Digital Disintegration: Techno-Blocs and Strategic Sovereignty in the AI Era

Stephen Weymouth

McDonough School of Business, Georgetown University, Washington, DC, USA
Email: stephen.weymouth@georgetown.edu

Abstract States are reshaping the global digital economy to assert control over the artificial intelligence (AI) value chain. Operating outside multilateral institutions, they pursue measures such as export controls on advanced semiconductors, infrastructure partnerships, and bans on foreign digital platforms. This digital disintegration reflects an elite-centered response to the infrastructural power that private firms wield over critical AI inputs. A handful of companies operate beyond the reach of domestic regulation and multilateral oversight, controlling access to technologies that create vulnerabilities existing institutions struggle to contain. As a result, states have asserted strategic digital sovereignty: the exercise of authority over core digital infrastructure, often through selective alliances with firms and other governments. The outcome is an emergent form of AI governance in techno-blocs: coalitions that coordinate control over key inputs while excluding others. These arrangements challenge the liberal international order by replacing multilateral cooperation with strategic—and often illiberal—alignment within competing blocs.

States are restructuring the global digital economy as they seek control over the artificial intelligence (AI) value chain. Operating outside multilateral institutions, they pursue measures such as export controls on advanced semiconductors, infrastructure partnerships, and outright bans on foreign digital platforms. Why has this fragmentation emerged, and what explains its form? This essay advances an elite-centered explanation: digital disintegration stems from state efforts to confront the power of private AI firms. A handful of companies dominate critical AI inputs, including advanced chips, compute, and foundational models.[1] States' attempts to address this dominance are splintering the digital order.

The authority of leading AI firms lies outside state control. It is infrastructural power: private authority derived from control of AI's technical foundations. Such command over advanced technologies produces vulnerabilities that the postwar

1. *Compute* refers to the specialized processing capacity for training and running AI models. I use *critical AI inputs* to denote the core components of the AI value chain. As a general purpose technology, AI is central to advances across most industries.

International Organization 79, Supplement 2025, pp. S57–S70
© The Author(s), 2025. Published by Cambridge University Press on behalf of The IO Foundation. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.
doi:10.1017/S0020818325101070

https://doi.org/10.1017/S0020818325101070 Published online by Cambridge University Press

liberal international order[2]—designed to discipline states rather than firms—is ill-equipped to manage.[3] As a result, governments are moving to contain this infrastructural power, reshaping digital governance around questions of sovereignty.

These developments revive debates about the impact of technology and globaliza- tion on state authority. Scholars have long examined the effects of interdependence on sovereignty,[4] with more recent emphasis on hybrid forms incorporating firms and international organizations.[5] Following the rise of the Internet, states pursued digital sovereignty by governing cross-border information flows, producing competing models of digital governance.[6] Recent scholarship extends this to AI, emphasizing how authority increasingly rests on control of critical inputs.[7] This essay explains state responses to AI infrastructural power, and their implications for the liberal international order.

I call these responses *strategic digital sovereignty*: the exercise of state authority over core digital infrastructure, undertaken unilaterally or through selective alliances. The aim is to constrain the power of private firms and contain the political, security, and economic vulnerabilities created by firms' control of key inputs. Strategic digital sovereignty often takes the form of *techno-blocs*—selective alliances that embed firms in state-led governance of AI infrastructure.

These alliances coordinate AI governance outside the reach of established international institutions. They replace rules-based multilateralism with strategic, often illiberal, alignment within competing blocs. Existing scholarship on superstar firms shows that the largest and most productive multinational corporations have traditionally promoted openness, lobbying and building networks in support of global supply chains.[8] Unlike earlier multinationals that favored openness, the superstar firms at the frontier of AI increasingly align with governments for strategic, sometimes protectionist, purposes. Techno-blocs now anchor the emerging digital order.

Digital Warlords: Private Authority Over AI

A handful of firms now dominate the technologies that support advanced AI. I call them *digital warlords* because they operate outside the boundaries of domestic regulation and multilateral oversight, setting the terms for who may access advanced AI technologies and under what conditions. Their power rests on their expertise and control over critical inputs such as advanced chipmaking (Nvidia,

2. This refers to multilateral organizations regulating trade and other commercial interactions, anchored in the GATT/WTO.

3. Bacchus 2022; Slaughter and McCormick 2021.

4. Keohane and Nye 1973; Krasner 1999; Sassen 1996.

5. Srivastava 2022; see also Büthe and Mattli 2011 on private regulatory authority.

6. Bradford 2023; De Gregorio and Radu 2022; Chander and Sun 2023; Couture and Toupin 2019; Farrell and Newman 2019a; Floridi 2020; Goldsmith and Wu 2006; Hulvey and Simmons 2025; Liu 2021; Simmons and Hulvey 2022; Weymouth 2023.

7. Aaronson 2025; Ishkhanyan 2025; Krishnamurthy 2025; Srivastava 2023; Veale, Matus, and Gorwa 2023.

8. Baccini, Pinto, and Weymouth 2017; Jensen, Quinn, and Weymouth 2015; Johns and Wellhausen 2016; Kim 2017; Kim et al. 2019; Kim and Milner 2021; Milner 1988; Osgood 2017; Osgood et al. 2017; Peters 2017; Wellhausen 2015; Zhang 2025.

https://doi.org/10.1017/S0020818325101070 Published online by Cambridge University Press

TSMC, ASML),[9] compute (Azure, Google Cloud, AWS, Alibaba Cloud), and frontier model development (OpenAI, Anthropic, DeepSeek). Unlike traditional multinationals, whose influence derives from lobbying, employment, or production, digital warlords exercise authority primarily through infrastructural control.[10] This authority makes them gatekeepers of the AI economy.

