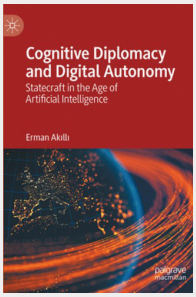
Cognitive Diplomacy and Digital Autonomy:
Statecraft in the Age of Artificial Intelligence

By Erman Akıllı
Cham: Springer Nature, 2025, 390 pages, €179.99, ISBN: 9783032044693

Reviewed by Emily Cruz Villegas, Ankara Hacı Bayram Veli University
DOI: 10.25253/99.2026282.BR3



In *Cognitive Diplomacy and Digital Autonomy: Statecraft in the Age of Artificial Intelligence*, Erman Akıllı explores the profound impact of digital technologies on sovereignty and diplomacy in a technopolar world, establishing digital autonomy as a defining challenge for states today. As a faculty member in International Relations at Ankara Hacı Bayram Veli University, Akıllı specializes in Artificial Intelligence (AI) in foreign policy, digital diplomacy, and public diplomacy. The author introduces foundational geopolitical concepts, including the technopolar world and sovereignty 2.0, before advancing to specialized constructs such as digital autonomy and cognitive diplomacy. This progression establishes a clear, intuitive hierarchical structure.

The book is organized into five parts and 15 sub-chapters, each written in article format, moving from conceptual and historical foundations to an analysis of digital autonomy, cognitive diplomacy, and their implications for governance and policy. The present analysis mirrors this structure, moving from a macro-level exploration of global order to the micro-mechanisms of digital statecraft. Firstly, classic sovereignty is reexamined in a context where governments, technological platforms, algorithmic processes, digital sovereignty, and transnational infrastructure drive competition. Today, sovereignty extends beyond territorial borders, encompassing "the control over narratives, data, and cognitive frameworks through which societies perceive themselves and the world" (p. 39). It is, therefore, multifaceted, evolving into the complex model of sovereignty 2.0. The recognition of the technopolar world as a geopolitical condition distinguishes this work from other scholarly perspectives. The author challenges arguments that characterize Big Tech firms as "Leviathan" or as new data sovereigns, asserting that such firms are not autonomous actors in global politics because they reflect and facilitate the needs and preferences of dominant political elites (p. 26). This position reinforces the view that nation-states remain the sole regulators of the territories and landscapes.

Still, it is argued that while governments are adapting to new technologies and actively developing policies, there is a noticeable shift in power dynamics, with state authority increasingly intertwined with corporate influence. Likewise, as cyberspace transcends territorial jurisdiction, it raises critical questions about the extent of state authority over online domains and the appropriateness of traditional concepts of sovereignty and intervention. In the author's view, the frequency and sophistication of cyber threats have fundamentally

altered the theoretical framework for analyzing security, revealing a sovereignty gap: even when states are formally sovereign within their digital borders, those borders often remain beyond unilateral control. The recurring question is about what happens when a state's sensitive information or a citizen's data are stored on a cloud server abroad. The narrative suggests that states must develop the capacity to manage and secure their cyber domains. Where security remains paramount, data sovereignty, algorithmic capacity, and hardware autonomy have become central to digital policy. Control over data and algorithms is positioned as vital as control over resources and territory, prompting critical examination of power dynamics under "algorithmic governance." The U.S., China, the European Union, India, and Brazil exemplify this through their pursuit of technological autonomy and semiconductor production.

Whether sovereignty 2.0 aligns with democratic oversight and the rule of law depends on government approaches to emerging challenges (p. 47). Current debates highlight data management in democratic contexts, with the author emphasizing that "the mere localization [of data] does not equal absolute control" (p. 60). Another theoretical concern is about who truly controls the data and algorithms that shape societal outcomes, particularly in diplomatic contexts where the locus of agency becomes ambiguous. Bias and fairness pose additional challenges for state governance over data flows and algorithmic decision-making. Algorithms are not neutral; they may reflect the hidden objectives of their creators. Therefore, regulatory frameworks and expertise should reduce reliance on "black box" systems by ensuring transparency and accountability.

