies (INSS).

Digital sovereignty develops in three stages. In the first stage, the state functions primarily as a user of external technologies and services—an arrangement that enables efficiency and innovation but creates dependency and risk. In the second stage, the state seeks infrastructural and regulatory control as an owner, including the establishment of domestic infrastructure (hardware, software, data centers) and setting cybersecurity and operational redundancy standards. This reduces dependency but does not ensure full autonomy. In the third stage, the state becomes a producer of core technologies, exercising control over intellectual property and critical knowledge, achieving comprehensive independence across the entire supply chain—from chip to algorithm.

Supply Chains, Energy, and Regulation: Core Components of Digital Sovereignty

Digital economy relies on cross-border supply chains, from advanced hardware to software and cloud services. This dependence exposes states to geopolitical and strategic vulnerabilities, as demonstrated by the global supply-chain crisis during the COVID-19 pandemic and US-China tensions in the semiconductor sector. Research indicates that strategic dependency management is preferable to full de-globalization. Strengthening domestic capabilities in areas of comparative advantage while maintaining controlled dependence in others allows for resilience while preserving efficiency and global economic cooperation.

At the same time, digital sovereignty requires an integrated systemic approach that recognizes data centers and AI infrastructure as strategic electricity consumers, prioritizes their grid connection, and simultaneously advances conventional and renewable electricity generation, storage capacity, and a modernized grid.

In parallel, regulation aligned with friendly regulatory systems, such as those of the United States and the European Union, constitutes a central tool. This alignment enables the state to set standards, define operational boundaries and rules, oversee foreign actors, and incentivize investment in capital-intensive projects while ensuring transparency and investor protection.

Israel's Status Assessment 2026

Although Israel benefits from a highly developed technological ecosystem, it is deeply dependent on global infrastructure (positioned between the user and owner stages, with a substantial gap before reaching producer status). Multinational corporations largely control cloud infrastructure, AI services, data centers, and supply chains, while the domestic regulatory framework is not always adapted to the scale of investment, risk profile, and unique characteristics of strategic digital infrastructure.²

² In this context, the entry of Nebius and the establishment of high-performance computing (HPC) and AI infrastructure, alongside the Israel Innovation Authority's national supercomputer initiative and the conditions attached to the project, signal a

This dependence generates short-term economic benefits but holds long-term strategic risks, as control over computing infrastructure and data constitutes a source of geopolitical and economic leverage. Without sufficient national control, Israel may face regulatory pressure, restricted access to critical services during times of crisis, and constraints on its civilian and security freedom of action.

Inherent market failures, stemming from high levels of required investment and long return on investment horizons, affect the development of strategic digital infrastructure. Relevant projects—server farms, cloud infrastructure, and high-performance computing facilities—require capital investments amounting to billions of dollars and involve substantial technological, regulatory, and operational risks. These characteristics do not align with conventional financial market structures or standard corporate governance models. Consequently, the private sector struggles to initiate and finance projects of national importance without state intervention or tailored regulatory adjustments.

Regulatory uncertainty constitutes an additional barrier. At present, Israel does not define server farms, cloud infrastructure, or AI systems as strategic assets critical to national infrastructure. The existing regulatory framework does not provide long-term certainty for investors and entrepreneurs. The absence of a national policy and coordination among regulators—across energy, planning and construction, finance, defense, and communications—leads to delays and high regulatory costs, deterring private investment. Under such conditions, regulation designed to protect the public and promote competition may, in practice, impede the development of critical infrastructure.

Finally, we are witness to an energy and infrastructure bottleneck, stemming from the gap between the growing demand for electricity and the pace of generation and grid development. Electricity demand is expected to grow rapidly in the coming years due to data centers,³ AI, transportation electrification, and climate change. However, the development of generation, transmission, and distribution infrastructure is characterized by long timelines and planning and regulatory constraints. Without

strategic opportunity to reduce dependence on foreign cloud infrastructure and to strengthen sovereign computing capabilities. At the same time, they underscore the need for a regulatory and infrastructural framework that ensures national control over these critical infrastructures.