Like historical warlords, they thrive where institutional authority is weak. Their competition centers on scarce resources like chips, talent, energy, capital, favorable policy, and market access. They do not govern populations by force, but their authority over strategic technologies gives them a warlord-like position in the digital economy, which states must confront. As with historical warlords, states may attempt to contain or co-opt their authority, but they remain independent centers of power that governments cannot fully control.

Their authority is embedded in the value chains that shape the digital economy. I refer to this as infrastructural AI power: the capacity of private firms to govern access to AI systems through control over their technical foundations.[11] For instance, Nvidia supplies 92 percent of data center GPUs,[12] and TSMC produces 65 percent of the world's foundry output.[13] Their platforms set standards and determine access. Nvidia's Compute Unified Device Architecture (CUDA) is a proprietary programming interface. It has become the de facto industry standard for AI development, a unilateral rule-making power that entrenches Nvidia's dominance. OpenAI similarly restricts access to its most advanced systems through usage and licensing terms. Like CUDA, these are privately enforced rules with global reach. Through these rules, firms can determine the terms of participation in the AI economy. Digital warlords exercise this infrastructural control largely independent of sovereign oversight.

Their infrastructural power grants them geopolitical significance. States depend on advanced AI for strategic purposes like military applications and to expand state capacity (for example, digital public infrastructure such as India Stack),[14] but private firms control its development. These private actors perform consequential functions, from moderating platform content to controlling global connectivity through proprietary submarine cables and cloud infrastructure. In this new era, leading firms operate as geopolitical actors in their own right, shaping not only markets but also the strategic decisions of states.[15] Given this leverage, these digital warlords engage in transactional cooperation, granting access to advanced systems in return for essential resources such as low cost energy or data center investments. The core externality is

9. On the geopolitics of microchip production, see Miller 2022.

10. DeNardis and Hackl 2015; Musiani 2022; Kak, West and Whittaker 2023.

11. This definition builds on Kemmerling and Trampusch 2023 and their concept of digital power resources. On how economic scale contributes to platform power, see Culpepper and Thelen 2020 and Girard 2024. In contrast, Mann 1984 defined infrastructural power as the capacity of states to organize society through administrative means. Farrell and Newman 2019b, 2023 show how states convert network centrality into coercive leverage.

12. IOT Analytics, The Leading Generative AI Companies, available at <https://iot-analytics.com/leading-generative-ai-companies/>.

13. Trendforce, 4Q24 Global Top 10 Foundries Set New Revenue Record. Available at <https://www.trendforce.com/presscenter/news/20250310-12510.html>.

14. Alonso et al. 2023.

15. Bremmer 2021; Lehdonvirta 2024.

https://doi.org/10.1017/S0020818325101070 Published online by Cambridge University Press

that this authority lies outside state control, creating political, security, and economic vulnerabilities. Social media giants shape the information environment in ways that states increasingly view as politically consequential. Governments now frame such risks in national security terms, as illustrated by US legislation banning TikTok or China's "Delete America" campaign.[16] Dual-use AI technologies raise further security concerns, as commercial models may be repurposed for drone applications or cyber warfare.[17] Economically, digital firms shift profits across jurisdictions by exploiting the mobility of intangible assets, eroding national tax bases.[18] These fault lines emerge from the imbalance between digital warlords' capacity to innovate and states' capacity to restrain.

These externalities are politically salient because they expose institutional limitations—states cannot fully internalize them.[19] Regulation is inadequate, and prior social compacts inapplicable. Embedded liberalism, as originally conceived, assumed that governments could compensate those who lost out from globalization through redistribution and domestic regulation.[20] That model presumes globalization's economic harms occur within national borders. Redistributive measures, like trade adjustment assistance, could at least in principle address labor market shocks.[21] But the fallout from digital warlords escapes these tools. Redistribution is no remedy when the threat is to sovereign authority itself.

The Limits of Multilateral Trade Rules in the Digital Economy

The liberal economic order is inadequate to govern the digital economy for two reasons. First, it lacks mechanisms to constrain the infrastructural power of digital warlords. Second, it struggles to discipline the sovereignty strategies that states adopt in response to the growing capabilities and externalities of these firms.

The multilateral trade regime was designed to govern the flow of goods and, later, traditional services. It has been slow to address digital services, and has not evolved to discipline AI infrastructure. Its rules rely on outdated categories, such as the distinction between goods and services or the modes of service supply, that are increasingly incoherent in the digital context.[22] Take robotics: AI systems like large language models and image recognition tools are now embedded in humanoid robots that provide services. Yet these machines are also physical goods. Such hybrid forms expose the limitations of the regime's path dependent rules, designed for an analog economy.

