©Toshkent davlat sharqshunoslik universiteti 25-aprel,2026

STRATEGIC ANALYSIS OF DIGITAL PROTECTIONISM (IN THE CASE OF MIDDLE POWERS)

Firdavs Azimkulov
University of World Economy and Diplomacy
Faculty of International Relations 4th year student

Abstract. The idealistic vision of a borderless internet has been replaced by aggressive geopolitical disputes and a rise in digital protectionism. Through the lens of the “Weaponized Interdependence” theory, this paper explores how superpowers leverage vital digital infrastructure for strategic dominance and surveillance. This drive for digital sovereignty has fractured the global digital ecosystem via strict data localization laws, resulting in a tri-polar tech landscape dominated by the distinct regulatory and technological models of the United States, China, and the European Union. Consequently, developing nations and middle powers face a high-stakes security dilemma, prompting a strategic shift toward “hedging” rather than full integration into a single bloc. By diversifying tech dependencies and investing in sovereign Digital Public Infrastructure (DPI), these nations aim to preserve their digital autonomy. A specific examination of Uzbekistan illustrates this third way of digital diplomacy, highlighting the country’s successful efforts to build alternative financial networks, aggressively localize citizen data, and develop an independent e-government cloud. Ultimately, the paper concludes that digital protectionism is the new global standard where a nation’s security is fundamentally defined by its ability to regulate its data territory.

Keywords: digital data, localization, cloud infrastructure, hedging, tech sovereignty, digital ecosystem.

INTRODUCTION For decades, people have been assuming that the rise of the digital world would outgrow the physical borders of our maps and that national sovereignty would become a relic of the past. The unrestricted movement of data within a globalized digital environment was intended to spark a new age of total global unity through the free exchange of information. That idealistic dream has officially ended. Instead of removing global boundaries, the internet has become the main battlefield for aggressive geopolitical disputes.

LITERATURE REVIEW If we want to understand why the internet is breaking apart, it is crucial to look at the theory called “Weaponized Interdependence” [1]. This theory was pioneered by scholars Henry Farrell and Abraham Newman. They refute the idea that global interconnectedness leads only to harmony and instead argue that states with control of vital junctions (such as trade routes or digital infrastructure) can transform these links into instruments of leverage. When a superpower country dominates the world’s vital sectors, for instance, the United States, with its dominant cloud computing infrastructure, or China’s leadership in 5G equipment, it can weaponize these connections for surveillance or political pressure. Hence, countries are no longer willing to tolerate the vulnerabilities of an open web. Under the name of digital protectionism, they are fracturing the global ecosystem into distinct zones of national sovereignty.

RESULTS Data localization. In the past, trade wars were fought with tariffs on industrial materials, such as taxing physical commodities like fruit or coal. However, the modern era has shifted the situation and nowadays, the most important trade barriers are the laws that stop data from moving freely between countries.

Although these laws are frequently framed as measures for citizen privacy or enhanced cybersecurity, the real strategic objective is deeply rooted in geopolitical strategy. Localizing data is a defensive maneuver to block foreign surveillance and meanwhile forces big tech companies to submit to local regulations rather than international laws. Moreover, a primary goal of these policies is to counteract the legal leverage provided by the U.S. CLOUD Act [2]. This act allows U.S. law enforcement to access data globally as long as it is managed by an American provider.

