IGCC REPORT

JUNE 2025

The International Political Economy of the Regulation of Digital Technology

Peter Cowhey

Digital technology is seeping into every corner of society. As the pace of technological change accelerates over the next decade, digitalization is poised to impose profound changes on the international political economy. A new digital regime is evolving to govern these effects, although it is uncertain how this regime will develop amid tectonic shifts in governing establishments, world geopolitics, and the scope of economic globalization. A broad array of interests are contesting how digital governance will play out across the globe, from digital businesses big and small to politicians balancing security and economic growth objectives. Uncertainty predominates, but looking at previous historical instances where new technology demanded cross-border governance can reveal clues as to how a digital regime can take shape in a more sovereignty-oriented world.

This report explores the digital order that underlies transnational tensions over regulating digital technologies, finding that the contours of the emerging digital regime will depend on how policymakers thread the needle between national security and fostering innovation, a balancing act for which the outcome is currently unclear.

IGCC
UC INSTITUTE ON GLOBAL CONFLICT AND COOPERATION

Authors

Peter Cowhey
Dean and Qualcomm Chair Emeritus
UC San Diego School of Global Policy and Strategy
Email: pcowhey@ucsd.edu

Acknowledgements

My thanks to the Jason Kuo, Stephan Haggard, Jonathan Aronson, and the 2024 Chinese Association of Political Science Annual Meeting at National Taiwan University for comments on this paper.

Suggested Citation

Cowhey, Peter. 2025. *The International Political Economy of the Regulation of Digital Technology*. IGCC Report. escholarship.org/uc/item/76q4n61d

This paper explores the global political economy of digital technology markets. This political economy will influence how government rules, international norms, the strategies of key private and nongovernmental actors, and decision-making processes—the global digital economy regime—evolve in digital technology markets over the next ten years.[1]

Digital technology is permeating every corner of economic and societal processes. It is important to specify the empirical scope of the digital regime to be examined. My focus will be on the governance of the implications of market structures and practices for global digital technologies.[2] Individual technologies for semiconductors, computing, software, communications, and artificial intelligence (AI) are important, but understanding their implications for the political economy of digital governance requires looking at their intersections. Even before the growing turbulence induced by a new wave of industrial policy and economic security policies, the implications of digital technology for global markets were nibbling away at the multilateral principles that had guided the world economy after 1945. However, digital dynamics were also creating new incentives for maintaining digital interdependence under revamped governance.

Forecasting how political and economic factors influence the evolving mechanisms of governance is very risky. Even before the 2024 election of President Donald Trump, traditional international economic institutions were subject to redefined roles, as was most visibly happening in trade in the name of "de-risking supply chains." Trump quickly further upended the regime. Interdependence depends partly on inertia; it is hard to sustain the resolve to abandon global economic regimes completely. But, even more fundamentally, the political economy of digital markets rests on a deeper array of interests than the typical focus on the giant digital technology firms suggests. This broader and deeper ecosystem of interests, and practical technological capabilities, is the *Digital Mittelstand*. The existence of the *Mittelstand* does not dictate the particulars of the digital economy regime but it does serve as a loose set of boundaries on the incentives for governance choices.

If technology capabilities and interests are one set of drivers of both continuity and change in the global digital regime, geosecurity and economic tensions, primarily involving the role of China and secondarily among nations of the Organization for Economic Cooperation and Development (OECD), will be the second set of drivers. Even if President Trump had not won the 2024 election, the digital ecosystem would have changed.

The second set of drivers include the rising pulse of industrial policies driven by concerns over economic competition and security concerns involving China.[3] These forces created uncertainty that further eroded the role of the World Trade Organization (WTO) and challenged how the usual fixes, such as emphasizing technical standard setting to cope with technological change, would work. The emphasis on sovereign geosecurity norms increased. Institutional fragmentation grew, and the world witnessed much more trial-and-error experimentation in both national and international rule making. All this had some positive virtues of creative learning about governing technology, but it was not costless. Most importantly, none of the changes before Trump necessarily implied large trade wars, a sweeping decline of interdependence, and an end to meaningful government coordination on digital markets.[4] Even with the Trump administration's disdain for much of the global economic regime and his decision to use sweeping tariffs to propel bilateral reciprocity deals, there are deep technological drivers and political economic interests that could allow a modified governance system for an interdependent global digital market.[5] It would be less coherent as a whole with somewhat different organizing principles and operational rules for each of its specialized governance tasks.

Section 1 of this paper begins with a discussion of the characteristics of digital technological change that impact choices about global governance. Section 2 focuses on the political economic importance of the *Digital Mittelstand*, a concept that shows how the global digital ecosystem has evolved. This *Digital Mittelstand* creates incentives that reinforce international cooperation on digital governance even if the specific arrangements change. Section 3 then discusses the consequences of uncertainties surrounding geoeconomics, security, and industrial policy for digital regime governance. The key role of China is central to this uncertainty. Section 4 sketches some design features of a global digital regime that could better cope with greater uncertainty. Section 5 concludes with specific examples of how governance could adapt. It draws from a sovereignty-oriented regime—international aviation—and then examines five policy challenges.