16. "Delete A" is an informal label for China's state-led effort to reduce dependence on US firms.
17. Horowitz 2020. Oppenheimer 2025 shows how digital interdependence creates cybersecurity externalities that states struggle to manage.
18. Djankov 2021; Weymouth 2023.
19. In contrast, states are often assumed to control the assets generating cross-border externalities and able to design institutions to manage them Keohane 1984.
20. Ruggie 1982. Mansfield and Rudra 2021 show how the digital revolution has eroded the domestic foundations of embedded liberalism, weakening state capacity to redistribute.
21. On the responsiveness of TAA, see Kim and Pelc 2021.
22. Azmeh, Foster, and Echavarri 2020; Bacchus 2022; World Trade Organization 2024.

https://doi.org/10.1017/S0020818325101070 Published online by Cambridge University Press

To be sure, some WTO instruments cover aspects of the digital economy. The General Agreement on Trade in Services (GATS) applies to cross-border digital services when commitments have been scheduled.[23] TRIPS protects the intellectual property of AI firms. And the Joint Statement Initiative on E-commerce (JSI), launched in 2017, seeks to liberalize digital trade through provisions on data localization and source code disclosure.[24] Yet most of these rules serve to empower digital warlords rather than constrain them. The limited attempts to protect state regulatory sovereignty, such as exceptions for privacy and security, remain legally and politically contested.

The global tax regime reveals a similar institutional failure. Rooted in the early twentieth-century economy, the system was designed to tax profits based on the location of physical production. But digital firms generate income from intangible assets, often without any physical presence. Firms further exploit these gaps by shifting profits to low-tax jurisdictions, eroding national tax bases.[25] With OECD-led tax reforms stalled, states have pursued unilateral digital services taxes,[26] another sovereignty measure that reflects the inability of multilateral institutions to address digital externalities.

The rise of digital services taxes underscores the second deficiency of the liberal international order: it lacks effective tools to discipline how states respond to firms' infrastructural power. Additional policies such as data localization mandates, platform bans, and semiconductor export controls fall largely outside WTO disciplines or are shielded by national security exceptions. Even when trade agreements do apply, enforcement is weak and tariff-based retaliation mechanisms are poorly suited to digital restrictions.

In sum, international institutions lack the capacity to constrain either the activities of digital firms or the sovereignty strategies their capabilities provoke. The liberal trade regime was built to discipline states. But as firm power increasingly threatens state authority, governments are reasserting control through ad hoc and at times illiberal measures. In the absence of effective global rules to manage either firm power or state responses, strategic digital sovereignty has emerged as the dominant mode of digital governance.

Strategic Digital Sovereignty and Techno-Blocs

Without effective multilateral rules, states are devising their own strategies to control the AI value chain. They pursue what I call *strategic digital sovereignty*: the exercise

23. Members continue to dispute technological neutrality, the idea that commitments to services liberalization apply to digitally delivered services Bacchus 2022.

24. Under the Biden administration, the United States withdrew support for core liberalizing provisions in the JSI, reflecting growing skepticism of multilateral disciplines that limit domestic digital "policy space." See "USTR Upends US Negotiating Position on Cross-Border Data Flows," CSIS, available at <https://www.csis.org/analysis/ustr-upends-us-negotiating-position-cross-border-data-flows>.

25. Arel-Bundock and Blais 2023 find consistent public support for multinational tax reform.

26. OECD 2018; Gelepithis and Hearson 2022; Heering, Crasnic, and Newman 2025.

https://doi.org/10.1017/S0020818325101070 Published online by Cambridge University Press

of state authority over core digital infrastructure through unilateral actions or selective alliances with firms and other governments. It is *strategic* in two respects. First, it is pragmatic: rather than formal institutions rooted in shared liberal values, states rely on flexible partnerships to secure or influence access to essential infrastructure. Second, it is geopolitical: sovereignty is projected outward to manage dependencies and externalities that cross borders.

States pursue strategic digital sovereignty through two nonmutually exclusive modes: unilateral measures and techno-bloc formation. Unilateral measures—such as export controls, data localization mandates, digital services taxes, and platform bans—aim to reduce strategic vulnerabilities and constrain firm power. Yet unilateralism cannot overcome material constraints. Because compute, talent, energy, and capital are globally dispersed, even powerful states must rely on partnerships to build AI capacity and address strategic vulnerabilities.

To that end, states form techno-blocs, aligning with firms and other governments to overcome these constraints and extend authority over private AI infrastructure. Within blocs, states contribute critical inputs and relax barriers in exchange for access to markets and advanced technologies. Techno-blocs differ from traditional state alliances in that they embed dominant AI firms directly into governance arrangements, turning critical AI inputs into leverage. They manage the externalities of infrastructural power by constraining it or co-opting it. Blocs themselves are not mutually exclusive: states may participate in several at once, perhaps joining one centered on compute partnerships while also joining another organized around energy cooperation or regulatory harmonization.

These arrangements are broadly beneficial to their participants. For firms, blocs deliver market access, resources, and regulatory stability, reinforcing their dominance at the frontier of AI. For policymakers, they are instruments to reassert sovereignty where unilateral measures fall short, demonstrating competence and securing access to advanced technologies in ways that may enhance political survival.

Although sovereignty is often framed as unilateral control, techno-blocs reflect a cooperative form. States selectively align with others to establish authority over AI where unilateral measures are inadequate.[27] Techno-blocs align incentives and coordinate governance across jurisdictions, addressing vulnerabilities that unilateral tools alone cannot overcome.

States combine unilateral and bloc strategies in different ways. One prominent variant is *AI mercantilism*, which uses trade policy to secure national control over the AI stack. The United States and China both pursue this approach, combining export controls with industrial policies to build domestic capacity while constraining rivals.[28] It reflects a mercantilist logic: securing control over critical AI inputs while excluding others to preserve national advantage.