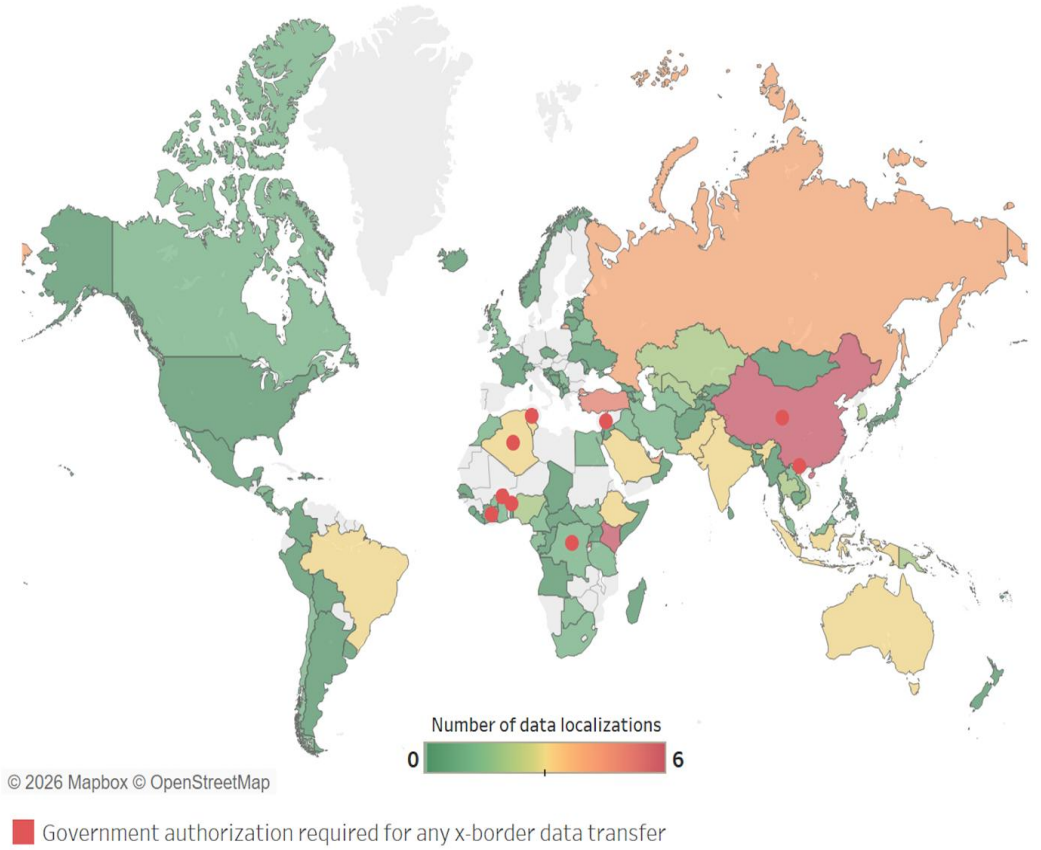
The Tri-Polar Splinternet. This drive for digital sovereignty has divided the global tech landscape into three separate geopolitical spheres competing for technological and regulatory dominance. The United States champions a market-hegemonic model. It pushes for minimal restrictions on data and emphasizes the expansion of global business. This strategy relies on the overwhelming global reach of American “hyperscalers” and tech leaders, such as Alphabet, Amazon and Microsoft [3]. However, the US actively leverages its control over the global tech stack by using export bans and sanctions as strategic weapons and plans to maintain its supremacy position [4].

China identified the risks of global interdependence in advance and thus Beijing shifted toward a sovereignty-first model to ensure total state control over its tech infrastructure. Unlike many Western nations that embraced the “borderless” myth, Beijing’s Great Firewall (initiated in the late 90s) was a direct response to this vulnerability and it was long before the term “weaponized interdependence” was coined. By using the Great Firewall and implementing strict Data Security Laws, China has built a closed digital ecosystem governed by state authority and sealed off its domestic internet from foreign influence. At this point, China is proactively encouraging partners to adopt Data Security Laws similar to China’s and assisting other nations to install fiber-optic cables, 5G antennas, and data centers through the Digital Silk Road initiative. [5]

The European Union – the fortress. The European Union has established a digital castle and since it does not have Silicon Valley of its own, it compensates for a lack of local tech giants by weaponizing legislation to shape the behavior of international companies in line with European values [6]. Legal structures such as the General Data Protection Regulation (GDPR), the Digital Markets Act (DMA) and local data storage mandates serve as regulatory barriers and they are designed to force American and Chinese platforms to submit to European rules.

This map of global data localization laws (Table 1) shows a clear picture of how the internet is splintering, breaking into pieces. A rising number of countries these days require (increasingly passing laws) that any data generated by their citizens be housed, handled, and

The Middle Power Dilemma. For developing nations and middle powers (particularly in regions like Central Asia or the Middle East, etc.), the breakup of the internet creates a high-stakes security dilemma. The division of the global digital ecosystem has forced middle powers into a precarious position. Indeed, choosing a tech pole is no longer just an economic decision for countries across the Global South. Because it risks alienating major global partners. If one state fully adopts either American or Chinese technology, it essentially means surrendering its own digital sovereignty. Ultimately, it results in dependence on state-linked hardware that may include backdoors or serve as a kill switch during a diplomatic crisis.



Source: World Bank Digital Trade Regulatory Readiness, 2025.
Notes: This map shows the number of data localization measures by country, highlighting those requiring government authorization for cross-border data transfers (red dots). For countries with a red dot, hover over the dot to view the details.

Table 1.

In response to superpower pressure, a new era – third way of digital diplomacy, is taking shape. Countries are now ‘hedging’ instead of full integration. In other words, they are stopping to put all of their data into one basket but diversifying to multiple global blocs. For instance, they might be using U.S. cloud services (AWS/Azure) for business, but Chinese 5G (Huawei) for telecommunications. Moreover, middle powers like the UAE or Singapore are constructing their own sovereign AI and data centers to act as neutral digital ground [7]. Singapore has committed over S$1 billion through 2029 to boost its sovereign AI capabilities. Singtel is building an AI grid of sustainable, liquid-cooled, and hyper-connected data centers and recently became a major stakeholder in control of data center operator STT GDC [8]. Singapore is partnering with neighbors (like Johor, Malaysia [9]) to expand AI capacity while ensuring data adheres to local, trusted standards. In 2026, nations are increasingly prioritizing Digital Public Infrastructure (DPI). They will enable middle powers to build independent payment systems and cloud facilities. For example, India’s Unified Payments Interface (UPI) has established itself as the world’s leading real-time payment system (which has been processing 18 billion transactions per month) and even surpassed the world-

renowned Visa system last year [10]. Through these types of initiatives, middle powers are effectively reducing their dependence on foreign-controlled proprietary systems.