1. Three Features of the Evolving Digital Technology Ecosystem

How are changes in digital technology driving choices and constraints for the global digital market regime? Any effort to highlight specific technological forces driving the global market requires caution about the big picture. Analyses of the digital ecosystem often confuse the impact of the digital innovation of the moment with the larger pattern of change. This larger pattern is the expanding array of economic and societal impacts arising from ever-faster rates of digital technological changes and broader penetration of digitalization into every facet of the economy and society. This upheaval often features surprising twists in market organization. For example, the newest technological cliché is that AI changes everything because its potential is vast—especially as it might achieve artificial general intelligence—even if its precise applications are still often speculative. However, AI is only part of a broader digital transformation that penetrates every part of global society and its political economy.

As a simplified mental model, imagine that electricity had initially penetrated large factories and urban enclaves, and then only later penetrated the rest of society's workings. Ubiquitous electrification (still not completely done) then spurred a second wave of profound consequences that were even greater than electricity's initial thrust (think of what mass electrification of households meant for social dynamics and labor markets, not to mention the demand curves for steel and plastics in new appliances).

Instead of looking at individual technologies, it is wiser to look at three characteristics of the evolution of digital technology, especially as it moves into its second wave.

A first effect results from the rapid pace of diffusion. The quick speed of widespread global deployments of each generation of digital innovations has only accelerated. The pace is much faster than the spread of mass aviation, electrification, or telephones.

Consider the accelerating diffusion of digital services. It took the World Wide Web about seven years to reach 100 million users when introduced in the mid-1990s. Both Facebook and YouTube took over four years to reach a similar user base. Instagram shrank the time to attain 100 million users to two-and-a-half years, and TikTok made it in only nine months. ChatGPT hit 100 million users in two months.[6]

The consequences for regime governance are more complicated than simply saying governments cannot keep pace with technology. In the short term, the early deployment of big digital innovations responds mainly to government choices that enable their initial takeoff. That was true of U.S. policies supporting large-scale research and development (R&D)—much for risky frontier work—venture capital financing for risky technology, and cautious (not absent) antitrust policy.[7] This mix made the United States into the birthplace of the Internet, cloud computing, and most of the other big digital innovations. These innovations altered the economics and operations of large-scale digital markets before most governments flagged policy concerns. Once deployed rapidly, economies of scale, first-mover advantages, and varying levels of network effects reinforce the shock of speed.

Governments can strongly influence the characteristics of digital markets over time, but they operate in a context where many features of the technological system already have deep roots which may be relatively immune from the effects of well-intentioned policy; they are baked in. For example, subsequent government pushes for more localized cloud facilities to handle some sensitive data have succeeded, but these national options had to be grounded in an already-interlocking global cloud infrastructure for cost and performance reasons. AI regulation will surely influence important features of AI technology and its uses. Yet, even as European Union (EU) authorities raced to an early round of sweeping AI regulations, the technology had already emerged to massive commercial investment.

As the discussion in Section 2 notes, rapid diffusion covering a greater range of technologies and their implications was nibbling away at multilateral governance by the 1990s. Sometimes, for example, solutions required institutional experiments. The growing speed and broader spread of digital innovation has heightened uncertainties about digital governance. The advent of the Internet required a major innovation in governance in the Internet Corporation for

Assigned Names and Numbers (ICANN), an institution that operates as a global nongovernmental organization (NGO) with a governmental advisory body. The precise balance of influence among technocrats, civil society representatives, and governments remains a contested subject.

The second feature of the digital ecosystem runs counter to popular discussions that dwell on the persistent size of a few big platform companies (e.g., Google and Amazon). In fact, there is a constantly shifting mix of advantages and roles of leading commercial players on the technology frontier, as the digital ecosystem grows more complex. This reality changes practical incentives and feasible options for national economic strategies, in part because new players come on the scene with particular interests and capabilities. They become agents of political and market change.

Digital technology over the past 45 years has been full of fundamental surprises and competitive upsets. Competitive surprises due to Schumpeterian dynamics disrupted mainframe platforms like those of AT&T and IBM (and their global counterparts) by the early 1990s, the rise of the Windows-Intel software and hardware platform in personal computing, the advent of the Internet and rise of the Web (along with the rise of routers and related technologies), the emergence of e-commerce, the explosion of mobile and broadband infrastructures enabling the app world of iOS and Android, the disruption of social media, the power of cloud computing and big data centers, and the emergence of new architectures (and production systems) dominating semiconductors and accelerating the explosion of generative AI. Running throughout these many changes was a deeper intermingling of software and digital services with the fate of traditional digital hardware markets. This mix, especially the role of services, did not fit neatly into the traditional policies governing global commerce that had been designed for a world of goods. Google is rich from search and its ad revenues, but its Android operating system (and its applications mimicking Microsoft systems) accelerated widespread innovation in mobile hardware markets, from handsets to component supplier systems. Along with Apple, the Android ecosystem accelerated the decline of personal computers' dominance in digital markets. It also, arguably, made South Korea's Samsung into one of its biggest beneficiaries. Today, Huawei has invested heavily to rid its operating system of Android code in order to champion an alternative to Microsoft, Apple, and Google software operating systems. Meanwhile, the infusion of AI into many digital systems makes it easier to offer