27. Sovereignty is often pooled or delegated, as states limit authority to achieve strategic aims. See, for example, Krasner 1999; Keohane 2002; Lake 2003. Srivastava 2022 shows that private actors can perform functions traditionally associated with state sovereignty.

28. In the United States these controls cover advanced semiconductors and cloud services, while in China they have focused more on strategic raw materials.

https://doi.org/10.1017/S0020818325101070 Published online by Cambridge University Press

In contrast, smaller states like the UAE and Saudi Arabia pursue *alignment strategies*, offering critical inputs such as capital, energy, or regulatory flexibility in exchange for integration into techno-blocs. A third variant is advanced by the European Union, which pursues *regulatory sovereignty*, using EU market access to globalize its legal standards for data and AI. The remainder of this section examines in greater detail how states implement these strategies in practice.

The United States blends unilateral action with techno-blocs in a form of AI mercantilism that constrains adversaries and secures technological access. In October 2022, the Biden administration imposed sweeping controls to restrict China's access to advanced AI technologies, including limits on high-end chip exports and US involvement in Chinese AI development. These controls expanded to other countries in 2023 and 2024, culminating in the AI Diffusion Rule, which established a tiered framework for licensing requirements on exports of advanced chips and cloud services. The rule classified countries based on their alignment with US national security interests, imposing stricter export controls on those in lower tiers. Countries such as Saudi Arabia and the UAE were placed in restrictive tiers, limiting their access to high-end AI hardware and services.[29] While formally unilateral, these measures were coordinated with allies such as the Netherlands and Japan, embedding export controls within a broader techno-bloc.[30]

The recent Gulf partnerships with the United States exemplify bloc-based approaches by smaller states. In return for access to leading Nvidia chips, Emirati authorities agreed to adopt US technology security standards, while offering to finance infrastructure and supply low cost energy for AI systems.[31] The deal includes a large compute campus in Abu Dhabi, operated by US cloud providers and the Emirati firm G42.[32] A parallel alignment is underway in Saudi Arabia. A consortium of US firms (Google, Oracle, Salesforce, AMD, Uber) and Saudi-backed DataVolt announced USD 80 billion in joint AI projects, including $20 billion for US-based data centers.[33] Nvidia also agreed to supply chips to Humain, a Saudi firm, under terms involving chip access and joint infrastructure investments.[34]

29. US Department of Commerce 2023; Heim 2025.

30. To be sure, many techno-blocs form among states with prior geopolitical alignment. But advanced firm capabilities, such as those of ASML (Netherlands) and Tokyo Electron (Japan) in the microchip value chain, shape these alignments.

31. US Department of Commerce, "UAE/US Framework on Advanced Technology Cooperation," available at <https://www.commerce.gov/news/press-releases/2025/05/uae/us-framework-advanced-technology-cooperation>.

32. Federico Maccioni, Manya Saini, and Yousef Saba, "UAE to Build Biggest AI Campus Outside US in Trump Deal, Bypassing Past China Worries," Reuters, 15 May 2025, <https://www.reuters.com/world/china/uae-set-deepen-ai-links-with-united-states-after-past-curbs-over-china-2025-05-15/>.

33. Max A. Cherney and Stephen Nellis, "US Tech Firms Nvidia, AMD Secure AI Deals as Trump Tours Gulf States," Reuters, 14 May 2025, available at <https://www.reuters.com/world/middle-east/saudi-arabia-partners-with-nvidia-spur-ai-goals-trump-visits-2025-05-13/>.

34. "Saudi Arabia and NVIDIA to Build AI Factories to Power Next Wave of Intelligence for the Age of Reasoning," Nvidia Newsroom, 13 May 2025, available at <https://nvidianews.nvidia.com/news/saudi-arabia-and-nvidia-to-build-ai-factories-to-power-next-wave-of-intelligence-for-the-age-of-reasoning>.

https://doi.org/10.1017/S0020818325101070 Published online by Cambridge University Press

China's model of strategic digital sovereignty combines unilateral control at home with techno-bloc formation abroad. Domestically, Beijing asserts authority over private technology firms through mandated alignment with national priorities.

Chinese authorities use laws governing data storage and cross-border flows[35] to scrutinize the activities of foreign and domestic firms when their influence threatens state control over the information environment.[36] Together, these efforts assert state authority over AI infrastructure.

Like the United States, China pursues strategic digital sovereignty abroad through AI mercantilism, treating advanced technologies as strategic assets. The Digital Silk Road bundles cloud services, fiber-optic infrastructure, surveillance platforms, and e-government tools into Belt and Road Initiative projects.[37] It extends beyond physical infrastructure to cloud networks. A recent study identifies ninety-seven Chinese cloud zones in thirty-seven partner countries, especially where trade ties are strong or states participate with China in regional arrangements such as the Shanghai Cooperation Organization.[38] Chinese technology exports often bundle digital governance tools such as biometric ID systems with cloud services, embedding Chinese surveillance technologies in partner states. For example, Huawei's Safe City project in Islamabad integrates facial recognition and real time suspect tracking into local security systems.[39] China's digital infrastructure exports deepen partner dependence while advancing its model of digital authoritarianism.[40]

Rather than AI mercantilism, the European Union anchors its techno-bloc in regulatory sovereignty, using its market size to globalize EU standards for digital governance. It establishes influence through legal frameworks such as the General Data Protection Regulation (GDPR), the Digital Markets Act (DMA), and the AI Act.[41] This approach reinforces norms of consumer protection but relies on extraterritorial regulation rather than multilateral institutions. The AI Act, for example, applies to any company offering AI systems to EU users, regardless of location. This strategy trades access for compliance within a regulatory techno-bloc anchored in European norms.[42] With few dominant firms in the AI stack, the EU converts market access into authority by embedding firms in its regulatory bloc through legal conditionality.