Explaining the above, the book delves into the fact that regulation and algorithmic expertise represent complementary dimensions. States should integrate algorithms within legal, ethical, and domestic frameworks to advance national objectives. However, each country's approach is shaped by distinct norms, strategies, and regulatory cultures, reflecting the inseparability of technological leadership from national interests. To illustrate this, the volume presents a comparative analysis of digital governance models in the U.S., China, and Russia (p. 125). The U.S. follows a laissez-faire approach emphasizing privacy, free markets, and limited government intervention, while China prioritizes collective security through mass surveillance and the Great Firewall. Russia, on the other hand, adopts a conservative stance and state authority to safeguard information sovereignty. These systemic foundations lead us to the book's central claim: digital autonomy is a "geopolitical necessity." Such autonomy is defined as the ability to act across three operational and interconnected pillars: presence, practice, and resilience (p. 110).

The justification for digital autonomy arises from the existence of "digital asymmetry," in which access to digital capabilities and control over informational architecture are concentrated among a limited number of states and corporations. As a result, states with greater computational capacity wield increased power and influence. The technological rivalry between the U.S. and China exemplifies the monopolization of AI technologies. Technological interdependence thus remains a critical concern, as no country achieves complete hardware autonomy. Peripheral states depend on foreign cloud systems, AI infrastructure, and foundational software supplied by leading technological powers. The author, however, asserts that peripheral countries often resist exclusive alignment with either the U.S. or Chinese digital models, instead adopting a "hybrid" approach. India and Türkiye

exemplify this trend by implementing strategic diversification and comprehensive policies to promote data sovereignty and mitigate dependency. Hence, digital autonomy should be understood as a structural countermeasure to inequalities within the digital domain.

The final chapters address the emergent domain of cognitive diplomacy. It facilitates the integration of human judgment with machine learning, providing a framework for understanding how governments pursue influence and resilience within the most intimate domain: the human mind (p. 169). The author emphasizes that, in diplomatic practice, AI models augment rather than replace human judgment; therefore, he addresses AI as a "transformative" force that reshapes the cognitive and organizational processes underlying diplomacy. Accordingly, a human-centric approach is presented as an ethical imperative: "AI must augment cognition, not overwrite conscience" (p. 240). While exploring ethical and legal concerns, such as algorithmic integrity, institutional responsibility, and strategic trust, the author concludes that integrating large language and predictive models into foreign policy is "a profoundly normative act." For cognitive diplomacy to succeed, it must enhance human sensibility while preserving the moral intuition and emotional intelligence that machines cannot replicate (p. 233). This encourages scholars to examine human cognitive architecture.

This work also warns that the absence of clear norms or agreed boundaries may unintentionally escalate tensions and undermine trust. As a result, policy frameworks should also require "explainability" in AI systems (p. 271), ensuring that clarity prevails over ambiguity. In this sense, an ethical framework is proposed, consisting of recommendations to safeguard human-centered principles in diplomacy. The primary objective is to foster ethical reasoning and intercultural understanding through intelligent systems grounded in international law principles. This highlights the importance of digital literacy, with an emphasis on digital self-reliance, human capital development, hybrid intelligence, cognitive resilience, and digital alliances. There is a clear need for guidance that supports rigorous research, enabling academics and policymakers to advance the field. The book thus serves the objective of providing stakeholders with a conceptual framework rather than metaphors and actionable strategies to navigate a global landscape shaped by technological sovereignty, cognitive advantages, and resilient diplomacy.

Lastly, a deeper engagement with middle powers and the Global South would help assess the broader applicability of the book's framework beyond major technological powers. Still, the originality of this work lies in its theoretical innovation, achieved through the synthesis of interdisciplinary knowledge from cognitive science and international relations. Akıllı provides a structured and multidimensional analysis at a time when academics, policymakers, and diplomats require conceptual tools to explain and respond to the rise of the so-called technopolarity. Such academic effort seeks to establish a robust knowledge base to support navigation of the rapidly evolving global landscape, making it valuable to both academic and policy audiences concerned with digital sovereignty and contemporary geopolitics.