alternative business models for digital advertising (such as on TikTok or specialized AI apps) that may erode Google's dominance of digital ads.[8] Consider how Intel, long a vertically integrated design and production firm, succumbed to the challenge of Taiwan Semiconductor Manufacturing Company Limited (TSMC) which operated as chip foundry for independent chip designers. TSMC then accelerated the dominance of specialized chip designers for most key uses. Their ranks ranged from Arm to Qualcomm to Nvidia. Nvidia's mastery of specialized semiconductors for gaming later became the basis for dominating the chips used for large AI models. Large AI raised fundamental questions about the sustainable advantages of many digital service platforms. And Meta seemed an unassailable social platform leader until TikTok discovered another digital user experience. Most recently, the United States' conviction that it had a substantial lead in both AI technology and its commercialization confronted a recalibration when a new Chinese firm, DeepSeek, showed that many AI applications did not require the large-scale models used by U.S. firms. These kinds of dynamics raise profound questions about predicting competitive advantages (by firm or country) and national security assurances.

Fairly rapid changes in the cutting edge of technology can have surprising implications for those seeking to harness digital services to advance national economic growth. It has certainly frustrated technocrats in the European Union. Even the biggest firms have a hard time sustaining leadership on a broad front of markets.[9] Yet, to be clear, specific competition problems can arise at any time in a particular market segment. Even if there are no violations of competition rules, the decisions of giant digital platforms on their design and commercial tradeoffs have large implications. For example, a decision by Apple to increase the number of steps for users to approve transferring their contacts lists wholesale to digital apps was justified as an upgrading of privacy protections. But app suppliers objected that it would reduce their ability to grow their network reach, perhaps to the profit of Apple.[10]

The third feature of the digital landscape is the rise of modularity as a design principle. Modularity emphasizes breaking down technical tasks into discrete building blocks with standardized transparent interfaces. Think of Lego building blocks in digital form. Modularity is the result of technological opportunity, commercial bargaining, and prudent use of traditional government competition policies.

As a commercial reality, modularity has surged because of the breakdown of the vertical integration model for big complex systems.[11] Global supply chains are one result of this breakdown. Much more careful, and flexible, drawing of boundaries around the core competence and updating the business model of a firm preoccupies top management.[12] All companies become strategic bargainers who seek multiple options for key technical inputs. For example, each large cloud provider has its own software system to simplify data management and compute tasks. But the big users of the cloud have successfully pressed for each software system to have modular features that allow the customer to move their compute task around among multiple commercial rivals. Such modular interconnection features are rarely perfect or costless, but market pressures force enough modularity to permit customers to switch if there is significant dissatisfaction.

As a technical matter, modularity has become a key design tool to address complexity even within the core digital operations of a company. Large software systems rely on a modular system with elaborate system management tools that let code modules be "checked out and in" for reuse or carefully documented modification for new processes.[13] This modular approach is one reason why all large software systems (e.g., Microsoft) can use open-source software from others in many pieces of its code. This ability to recycle and adapt open-source code reduces the cost and time of completing many programs.

On a complementary front, antitrust policy in classic cases against AT&T, IBM, and Microsoft all involved government actions to increase the modularity of offerings of major market suppliers.[14] Transparency of applications interfaces (whether hardware or software) to allow competitors to more easily interconnect selectively to the dominant supplier's system was crucial. Today, the competition cases to force Apple and Google to offer alternative financial mechanisms for apps using their stores revolve around requiring new forms of modular design in app marketplaces.[15]

Modularity is so fundamental that its implementation details will always spur specific disputes, but it has changed the way digital markets work and the options for governance. Getting competition rules correct for modular designs is tricky because they need to incentivize designs that work globally. They are also crucial because they influence the ability of specialists to innovate in the market while recognizing that massive digital infrastructures are also vital.

Modularity also has major implications for digital security. On the one hand, it increases the variety of digital inputs. These inputs may either come from suspect sources—as the U.S. government feels about some code from Chinese systems—or it may be digital assets that are not sufficiently updated to deal with constantly changing digital risks, as is often the worry about digital consumer products. On the other hand, as modularity becomes ever more sophisticated, governments could learn how to require software system swaps—from one software program to another—for certain security systems. The U.S. government (and many others) already requires forensic software analysis for certain products and services to assure legitimate (unhacked) code from approved suppliers. Later, I shall illustrate this approach for the electric vehicle (EV) industry.