35. These include the Cybersecurity Law (2017), Data Security Law (2021), and the Personal Information Protection Law (2021) Creemers 2022.

36. Dragu and Lupu 2021. Liu 2024 shows that the Chinese government initially allowed E-commerce platforms to fill institutional voids but later pursued antitrust crackdowns as their influence grew. On the distributional consequences of autocratic digital surveillance, see Sun 2024.

37. Erie and Streinz 2021.

38. Lehdonvirta, Wu, and Hawkins 2025.

39. "China Eximbank Provides RMB 850 Million Government Concessional Loan for Safe City Islamabad Project," AIDDATA, available at <https://china.aiddata.org/projects/37016/>.

40. Heeks et al. 2024.

41. The GDPR establishes rules for data protection and privacy. The DMA constrains the control of "gatekeeper" firms over digital infrastructures. The AI Act classifies AI applications in risk tiers, prohibiting those deemed highest risk.

42. Bradford 2023; Csernatoni 2025.

https://doi.org/10.1017/S0020818325101070 Published online by Cambridge University Press

Within this framework, some member states pursue distinct techno-blocs. France, for instance, extends the EU's model by promoting an "AI Third Way," a sovereign alternative to both US and Chinese dominance in AI. Its strategy combines domestic investment in data centers (jointly financed by the UAE investment fund MGX) with the development of domestic platforms like Mistral Compute.[43] Reflecting its position in the AI stack, this approach pursues unilateral AI development within the EU techno-bloc. Likewise, Germany is developing a sovereign AI system for public services, built in partnership with OpenAI but hosted in the cloud of SAP, a German firm.[44] This approach draws on OpenAI's capabilities while complying with national data security and regulatory requirements.

In sum, states are fragmenting the digital order, producing rival centers of technological authority. Digital sovereignty strategies reflect states' geopolitical alignments, institutions, and positions in the AI stack. Each strategy, however, seeks to manage vulnerabilities created by private firms' control of key inputs.

Implications for the Liberal International Order

The pursuit of strategic digital sovereignty is reshaping the liberal international order. Techno-blocs often embed digital warlords in governance, elevating them from subjects of regulation to strategic partners. The result is illiberal alignment: opaque rather than transparent, transactional rather than rules based, exclusive rather than universal. Some sovereignty initiatives still pursue liberal aims like protecting privacy or banning high-risk AI applications. The EU exemplifies this approach, using legal frameworks to discipline firms. Yet this remains an exception, and may come at the cost of limiting the capacity to develop advanced systems.

The consequences of techno-bloc competition go beyond the splintering of the digital order. Techno-blocs create a hierarchy in which a few states and firms control the AI frontier, while others are relegated to subordinate roles with more limited sovereignty.[45] These arrangements extend beyond technical dependence. In some ways, they resemble extractive institutions of the past. In what has been called digital colonialism,[46] dominant firms extract and monetize data, while contributing little in tax revenue or employment. This could lead to rising inequality across states as digital warlords consolidate their economic dominance.

Such outcomes raise the question of whether AI will follow the trajectory of earlier technological shocks, or whether its features make it a distinct challenge.

43. Chavez 2025.
44. "SAP and OpenAI to Deliver Sovereign AI Solutions in Germany," Yahoo Finance, 25 September 2025, available at <https://finance.yahoo.com/news/sap-openai-deliver-sovereign-ai-100708451.html>.
45. On hierarchy in international relations, see Lake 2011.
46. Kwet 2019; Couldry and Mejias 2019; Rondeaux 2025.

https://doi.org/10.1017/S0020818325101070 Published online by Cambridge University Press

Previous infrastructural advances, such as electricity or telecom, were eventually brought under international regimes or subject to regulated monopolies. Like those earlier cases, AI is a general purpose technology. But its combination of features makes it harder for states to contain. AI innovation has outpaced the capacity of institutions to adapt. The mobility of intangible assets and AI-enabled digital services complicate the establishment of rules for trade and taxation. And its dual use features combine economic and security capabilities in ways rivaled perhaps only by nuclear technology. AI thus represents a technological exception, with features that make multilateral solutions especially difficult to achieve.

Crucially for international cooperation, AI also represents a systemic catalyst. It is accelerating a fragmentation of the international order in which authority over technological infrastructure becomes a central axis of division.

Despite growing fragmentation, alternative approaches to digital governance are emerging. Scholars have advocated models that disperse authority across multiple levels of governance, rather than within hierarchical blocs,[47] building on broader insights from the institutional complexity literature.[48] And international institutions themselves are developing models of transparency and regulatory convergence. For instance, the WTO promotes early notification of AI regulations to manage cross-border frictions, and a new emerging technologies unit builds negotiator capacity.[49] Other initiatives, such as the US–EU Trade and Technology Council[50] and OECD work on multinational tax reform, remain limited but show that international coordination has not disappeared entirely.

For international organizations to play a meaningful role, however, they would need to evolve beyond their original design. Existing trade and tax institutions were built to discipline states, not firms that control AI infrastructure. Constraining digital warlords would require new mandates: oversight of data flows and privacy, transnational competition rules, and mechanisms to tax digital revenues at their source.[51] The initiatives noted before point in this direction but lack the necessary authority and scope.