Uzbekistan can be a good example to examine the middle power behavior in the current situation. Uzbekistan successfully created an independent financial network and unified its two main national payment systems, Humo and Uzcard. Instead of relying entirely on Western financial systems (SWIFT), Uzbekistan is building alternative global connections. Recently, the Central Bank of Uzbekistan and the National Payments Corporation of India (NPCI) have agreed to integrate Humo and Uzcard with India’s Unified Payments Interface (UPI). At the same time, Uzbekistan has deeply embedded Chinese financial tech into its infrastructure. The national network fully supports UnionPay across its ATMs and payment terminals.

Besides financial systems, Tashkent is aggressively localizing its data to protect state security. According to Article 27-1 of Uzbekistan’s “Law on Personal Data” (adopted 2021), any organization processing the personal information of Uzbek citizens must store that data on physical servers located inside the country [11]. In recent years, the state regulator (**Uzkomnazorat**) has used [12] this article to restrict access to major services like Skype, Twitter, and TikTok when they failed to transfer their data to local facilities. This legal requirement forces both domestic and foreign companies to respect the nation's digital borders. Furthermore, in order to facilitate data localization continuously in the future, the government relies on a single state tech agency, Uzinfocom, to build and manage a completely independent e-government cloud. This cloud network runs the critical national infrastructure of the country, such as the my.gov.uz portal, the MyID biometric system, and digital healthcare databases.

CONCLUSION

The dream of a unified World Wide Web has vanished and it turned into multiple divided digital landscape. Every intra-state connection is a potential front line in a tech war. It seems that throughout this 21st century, digital protectionism will be the global standard. In this new world order, security is measured by the height of a nation’s digital walls. The idealistic vision of a borderless internet has largely given way to aggressive geopolitical maneuvering. In other words, the security of a nation will be defined by its ability to restrict and regulate its data territory.]

LIST OF REFERENCES

1. Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. International Security, 44(1), 42–79. Retrieved from https://doi.org/10.1162/isec_a_00351
2. U.S. Department of Justice. (2023, October 24). Criminal Division | CLOUD Act resources. Retrieved from https://www.justice.gov/criminal/cloud-act-resources
3. Xenoss. (2024). Hyperscale data center. Xenoss AI and Data Glossary. Retrieved from https://xenoss.io/ai-and-data-glossary/hyperscale-data-center
4. International Trade Administration. (2026). U.S. export controls. U.S. Department of Commerce. Retrieved February 26, 2026, from Retrieved from https://www.trade.gov/us-export-controls
5. Erie, M. S., & Streinz, T. (2021). The Beijing effect: China’s ‘Digital Silk Road’ as transnational data governance. New York University Journal of International Law and Politics, 54(1), 1–92.

6. EU asserts ‘sovereign right’ to regulate tech after Trump threat. (2025, August 26). The Straits Times. Retrieved from https://www.straitstimes.com/world/europe/eu-asserts-sovereign-right-to-regulate-tech-after-trump-threat
7. Benito, A. (2025, December 29). Middle East tech trends 2026: AI, cyber security and sovereign infrastructure take centre stage. Computer Weekly. Retrieved from https://www.computerweekly.com/news/366636636/Middle-East-tech-trends-2026-AI-cyber-security-and-sovereign-infrastructure-take-centre-stage
8. Ngui, Y., & Nair, R. (2026, February 4). KKR, Singtel pay $5.2 billion for full control of data centre operator STT GDC. Reuters. Retrieved from https://www.reuters.com/business/media-telecom/kkr-singtel-consortium-pay-52-billion-take-full-control-stt-gdc-2026-02-04/
9. Lin, T. (2025, November 12). The Singapore-Johor AI Corridor: A sandbox for U.S.-China tech coopetition and model for cross-border digital cooperation? Technode Global. Retrieved from https://www.technode.global/2025/11/12/the-singapore-johor-ai-corridor-a-sandbox-for-u-s-china-tech-coopetition-and-model-for-cross-border-digital-cooperation/
10. News18. (2025, July 21). India’s UPI surpasses Visa to become world’s top real-time payment system: IMF. Retrieved from https://www.news18.com/business/banking-finance/indias-upi-surpasses-visa-to-become-worlds-top-real-time-payment-system-imf-ws-lo-9453091.html
11. Law of the Republic of Uzbekistan “On Personal Data”, LRU-547. (2019). Lex.uz. Retrieved from https://www.lex.uz/docs/4831939
12. Uzbekistan blocks Twitter, TikTok and VKontakte. (2021, July 5). Tashkent Times. Retrieved from https://tashkenttimes.uz/national/7168-uzbekistan-blocks-twitter-tiktok-and-vkontakte