Faster diffusion of innovation covering a growing scope of the economy and society, shifting competitive advantages and capabilities in an evolving digital ecosystem, and the growth of modular design options mean that there is substantial uncertainty about which policy options work best over time. Are efforts through technology controls to slow Chinese influence in digital markets feasible over the long term? Or, consider how the specialized software systems for electric vehicles and other manufactured products raise new cybersecurity questions.[16] Decisions on American regulation of TikTok depend partly on whether it is feared for its collection of data on American citizens or because of how its algorithms may influence American public opinion. Identifying realistic regulations of AI is desirable but hard when the technology evolves frenetically. Is it even feasible to have a digital regulatory agency, or is it better to keep regulation in agencies equipped to evaluate specific use applications?[17] The evolving digital ecosystem's effects on governance options, eroding many older policy principles while creating incentives to adapt to the dynamics of a *Digital Mittelstand*, were further propelled by the later rise of industrial and security policies sketched out in Section 3.

2. The Implications of the *Digital Mittelstand*

All three dynamics have created a digital ecosystem where giant platform companies coexist with, and depend on, a growing global diversification of specialized digital equipment, software, communications, and digital service companies. This is the *Digital Mittelstand*.

As an illustration, consider the more familiar case of manufacturing. Germany's manufacturing giants, like Volkswagen and Siemens, have long depended on a large manufacturing *Mittelstand* of smaller specialist suppliers, who have revenues ranging from the tens of millions to around 1 billion euros.[18] Many of these firms have now evolved to become particularly technology focused, especially in the application of digital tech.[19]

Most significantly, the *Digital Mittelstand* expands because even digital giants specialize around core competencies while turning to complementary partnerships for other activities. As a simple example, Netflix does not deliver its programming on a global basis. It is done by content delivery networks who specialize in reliable transport and low latency, interactive delivery of the Netflix user interface and content. The big data flows done among cloud computing centers may—as with Google—be done on fiber optic infrastructure owned by the cloud provider, but its reliable provision just as frequently rests on specialized suppliers around the world, of which Asian providers from Singapore and India figure prominently.

Global platforms in e-commerce have far less dominance outside of their original core markets than many expected. Big digital platforms build their business models around certain strategies, talent, and cost structures, and often it is difficult to redo them for other markets. Europe does well in some specialized travel and music e-commerce platforms. Specialized knowledge of local business customers, household consumer demand preferences, logistics, and government practices often lend significant advantages to regional (e.g., Southeast Asia) or local firms. Japanese firms, like Rakuten, specialize in adopting to Asian consumers. Local and regional e-commerce firms dominate Amazon in most middle-income countries. Flipkart is the leader in South Asia. Shopee is top in the Philippines, Thailand, and Indonesia, while MercadoLibre is the biggest in Argentina and Brazil.[20]

Supply chain management systems are now fundamental to every effort to "de-risk" supply chains for resilience, real-time adjustments, and security while managing costs effectively. But the biggest digital platforms do not dominate. Two big but specialized firms, Oracle and SAP (a German firm), are the largest suppliers but there are huge numbers of skilled specialists for particular global market niches. This includes a rich variety in smaller markets of lower-income countries. For example, a successful Vietnamese logistics company (sShip) relies on Google tech but succeeds in its global shipping service because it knows how to navigate the complexities of Vietnamese ground transport and meet shipping schedules reliably.[21] More generally, digital services and infrastructure have become critical for supply chain management (including product safety) for agriculture products and manufacturing while enabling export-oriented service ventures such as healthcare in the Philippines.

Just as significantly, the digital infrastructure itself (such as cloud computing facilities) and the second wave of digital expansion into deeper penetration of manufacturing and its related services (such as maintenance) rely on a vast array of digital specialists. Focusing only on the platform giants ignores much of the action. Consider the picture for how the *Digital Mittelstand* shapes manufacturing through physical design software. For example, computer assisted design (CAD) software features leadership by an American specialist, Autodesk, plus software groups in European industrialists, Siemens and Dassault Systemes. Electronic Design Software (vital for semiconductors) is led by Cadence and Synopsis. And simulation software features Ansys and Altair.[22]

As another example, digital twins are assuming a larger role in corporate management and production.[23] Large-scale models for a new manufactured product allow it to be modeled completely, tested for performance by other models fueled by massive data (e.g., digital models of wind tunnel test designs for aircraft), and then generate a detailed manufacturing plan, including process checklists for quality control. Meanwhile, the growth of cheap networked sensors allows continuous feedback during manufacturing implementation for error correction. Financial models and human resource models complement the physical twin. Twins are even being deployed to test and guide fertilizer and chemical insecticides to be dispersed by smart tractors. Meanwhile, telecom carriers are using digital twins to manage their networks from technical design and operation to capital expenditure planning.

All of the activities generate massive volumes of data collection and use with growing global scope in order to improve predictive powers and operational efficiencies. The growing share of digital content (and financial value) in all major products means all commercial actors—and, as they realize the stakes, their governments—have incentives to become specialists as smart users or suppliers in some aspects of digital. And it does not pay to reinvent the full array of interdependent digital inputs. Analysts of the future of digitally enabled manufacturing identify at least five major clusters of sophisticated capabilities, each with their own global leadership array, as essential for this progress.