The stakes are profound. As states prioritize control over core digital technologies, the liberal international order risks becoming a relic of the analog era. Unless institutions evolve to constrain infrastructural power and coordinate governance, unilateral barriers and techno-blocs will entrench illiberal fragmentation. AI governance is emerging as a central axis of international politics, accelerating the shift from cooperation under rules to competition over the world's most consequential technologies.

47. Ishkhanyan 2025; Krishnamurthy 2025; Olugbade 2025; Schmitt 2022.
48. Alter and Meunier 2009; Abbott, Green, and Keohane 2016.
49. World Trade Organization 2024.
50. Young 2024; Birchfield 2024.
51. Weymouth 2023 describes this as the digital globalization "paradox": sustaining cross-border digital integration requires coordinated regulation of dominant firms, not just coordinated liberalization. See also World Trade Organization 2024, which highlights risks of regulatory fragmentation in AI governance.

https://doi.org/10.1017/S0020818325101070 Published online by Cambridge University Press

References

Aaronson, Susan Ariel. 2025. The Dangers of AI Nationalism and Beggar-Thy-Neighbour Policies. *Journal of World Trade* 59 (3):397–430.

Abbott, Kenneth W., Jessica F. Green, and Robert O. Keohane. 2016. Organizational Ecology and Institutional Change in Global Governance. *International Organization* 70 (2):247–27.

Alonso, Cristian, Tanuj Bhojwani, Emine Hanedar, Dinar Prihardini, Gerardo Uña,and Kateryna Zhabska. 2023. *Stacking up the Benefits: Lessons from India's Digital Journey.* International Monetary Fund.

Alter, Karen J., and Sophie Meunier. 2009. The Politics of International Regime Complexity. *Perspectives on Politics* 7 (1):13–24.

Arel-Bundock, Vincent, and André Blais. 2023. Where Should Multinationals Pay Taxes? *International Studies Quarterly* 67 (2):sqad012.

Azmeh, Shamel, Christopher Foster, and Jaime Echavarri. 2020. The International Trade Regime and the Quest for Free Digital Trade. *International Studies Review* 22 (3):671–92.

Bacchus, James. 2022. *Trade Links: New Rules for a New World*. Cambridge University Press.

Baccini, Leonardo, Pablo M. Pinto, and Stephen Weymouth. 2017. The Distributional Consequences of Preferential Trade Liberalization: Firm-Level Evidence. *International Organization* 71 (2):373–95.

Birchfield, Vicki L. 2024. From Roadmap to Regulation: Will There Be a Transatlantic Approach to Governing Artificial Intelligence? *Journal of European Integration* 46 (7):1053–71.

Bradford, Anu. 2023. *Digital Empires: The Global Battle to Regulate Technology.* Oxford University Press.

Bremmer, Ian. 2021. The Technopolar Moment: How Digital Powers Will Reshape the Global Order. *Foreign Affairs* 100 (6):112–28.

Büthe, Tim, and Walter Mattli. 2011. *The New Global Rulers: The Privatization of Regulation in the World Economy.* Princeton University Press.

Chander, Anupam, and Haochen Sun. 2023. *Data Sovereignty: From the Digital Silk Road to the Return of the State*. Oxford University Press.

Chavez, Pablo. 2025. France Pursues an AI "Third Way": Sovereignty Emerged As a Core Theme of the Paris AI Action Summit. Is It a Viable Strategy? *Bandwidth* (Center for European Policy Analysis), 13 February 2025. <https://cepa.org/article/france-pursues-an-ai-third-way/>.

Couldry, Nick, and Ulises A. Mejias. 2019. The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism. In *The Costs of Connection*. Stanford University Press.

Couture, Stéphane, and Sophie Toupin. 2019. "What Does the Notion of "Sovereignty" Mean When Referring to the Digital?" *Politics and Governance* 7(4):6–18.

Creemers, Rogier. 2022. "China's Emerging Data Protection Framework." *Journal of Cybersecurity* 8(1): tyac011.

Csernatoni, Raluca. 2025. The EU's AI Power Play: Between Deregulation and Innovation. Carnegie Europe <https://carnegieendowment.org/research/2025/05/the-eus-ai-power-play-between-deregulation-and-innovation?lang=en>.

Culpepper, Pepper D., and Kathleen Thelen. 2020. Are We All Amazon Primed? Consumers and the Politics of Platform Power. *Comparative Political Studies* 53 (2):288–318.

De Gregorio, Giovanni, and Roxana Radu. 2022. Digital Constitutionalism in the New Era of Internet Governance. *International Journal of Law and Information Technology* 30 (1):68–87.

DeNardis, Laura, and Andrea M. Hackl. 2015. Internet Governance by Social Media Platforms. *Telecommunications Policy* 39 (9):761–70.

Djankov, Simeon. 2021. How Do Companies Avoid Paying International Taxes? Peterson Institute for International Economics.

Dragu, Tudor, and Yonatan Lupu. 2021. Digital Authoritarianism and the Future of Human Rights. *International Organization* 75 (4):337–59.

https://doi.org/10.1017/S0020818325101070 Published online by Cambridge University Press

Erie, Matthew S., and Thomas Streinz. 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.

Farrell, Henry, and Abraham L. Newman. 2019a. Of Privacy and Power: The Transatlantic Struggle over Freedom and Security. In *Of Privacy and Power*. Princeton University Press.

