DOI: https://doi.org/10.36719/2789-6919/55/79-82

**Elgiz Abdurahmanli**
Azerbaijan University of Tourism and Management
PhD student
https://orcid.org/0009-0002-3504-9974
abdurahmanli_e @mail.ru

# The Geopolitical Architecture of Cyberspace: Cyber Sovereignty, Digital Power, and Normative Competition

**Abstract**

This article examines the geopolitical architecture of cyberspace through the interconnected concepts of cyber sovereignty, digital power, and normative competition. It argues that cyberspace has evolved into a strategic domain in which states reinterpret sovereignty, accumulate technological capabilities as instruments of influence, and compete to shape global digital norms. The study analyzes how national approaches to data governance, platform regulation, and cybersecurity reflect broader ideological and geopolitical divisions. It further explores the hybrid nature of digital power, where state and corporate actors jointly shape technological standards and global regulatory frameworks. The article concludes that cyberspace is characterized by a structural tension between fragmentation and interdependence, creating a complex environment in which authority, influence, and legitimacy are continuously renegotiated.

***Keywords*:** *cyberspace, cyber sovereignty, digital power, digital geopolitics, normative competition, data governance, cybersecurity, global digital governance*

**Elgiz Abdurahmanlı**
Azərbaycan Turizm və Menecment Universiteti
doktorant
https://orcid.org/0009-0002-3504-9974
abdurahmanli_e @mail.ru

# Kiberfəzanın geosiyasi arxitekturası: kiber suverenlik, rəqəmsal güc və normativ rəqabət

**Xülasə**

Bu məqalə kiberfəzanın geosiyasi arxitekturasını kiber suverenlik, rəqəmsal güc və normativ rəqabət anlayışlarının qarşılıqlı əlaqəsi çərçivəsində təhlil edir. Məqalədə əsaslandırılır ki, kiberfəza suverenliyin yenidən şərh olunduğu, texnoloji imkanların təsir aləti kimi toplandığı və qlobal rəqəmsal normaların formalaşdırılması uğrunda rəqabətin getdiyi strateji bir müstəviyə çevrilmişdir. Tədqiqat milli səviyyədə məlumatların idarə olunması, platforma tənzimlənməsi və kibertəhlükəsizlik sahəsində yanaşmaların daha geniş ideoloji və geosiyasi bölünmələri necə əks etdirdiyini araşdırır. Eyni zamanda, rəqəmsal gücün hibrid xarakteri təhlil olunur; burada dövlət və korporativ aktorlar birlikdə texnoloji standartların və qlobal normativ çərçivələrin formalaşmasında iştirak edirlər. Məqalədə nəticə olaraq göstərilir ki, kiberfəza fraqmentasiya ilə qarşılıqlı asılılıq arasında struktur gərginliklə səciyyələnir və bu mühitdə hakimiyyət, təsir və legitimlik daim yenidən müəyyən olunur.

***Açar sözlər:*** *kiberfəza, kiber suverenlik, rəqəmsal güc, rəqəmsal geopolitika, normativ rəqabət, məlumatların idarə olunması, kibertəhlükəsizlik, qlobal rəqəmsal idarəetmə*

## Introduction

Cyberspace has evolved from a technical communications infrastructure into a central arena of geopolitical contestation (Lobaslova, 2020). States no longer perceive digital networks merely as tools of economic modernization; rather, they treat them as strategic domains comparable to land, sea, air, and space. The geopolitical architecture of cyberspace is therefore shaped by three interrelated dynamics: cyber sovereignty, digital power, and normative competition. Together, these dimensions determine how authority is exercised, how influence is projected, and how rules are negotiated in the digital era.

This article analyses the structural components of cyberspace's geopolitical order, focusing on the transformation of sovereignty in the digital realm, the emergence of digital capabilities as instruments of power, and the ongoing competition over global cyber norms.

**Research**

*Cyber Sovereignty: Redefining Authority in the Digital Domain*. Traditional sovereignty rests on territorial control and the monopoly of legitimate authority within defined borders (Biersteker, 2013). Cyberspace challenges this Westphalian framework because digital networks transcend physical boundaries, enabling cross-border data flows and decentralized governance structures (Pierucci, 2025). In response, many states have advanced the concept of cyber sovereignty, asserting the right to regulate and control digital infrastructure, data flows, and online content within their jurisdictions.

Cyber sovereignty manifests in several policy instruments. These include data localization laws, national firewalls, domestic cloud infrastructure mandates, and state-controlled digital platforms (Prokopyshyn & Trushkina, 2025). Proponents – primarily state actors advocating cyber sovereignty, national security institutions, and digital industrial policy strategists – argue that such measures enhance national security, protect cultural identity, and safeguard economic interests. Critics – including multi-stakeholder internet governance advocates, liberal democratic policymakers, multinational technology firms, and civil society organizations – argue that excessive digital control contributes to internet fragmentation and undermines openness, interoperability, and innovation.

The tension between open internet governance and state-centred control reflects deeper ideological differences. Liberal democracies generally emphasize multi-stakeholder governance, transparency, and interoperability. Conversely, some states advocate for centralized governance models prioritizing state authority over digital infrastructure. As a result, cyberspace has become a contested domain where sovereignty is reinterpreted rather than abandoned.

*Digital Power: Technology as Strategic Capital*. Digital power refers to the capacity of states and corporations to shape global outcomes through technological superiority, data control, and cyber capabilities (Lorci, 2024). Unlike conventional military power, digital power operates across economic, informational, and cognitive dimensions.

Three core components define digital power:

First, technological innovation capacity. Leadership in artificial intelligence, semiconductor production, quantum computing, and advanced telecommunications provides strategic advantages. States that control critical technologies influence global supply chains and standards.