As the next wave of digital services penetrate everything, the complexity and diversity of digital suppliers grows. This powerful force leads growth-oriented economies, especially in the Asia-Pacific region, to reject the most restrictive digital protectionism. The functional incentives to work together created by the digital ecosystem, especially by the *Digital Mittelstand*, influence how geoeconomics and industrial and regulatory policies play out globally. Scholars of international relations commonly refer to these functional incentives to cooperate as a "coordination" game. However, as I shall discuss, coordination often emerges only after travelling on a far messier and conflictual path.[24] The dominant coordination mechanisms will also evolve.

Having to evolve policies within de facto technological design parameters by early deployments produces strong political tensions.[25] This is doubly so when a major economic power, such as the EU, is frustrated over its lack of leadership in the most prominent digital firms.[26] Meanwhile, legitimate desires for risk management get amplified by populist political pressures that demand still more stringent regulation to respond to regional preferences, such as privacy protection.

In sum, the digital technology ecosystem has both incentives for coordination across jurisdictions and a potent mix of competition sensitivities, social concerns, and security issues. The speed and scope of digital deployments, the uncertainty about the efficacy of various governance mechanisms, the disruptions in technological leadership, the trend toward modularity in design and implementation, and the growing role of a *Digital Mittelstand* are factors shaping the political economy for the digital technology regime.

3. Industrial Policy and Geosecurity Issues Driving Change in the Digital Regime

Geosecurity and geoeconomics also propel changes in the digital ecosystem's governance. The biggest democratic market economies—represented in the OECD—have lost substantial economic power. This raised concerns over their economic future and security vulnerabilities. This decline also made it harder for the United States (or the OECD as a group) to establish strategic focal points—policies and practices anchoring conduct in large core of the world market—for shaping, interpreting, and implementing global norms and policies for digital markets.

This concern over eroding OECD power cloaks a subtler, corrosive reality. The U.S. share of global gross domestic product (GDP) has not changed much in the past 30 years. It is the rest of the OECD that has slipped in the global GDP tables. The weight of China, in particular, and the larger middle-income countries has grown in comparison to the rest of the OECD. This has raised fears in the rest of the OECD, especially the EU, that it has become more vulnerable to the policy whims of the United States and the growing power of China. One possible way of understanding the Trump administration's penchant for the unilateral redesign of global economic rules is that it did not see its allies as adding much "muscle" to its bargaining position with China while adding a morass of diplomatic complexity and niceties.

Lower growth rates, issues of economic equity, and alarm over the implications of digital change for governance priorities, have led most OECD countries to renewed industrial policy along with ambitious regulatory and competition guidelines for digital tech. This leads to complicated subsidy schemes for critical industries that often tilt toward domestic firms to some degree and regulatory safeguards designed to foster home market strengths.

And the United States, out of security concerns over China and anxieties about its own economic performance, has become more engaged in industrial policies, some of which discriminate against traditional allies. The Biden administration worked to minimize these conflicts with partial success in new regional technology councils in Europe and Asia. However, the advent of the Trump administration has only intensified possible economic clashes.

Even before Trump, U.S. policy shifts had prompted a rising chorus of demands for EU policies that would promote their digital firms and diminish reliance on U.S. digital firms. The EU suspects its failure to be in the very top ranks of digital tech (SAP, ASML, and Arm are its biggest players) is because of unfair competition from American firms and rising threats from Chinese firms. The difficulties of achieving unification of the internal EU digital market also are a drag.[27] The proposals for change include heightened government subsidies, more seamless integration of the EU internal market for digital tech, and fine tuning vigorous regulatory policies targeting U.S. firms as part of the policy mix.[28]

As a rule of thumb, even well-justified industrial policies usually have features that can trigger international economic disputes. The decades-long U.S.-EU trade clashes over aerospace policies supporting Boeing and Airbus exemplify how complicated and persistent these disputes can be. Digital technology covers a far wider landscape. Two key instruments of industrial policy further illustrate the tensions. They are the subsidies for national production facilities (as is the case with semiconductors or green technologies like batteries) or protective tariffs for critical industries. Subsidies—often including special rules for labor protections in some countries—will expand because they are popular in general electoral politics and in business circles. Moreover, when properly targeted and implemented for vital national security issues, subsidies to induce TSMC and Samsung to create semiconductor fabs in the United States don't produce major distortions in competition. The question is whether subsidies are available only to domestic firms or to all producers meeting the project guidelines (which may include security provisions). And the issue on tariffs is whether they are designed so as to essentially ban a particular product from another country or if they permit other supply options, such as local production through foreign direct investment. This is a key question for U.S. and EU tariffs on Chinese electric vehicles that are discussed later.

The political and economic tensions among OECD nations and between the OECD and most of the rest of the world would have sufficed—along with the changing governance implications of digital technology trends—to induce some digital regime change. But it is the rivalry with China that accelerated disruption over the past ten years, roughly starting with the late Obama administration.