Farrell, Henry, and Abraham L. Newman. 2019b. Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security* 44 (1):42–79.

Farrell, Henry, and Abraham Newman. 2023. *Underground Empire: How America Weaponized the World Economy*. Henry Holt and Co.

Floridi, Luciano. 2020. The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy and Technology* 33 (3):369–78.

Gelepithis, Margarita, and Martin Hearson. 2022. The Politics of Taxing Multinational Firms in a Digital Age. *Journal of European Public Policy* 29 (5):708–27.

Girard, Tyler. 2024. National Identity and the Limits of Platform Power in the Global Economy. *International Studies Quarterly* 68 (3):sqae090.

Goldsmith, Jack, and Tim Wu. 2006. *Who Controls the Internet? Illusions of a Borderless World*. Oxford University Press.

Heeks, Richard, Angelica V. Ospina, Christopher Foster, Ping Gao, Xia Han, Nicholas Jepson, Seth Schindler, and Qingna Zhou. 2024. China's Digital Expansion in the Global South: Systematic Literature Review and Future Research Agenda. *The Information Society* 40 (2):69–95.

Heering, Jonas, Loriana Crasnic, and Abraham Newman. 2025. When Digital Taxes Come Due: National Digital Taxes and the Negotiation of the OECD Inclusive Framework. *New Political Economy* 30 (2):178–93.

Heim, Lennart. 2025. Understanding the Artificial Intelligence Diffusion Framework. *Perspectives* (RAND Corporation). <https://www.rand.org/pubs/perspectives/PEA3776-1.html>.

Horowitz, Michael C. 2020. Do Emerging Military Technologies Matter for International Politics? *Annual Review of Political Science* 23 (2020):385–400.

Hulvey, Rachel A., and Beth A. Simmons. 2025. Borders in Cyberspace: Digital Sovereignty Through a Bordering Lens. *International Studies Quarterly* 69 (3):sqaf047.

Ishkhanyan, Artur. 2025. The Sovereignty-Internationalism Paradox in AI Governance: Digital Federalism and Global Algorithmic Control. *Discover Artificial Intelligence* 5 (1):123.

Jensen, J. Bradford, Dennis P. Quinn, and Stephen Weymouth. 2015. The Influence of Firm Global Supply Chains and Foreign Currency Undervaluations on US Trade Disputes. *International Organization* 69 (4):913–47.

Johns, Leslie, and Rachel L. Wellhausen. 2016. Under One Roof: Supply Chains and the Protection of Foreign Investment. *American Political Science Review* 110 (1):31–51.

Kak, Amba, Sarah Myers West, and Meredith Whittaker. 2023. Make No Mistake—AI Is Owned by Big Tech. *MIT Technology Review*. <https://www.technologyreview.com/2023/12/05/1084393/make-no-mistake-ai-is-owned-by-big-tech/>.

Kemmerling, Michael, and Christine Trampusch. 2023. Digital Power Resources (DPR): The Political Economy of Structural and Infrastructural Business Power in Digital(ized) Capitalism. *Socio-Economic Review* 21 (4):1851–76.

Keohane, Robert O. 1984. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton University Press.

Keohane, Robert O. 2002. Ironies of Sovereignty: The European Union and the United States. *Journal of Common Market Studies* 40 (4):743–65.

Keohane, Robert O., and Joseph S. Nye. 1973. Power and Interdependence. *Survival* 15 (4):158–65.

Kim, In Song. 2017. Political Cleavages within Industry: Firm-level Lobbying for Trade Liberalization. *American Political Science Review* 111 (1):1–20.

Kim, In Song, and Helen V. Milner. 2021. Multinational Corporations and Their Influence Through Lobbying on Foreign Policy. In *Global Goliaths: Multinational Corporations in a Changing Global Economy*. Brookings Institution, 497–536.

https://doi.org/10.1017/S0020818325101070 Published online by Cambridge University Press

Kim, In Song, Helen V. Milner, Thomas Bernauer, Iain Osgood, Gabriele Spilker, and Dustin Tingley. 2019. Firms and Global Value Chains: Identifying Firms' Multidimensional Trade Preferences. *International Studies Quarterly* 63 (1):153–67.

Kim, Sung Eun, and Krzysztof Pelc. 2021. How Responsive Is Trade Adjustment Assistance? *Political Science Research and Methods* 9 (4):889–98.

Krasner, Stephen D. 1999. *Sovereignty: Organized Hypocrisy*. Princeton University Press.

Krishnamurthy, Vivek. 2025. Anchoring Digital Sovereignty. *Chicago Journal of International Law* 25 (2):2.

Kwet, Michael. 2019. Digital Colonialism: US Empire and the New Imperialism in the Global South. *Race and Class* 60 (4):3–26.

Lake, David A. 2003. The New Sovereignty in International Relations. *International Studies Review* 5 (3):303–23.

Lake, David A. 2011. *Hierarchy in International Relations*. Cornell University Press.

Lehdonvirta, Vili. 2024. *Cloud Empires: How Digital Platforms are Overtaking the State and How We Can Regain Control*. MIT Press.

Lehdonvirta, Vili, Boxi Wu, and Zoe Hawkins. 2025. Weaponized Interdependence in a Bipolar World: How Economic Forces and Security Interests Shape the Global Reach of US and Chinese Cloud Data Centres. *Review of International Political Economy* 32 (5):1442–67.