³ According to various scenarios, data centers are expected to add tens of TWh annually to the electricity sector and to require installed capacity of several thousand megawatts. Their contribution to peak demand is projected to become significant in the coming decade, as more than 2,000 additional MW during peak hours will be needed by 2050, both in summer and in winter. The inclusion of data centers is altering the overall growth trajectory of the electricity sector and accelerating its average annual growth rate.

accelerated development of the electricity sector, critical digital infrastructure may encounter supply limitations, undermining the reliability of digital services and weakening Israel's digital and economic resilience.

From Challenges to Opportunities: The Need for Enabling Regulation and Proactive Infrastructure Policy

The challenges outlined above indicate that digital sovereignty cannot rely on market forces alone and cannot be a byproduct of general technology policy. It constitutes a multi-dimensional systemic challenge requiring proactive state intervention, inter-ministerial coordination, and long-term infrastructure planning. Dependence on foreign infrastructure, market failures in capital-intensive projects, regulatory uncertainty, and energy bottlenecks are not isolated problems but symptoms of the lack of an integrated framework for digital sovereignty. Accordingly, an enabling regulatory approach is required—one whose objective is not merely to minimize risk but also to facilitate investment, create certainty, and accelerate the development of critical infrastructure.

Enabling regulation entails establishing stable, long-term rules, prioritizing digital and energy infrastructure at the national level, and removing structural barriers to financing strategic projects. In this context, the state is a regulator, a strategic planner, an infrastructure coordinator, and at times an investment partner. This model is familiar from the energy, water, and transportation sectors and is now required in the digital domain, where computing and data infrastructure constitute foundational national resources.

Policy Recommendations for Advancing Digital Sovereignty in Israel

First, a strategy for national digital sovereignty should be formulated, formally defining cloud infrastructure, data centers, AI infrastructure, and data assets as strategic national assets—similar to energy, water, and communications infrastructure. This strategy should include quantitative targets, gap analysis, and a multi-year investment plan and should be managed at the inter-ministerial level.

Second, regulatory and structural reform is required in the financing and corporate governance of capital-intensive projects. Dedicated capital structures for digital infrastructure projects should be considered—such as public-private partnerships, dual-control mechanisms, or hybrid financing instruments—while ensuring transparency, oversight, and investor protection. Adapting the regulatory framework to the characteristics of strategic projects may mitigate market failures and enable private-sector entrepreneurship at the national scale.

Third, an integrated infrastructure policy in the energy sector should be implemented, recognizing data centers and AI infrastructure as strategic electricity consumers and granting them priority in generation, grid, and storage planning. This policy should include accelerated licensing tracks, stringent standards for redundancy and

reliability, and early coordination between developers and electricity and planning regulators. Without exceptional acceleration in transmission and distribution grid development, investment in digital infrastructure will not translate into operational capacity.

Fourth, a sovereign hybrid cloud and data governance framework should be developed, defining clear rules for the storage and processing of sensitive data and enabling integration between government cloud, private cloud, and global cloud services under regulatory supervision. This framework should balance security, privacy, competition, and innovation while ensuring subordination to Israeli law.

Finally, a permanent strategic forum on digital sovereignty should be established, comprising representatives of the government, defense establishment, industry, and academia. The forum should focus on policy formulation, risk assessment, and regulatory adaptation to technological developments. It could serve as a platform for policy co-creation, ensuring that national policy remains dynamic, knowledge-based, and responsive to evolving geo-technological realities.

Conclusion: Between Global Dependence and Technological Independence—Digital Sovereignty as the Balancing Point

Israel stands at a critical juncture in which computing, data, and energy constitute integrated strategic resources. Transitioning from dependence on foreign infrastructure to digital-energy sovereignty is a necessary condition for preserving Israel's status as a technological leader and a sovereign state. Developing sovereign digital and energy infrastructure will not only strengthen national security and economic resilience but will also serve as a significant growth engine, generating high-skilled employment, attracting foreign investment, and reinforcing Israel's position as a global hub for advanced technologies. Implementing a proactive policy in accordance with the recommendations outlined in this document will safeguard Israel's technological, economic, and strategic independence in the AI era.