There is a growing conviction among OECD countries (as well as many other countries) that China has become both a security challenge and a disruptive economic and technological power endangering OECD companies by design of the Chinese political leadership under President Xi. Until Xi, China had moved in spurts to a more market-organized economy and political institutions with some degree of internal political checks and balances. This state of affairs was not a perfect fit for global economic governance, but it seemed manageable without requiring China's conversion to full-blooded domestic liberalization and democratization. Then, under Xi, fears about the security of Communist Party rule due to domestic and global pressures prompted a reversion to more centralized political control and greater government control of the economy, especially its technology sectors.[29]

Xi's approach has emphasized a larger (but not exclusive) role for state-owned enterprises and a reinvigorated use of Communist Party cadres within private firms to emphasize the party's ability to steer the transformation of the Chinese economy. There were ambitious policies to massively subsidize and achieve Chinese leadership of key global technology markets. This included the revamping of the Chinese R&D system ranging from elite universities through new industrial consortia and applied engineering centers. Two special stamps of these technology efforts were a greater emphasis on supporting massive manufacturing capacity compared to other advanced technology nations and a detailed plan for fusing its efforts to achieve global market and military technology leadership. A byproduct of this integrated national strategy was a continued emphasis on expanding manufactured exports in digital markets and the detailed pathways to limiting foreign technologies' role in China over time. In the long term, China would emerge as the technological leader of a greatly revamped global order.[30]

The OECD nations responded to China with mutually reinforcing initiatives of industrial and security policy that produced many disruptions. Policies to "de-risk" global supply chains featuring subsidies for nearshoring manufacturing and stronger security rules on inward-bound foreign investment from China are prominent. Technology restrictions by regulation (involving major U.S. allies), such as those imposed by the United States on the use of Huawei technology for mobile communications or on the sale of advanced semiconductor chips and production technology to China became staples of digital policy. The issue will be how sweeping they will become. Increased screening of outward-bound U.S.

foreign direct investment as part of a technology control program will, to a degree unknown, clash with traditional global market practices. The Biden administration in its closing days issued a directive limiting the sale of advanced semiconductors to many countries by grouping them into tiers of presumed security alignment with the United States in regard to China and other countries posing security risks. The Trump administration upended this order, but it may well come up with its own variant.

Meanwhile, many of the Asia-Pacific and faster-growing middle-income countries also have worries about China, but are skeptical about being fenced in by a Cold War-style set of choices between OECD and Chinese digital technologies. The effects of changing digital technology advantages and their participation in the *Digital Mittelstand* give them strong incentives to avoid being locked in. And these countries represent a rapidly growing share of the world market.[31]

National strategies will vary. For security reasons and because its companies have thrived in the *Digital Mittelstand*, Japan is a firm ally on U.S. technology controls. Countries wishing to host major cloud computing complexes to drive AI large language models (LLMs), such as the United Arab Emirates, may be reluctant to freeze out Chinese digital tech, but may sign onto technology control agreements (especially export controls involving China) as a price of access to leading-edge U.S. technology. But this depends on their conviction that the U.S. technological lead is unassailable for commercial purposes, an uncertain proposition. India has reservations about Chinese digital tech but is reluctant to join a general divorce from it.

Many countries feature significant intermingling of OECD and Chinese digital capabilities on the ground floor of their national economies. The hotbed of data center growth in Southeast Asia is dominated by U.S. firms, but Chinese firms are rarely excluded. As a further example, despite vigorous U.S. diplomacy, Huawei remains entrenched in many countries that like Huawei's less expensive yet reliable technology. Consumer technologies and routine digital office equipment, which are networked, are often Chinese. This opens new avenues for security risks that can reach back to the United States because networked digital technology has global links that cannot be contained outside American borders.

When the United States warns other nations of digital risks from Chinese tech, such as spying, they sometimes pay heed. However, frequently these countries don't see much difference between possible Chinese spying and the work of America's National Security Agency.

When the dominant market powers can no longer be counted upon to proceed with consistent policies over time, it changes the global regime. It reduces the ability of those market leaders, whose economic strength has ebbed somewhat, to create informal focal points (credible signals about behavior) that can induce other countries to trust more expansive international commitments traditionally championed by a leading power like the United States. [32] Section 4 explains the consequences of these uncertainties for digital governance.

4. How Uncertainty Changed Incentives for the Design of the Global Regime

Even without the Trump administration's embrace of policy uncertainty as a bargaining wedge, uncertainty had produced a tilt in the global digital regime toward narrower, more contingent commitments on international market opening. It eroded confidence in the ability to write, implement, and enforce more sweeping policy commitments (or, in the economics literature, contracts) because the strategies of the biggest players are less predictable.[33] When the biggest market players, private or public, get less predictable, it raises problems for other actors in deciphering the implications of the market rules. Moreover, as Section 1 argued, the changing digital technology ecosystem has created both uncertainties about competitive advantages and incentives to find new policy tools to maintain interdependence.