Liu, Lizhi. 2021. The Rise of Data Politics: Digital China and the World. *Studies in Comparative International Development* 56 (1):45–67.

Liu, Lizhi. 2024. *From Click to Boom: The Political Economy of E-Commerce in China*. Princeton University Press.

Mann, Michael. 1984. The Autonomous Power of the State: Its Origins, Mechanisms and Results. *European Journal of Sociology/Archives Européennes de Sociologie* 25 (2):185–213.

Mansfield, Edward D., and Nita Rudra. 2021. Embedded Liberalism in the Digital Era. *International Organization* 75 (2):558–88.

Miller, Chris. 2022. *Chip War: The Fight for the World's Most Critical Technology*. Scribner.

Milner, Helen V. 1988. *Resisting Protectionism: Global Industries and the Politics of International Trade*. Princeton University Press.

Musiani, Francesca. 2022. Infrastructuring Digital Sovereignty: A Research Agenda for an Infrastructure-based Sociology of Digital Self-Determination Practices. *Information, Communication and Society* 25 (6):785–800.

OECD. 2018. Tax Challenges Arising from Digitalisation: Interim Report 2018.

Olugbade, Olajide. 2025. In Search of a Global Governance Mechanism for Artificial Intelligence (AI): A Collective Action Perspective. *Global Public Policy and Governance* 5:139–61.

Oppenheimer, Harry. 2025. Digital Interdependence and Power Politics. *British Journal of Political Science* 55:e93.

Osgood, Iain. 2017. The Breakdown of Industrial Opposition to Trade: Firms, Product Variety, and Reciprocal Liberalization. *World Politics* 69 (1):184–231.

Osgood, Iain, Dustin Tingley, Thomas Bernauer, In Song Kim, Helen V. Milner, and Gabriele Spilker. 2017. The Charmed Life of Superstar Exporters: Survey Evidence on Firms and Trade Policy. *The Journal of Politics* 79 (1):133–52.

Peters, Margaret E. 2017. *Trading Barriers: Immigration and the Remaking of Globalization*. Princeton University Press.

Rondeaux, Candace. 2025. Compute or Be Computed: Strategies for the AI Sovereignty Shell Game. *Planetary Politics* (blog), New America. 20 May. <https://www.newamerica.org/planetary-politics/blog/compute-or-be-computed/>.

Ruggie, John Gerard. 1982. International Regimes, Transactions, and Change: Embedded Liberalism in the Postwar Economic Order. *International Organization* 36 (2):379–415.

Sassen, Saskia. 1996. *Losing Control? Sovereignty in the Age of Globalization*. Columbia University Press.

Schmitt, Lewin. 2022. Mapping Global AI Governance: A Nascent Regime in a Fragmented Landscape. *AI and Ethics* 2 (2):303–14.

https://doi.org/10.1017/S0020818325101070 Published online by Cambridge University Press

Simmons, Beth A., and Rachel A. Hulvey. 2022. Cyberborders: Exercising State Sovereignty Online. *Temple Law Review* 95:617.
Slaughter, Matthew, and David H. McCormick. 2021. Data Is Power: Washington Needs to Craft New Rules for the Digital Age. *Foreign Affairs* 100:54.
Srivastava, Swati. 2022. *Hybrid Sovereignty in World Politics*. Cambridge University Press.
Srivastava, Swati. 2023. Algorithmic Governance and the International Politics of Big Tech. *Perspectives on Politics* 21 (3):989–1000.
Sun, Meicen. 2024. Damocles's Switchboard: Information Externalities and the Autocratic Logic of Internet Control. *International Organization* 78 (3):427–59.
US Department of Commerce. 2023. Implementation of Additional Export Controls on Advanced Computing Items; Supercomputer and Semiconductor End Use; Updates to the Entity List. Technical Report 88 FR 73458 Federal Register. Interim Final Rule.
Veale, Michael, Kira Matus, and Robert Gorwa. 2023. AI and Global Governance: Modalities, Rationales, Tensions. *Annual Review of Law and Social Science* 19 (1):255–75.
Wellhausen, Rachel L. 2015. *The Shield of Nationality.* Cambridge University Press.
Weymouth, Stephen. 2023. *Digital Globalization: Politics, Policy, and a Governance Paradox*. Cambridge University Press.
World Trade Organization. 2024. Trading with Intelligence: How AI Shapes and Is Shaped by International Trade. <https://www.wto.org/english/res_e/publications_e/trading_with_intelligence_e.htm>.
Young, Alasdair R. 2024. Governing the Digital Economy: Transatlantic Accommodation and Cooperation. *Journal of European Integration* 46 (7):973–92.
Zhang, Hao. 2025. Commerce, Coalitions, and Global Value Chains: Coordinated and Collective Lobbying on Trade. *American Journal of Political Science* 1–19.

Author

Stephen Weymouth is the Dean's Professor of International Political Economy in the McDonough School of Business at Georgetown University. He can be reached at stephen.weymouth@georgetown.edu.

Acknowledgments

I thank Ross Andersen, Marc Busch, Lizhi Liu, David Steinberg, the editors, and the anonymous referees for helpful comments. All errors are my own.

Keywords:

Artificial intelligence; AI governance; digital economy; digital sovereignty; emerging technologies; liberal international order; private authority

Date received: June 16, 2025; Date revised: September 13, 2025; Date accepted: September 23, 2025

https://doi.org/10.1017/S0020818325101070 Published online by Cambridge University Press