Second, data governance and platform dominance. Digital platforms accumulate vast amounts of user data, enabling predictive analytics, targeted communication, and algorithmic influence. Control over such data translates into economic leverage and soft power projection.

Third, cyber capabilities and resilience. Offensive cyber operations, cyber espionage, and critical infrastructure protection form part of modern strategic doctrine. Cyber deterrence has emerged as a complex and evolving concept, as attribution challenges complicate traditional deterrence models.

Digital power is not monopolized by states. Technology corporations function as geopolitical actors, shaping standards, controlling infrastructure, and influencing regulatory frameworks. This hybridization of power blurs the boundary between public and private authority, creating a multilayered governance structure.

*Normative Competition: The Struggle for Digital Rules*. Beyond infrastructure and capabilities lies the normative layer of cyberspace (Carr & Erskine, 2016). Competing visions of digital order shape international debates over data governance, privacy, cybersecurity, and information control (Mugamba, 2025).

Normative competition operates at three levels:

At the international level, states negotiate frameworks for responsible state behaviour in cyberspace, including norms on critical infrastructure protection and non-interference. However, consensus remains limited due to divergent political systems and security interests.

At the regional level, regulatory models influence global standards. Data protection regimes, cybersecurity directives, and digital market regulations often extend beyond territorial boundaries through extraterritorial application and market size effects.

At the domestic level, national legal frameworks embody ideological preferences regarding freedom of expression, surveillance, and digital rights. These domestic choices aggregate into broader normative blocs that compete for global legitimacy.

The result is a fragmented but interconnected normative environment in which digital standards are instruments of strategic influence (Arslan, 2025). States attempt to export their regulatory models through trade agreements, technological partnerships, and development initiatives.

*Fragmentation vs. Interdependence*. Despite increasing fragmentation, cyberspace remains structurally interdependent (Lambach, 2020). Global supply chains for hardware components, transnational data flows, and shared digital platforms create mutual vulnerabilities. Complete digital decoupling is economically costly and technically complex (Zhen, et al., 2022).

This duality – fragmentation alongside interdependence – defines the contemporary geopolitical architecture of cyberspace. States pursue autonomy in critical technologies while remaining embedded in global digital networks (Broeders, et al., 2023). Strategic competition thus unfolds within a framework of unavoidable connectivity.

*Implications for Global Governance*. The future of cyberspace governance will depend on the interaction between sovereignty claims, technological capabilities, and normative alignment (Kadlecová, 2024). Three potential trajectories can be identified:

One trajectory involves further fragmentation, leading to regionally bounded digital ecosystems with limited interoperability.

Another scenario envisions managed competition, where rival blocs coexist but maintain baseline coordination on cybersecurity and critical infrastructure protection.

A third possibility involves renewed multilateral engagement aimed at establishing universal digital norms and cooperative security frameworks.

The direction taken will significantly affect economic integration, innovation ecosystems, and geopolitical stability.

## Conclusion

The geopolitical architecture of cyberspace is defined by the interplay of cyber sovereignty, digital power, and normative competition. States reinterpret sovereignty to assert control over digital domains; they accumulate technological and data-driven capabilities as instruments of power; and they compete to shape global norms governing digital space.

Cyberspace is neither a borderless utopia nor a fully fragmented domain. It is a strategically contested environment where authority, influence, and legitimacy are continuously renegotiated. Understanding its architecture requires integrating legal, technological, economic, and geopolitical perspectives. As digital transformation deepens, cyberspace will remain a central arena in the reconfiguration of global power.

## References

1. Arslan, S. (2025). Strategic Approach to the Role of Normative Power and its Instruments in Eu Foreign Policy in the Digital Age: 2010–2025. *International Journal of Academic Research in Economics and Management Sciences*, *14*(4), 323–359.
2. Biersteker, T. J. (2013). State, sovereignty and territory. *Handbook of international relations*, 245–272.
3. Broeders, D., Cristiano, F., & Kaminska, M. (2023). In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of its Geopolitical Ambitions. *JCMS: Journal of Common Market Studies*, *61*(5), 1261–1280.
4. Carr, M. M., & Erskine, T. (2016). Beyond "Quasi-Norms": The Challenges and Potential of Engaging with Norms in Cyberspace. NATO Cooperative Cyber Defence Centre of Excellence.
5. Kadlecová, L. (2024). *Cyber Sovereignty: The Future of Governance in cCyberspace*. Stanford University Press.
6. Lambach, D. (2020). The Territorialization of Cyberspace. *International Studies Review*, *22*(3), 482–506.
7. Lobastova, S. (2020). Geopolitics of Cyberspace and Virtual Power. *Journal of Liberal Arts and Humanities*, *3*, 97–113.
8. Lorci, E. (2024). Assessing Power and Hierarchy in Cyberspace: An approach of Power Transition Theory. *Applied Cybersecurity & Internet Governance*, *3*(2), 7–37.
9. Mugamba, E. (2025). Global Data Governance in Digital Law: A Comparative Analysis of EU and Global Approaches to Cybersecurity Legislation. *Journal of Smart Computing and Quantum Technologies*, *1*(1), 1–19.
10. Pierucci, F. (2025). Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace. *Digital Society*, *4*(1), 27.
11. Prokopyshyn, O., & Trushkina, N. (2025). The Geopolitics of Cybersecurity: A Comparative Analysis of National Strategies for Digital Sovereignty. *Politics & Security*, *12*(2), 59–71.
12. Zhen, Y. A. N. G., Jin, C. H. E. N., & Jizhen, L. I. (2022). Global Value Chains in the Era of Digital Economy: Trends, Risks and Countermeasures. *Frontiers of Economics in China*, *17*(1).

Received: 05.11.2025
Approved: 13.02.2026