As of early 2025, it is hard to know where Trump administration policy will land. Massive tariffs are intended to force revisions in both tariff and nontariff barriers in all other countries while forcing some industries to cut imports drastically while boosting production in the United States. But, announcements of over one hundred trade negotiations on short time schedules suggest results will be wildly uneven. This section focuses on identifying a baseline of effects from growing uncertainty for the digital regime. If we have this baseline better identified, it will be easier to probe how the Trump preferences, once clear in operational terms, might further tilt the regime.

Imagine that more of the Biden style of industrial and security policy continued to prevail. What would narrower, contingent contracting and loss of credibility by key leaders produce? A decline in multilateralism and the rise of strategies featuring "regime complexes" is the first-order effect. Regime complexes place greater priority on a more fragmented specialized set of international institutional arrangements. It also features both greater political oversight of key technical coordination practices and newly dispersed participation in these exercises. Institutional fragmentation is accompanied by greater reliance on "soft law" and the use of performance metrics for setting coordination of national markets in the digital regime. Initiatives of significance for digital governance will become less anchored on traditional OECD leadership. Policy practices will embrace more experimentation and feature renewed emphases on the use of national authorities to implement and adjudicate soft law principles and rules.

A greater reliance on a fragmented regime complex is a fundamental effect of growing uncertainty for geopolitical or technological management reasons. This weakened global and regional multilateralism. Multilateral regimes emphasized core principles of strong nondiscrimination, indivisibility, and diffuse reciprocity in regime principles and rules. An emphasis on anchoring economic regimes around a major multilateral institution was a key feature of the post-1945 era.[34] The embattled WTO embodied such nondiscrimination safeguards in trade as its most favored nation and national treatment rules. The biggest liberalizations of digital markets in recent years were the WTO's basic telecommunications services and information technology agreements that liberalized information service markets and cut tariff and other barriers for much of the hardware used in digital ecosystems. The rise of networked computing and the Internet helped to induce agreement to service-market liberalization because these technologies fundamentally changed the incentives for all companies and countries seeking digital technology leadership.

One reason for the diplomatic success on hardware was the *Digital Mittelstand*; many countries were now parts of global digital supply chains as specialized suppliers and even more countries valued less expensive arrays of digital hardware. However, the corroding forces of uncertainty (such as fears over cybersecurity of equipment) began to erode trust in agreements that did not

allow discrimination against particular national suppliers. Further limited progress arose only in smaller pacts among trusted partners, such as the digital trade articles in the United States–Mexico–Canada Agreement (USMCA) in North America.

Declining multilateralism has led to institutional fragmentation, employing more emphasis on new sets of policy tools. Scholars of international relations have captured such dynamics with the concept of a regime complex. The point of this concept is that there can be an overall strategic anchor for international governance of a sector such as digital technology even when the piece parts (the source of complexity) may vary in some of their key governance principles and policies. Good order is not always a product of perfectly tidy behavior (or expectations).[35] Importantly, for the Biden administration, the introduction of greater regime complexity did not mean the end of the "rules-based international order." While this term is greatly suspect in the mind of many in Trump's foreign policy team, Trump's push for many new bilateral trade deals featuring similar innovations on nontariff barriers might yield a more fragmented version of the regime complex already emerging under Biden.

In digital markets, the advent of market competition as the dominant mode for telecommunications and information services in the 1990s meant growing regime complexity even at the height of multilateralism. Trade policy institutions began to anchor and constrain the choices of traditional intergovernmental institutions more focused on top-down regulation of some technical issues (e.g., the International Telecommunication Union). Meanwhile, the emergence of the Internet produced a nongovernmental coordination body that handled the technology's core name and numbering system, a move that distressed some governments that wanted more direct control.[36] Despite these regime complexities, market participants had a reasonable mental map of how to build a global strategy around the institutional pieces. As a result, global investment and cross-border trade in the telecommunications and information services markets exploded and fostered the rapid diffusion of the Internet and the World Wide Web.

In short, the record of regime complexes shows that meaningful global expectations about the operation and governance of key technology markets can exist even while allowing for varying degrees of emphasis on national sovereign rights and diverse institutional anchors. It also recognizes that broader diffusion

of global geoeconomic power requires more variation on particular issues of special importance to countries both within and outside the OECD. This often leads to institutional fragmentation and specialization.

The fragmentation of international digital governance into more specialized regional and "minilateral" functional arrangements accelerated under the Biden administration. Its trade and security policies focused on nurturing specialized regional "technology clubs" for technology regulation, including security controls, at the expense of the WTO or even global "plurilateral" deals for key technology markets.[37] Although careful to keep endorsing WTO rules, EU policy often followed a similar approach. Much of the policy attention was on ad hoc accommodations of the side effects on other club members from new industrial policies, creating best practices to "de-risk" supply chains highly dependent on China, and coordination of national regulatory policies to control the flow of critical digital technologies to China.[38] Tellingly, multilateralism was not a core organizing principle.

The growing importance of regime complexity means that even the arenas of global digital regimes typically considered the most apolitical, such as setting technical standards or safety codes, become subject to new processes and political leadership.

Scholars have noted these wonky technical domains correspond to game theory's coordination logic. This logic suggests all actors have a top priority of settling on a regime solution to perform an international task even if they might disagree about the best solution. While Krasner long ago noted that coordination might benefit some more than others, all countries still find coordination to be compelling.[39] This still is true in the digital space; the *Digital Mittelstand* has a vested interest in coordination. However, the future terms for coordination are subject to national clashes of interest and tensions created by shifting advantages among firms in digital markets. When multilateralism recedes and institutional fragmentation in regime complexes becomes more prominent, coordination frameworks can vary.

In the 1960s, global satellite communications were deemed a coordination challenge of such significance that enormous policy ingenuity went into the creation of a monopoly, intergovernmentally controlled corporation (Intelsat) to provide global satellite communications.[40] Subsequently, as technology shifted

the economics of communications, coordination shrank mainly to global administration of radio spectrum available for competitive satellite systems. Intelsat withered.

In an era of greater technological uncertainty and geopolitical stress, delegation of formulating the expert details needed for global operations becomes overlaid by greater political oversight. Delegation to experts emphasizes more diverse participants in expert groups, often called multistakeholder (civil society) governance. This is the story of Internet governance as it has evolved through many furious debates about how to weigh the guidelines and participation in decisions in a body outside the control of traditional international organizations. Greater transparency in the proceedings of expert groups and stronger monitoring by governments is another safeguard response. To this end, national regulatory authorities start to play a more prominent role in international coordination, sometimes at the expense of established agencies for international economic policy.

The evolution of delegation will confront growing geopolitical difficulties. There are more concerted efforts to "game" these technocratic processes by governments. A traditional tactic of subtly stacking the deck of expert bodies by specialized membership rules or decision processes in self-interested manners has become more prominent. These include the recent growth of influence-building initiatives by "illiberal regimes" in the coordination work of international organizations at the global and regional levels.[41] As a result, national security and other sensitive regulatory concerns matter more for these efforts; fragmentation of the institutions charged with standards work is likely in order to provide an official basis for inclusion or exclusion of certain national experts.

To illustrate, once governments realized that different technical architectures implied very different market advantages in the mobile communications industry, the traditional standards process became subject to a major diplomatic dispute between the United States and the EU. That was resolved by tweaking practices governing standards by the early 2000s. More recently, French actions on protecting sovereignty for data security (through requiring joint ventures to supply cloud services for certain data) and the EU's bypassing of global standards organizations again reflect these geopolitical dynamics.[42] And the EU suggested that it and the United States could work out certain alternatives to global standards in the U.S.-EU Trade and Technology Council.[43]

Beyond the classic coordination problems for the digital regime are new issues specific to digital technology, such as privacy protection and AI regulation, and traditional market access issues—such as the rules for cross-border data flows—in an era of attenuated multilateralism. Many of these digital items touch hot-button political topics for countries involving the implications of digital technologies for civil liberties (e.g., privacy in the EU) or national sovereignty (e.g., monitoring of cross-border data flows in Indonesia). Nonetheless, despite the divisions flagged by these political sensitivities, there is much common ground among countries (and within the *Digital Mittelstand*); however, formal binding rules for the international market could be hard to achieve.

In an era featuring the virtues of a regime complex, these issues often went into institutions with very little power to set binding rules for global commerce. An emphasis on regime complex approaches permitted countries to negotiate with a focus on broad performance metrics to move along efforts at cross-national regulatory coordination. This was a form of "soft law," emphasizing functional capacities rather than specific market rules.[44] In this approach, national regulators choose implementing modalities (and choose among their practical tradeoffs), but agree on predictable parallelism in the rough parameters of national regulatory approaches. This reduces the worst contradictions and variances among national rules, thereby allowing interdependent technology markets to work more effectively. Sometimes this soft law approach is tied to a trade agreement with a credible dispute settlement mechanism that can enhance the significance of the soft law. Even lacking a trade mechanism for dispute settlement, as with the Asia-Pacific Economic Cooperation (APEC) digital technology principles, the negotiated agreement on common approaches reduces regulatory tangles for regional markets. Moreover, broad sets of global principles (like the OECD privacy principles) may be cited as foundational starting points for reconciling divergent regional and national governance regimes, whether for privacy or AI.[45]

The question was whether newer institutional frameworks like APEC or some other entity could create a viable platform for common framework principles endorsed by countries such as India and Indonesia. Certainly, the growth of various regional international trade agreements, featuring significantly different levels of policy ambition, suggested both institutional fragmentation and an opening for policy experimentation.

Uncertainty about the specific implications of digital technology for good governance and greater emphasis on narrower international commitments in regime complexes is leading to more embraces of experimental governance that stress the need to rethink the fit between various governance structures and technological and market realities. This is important when there are fundamental uncertainties about the technology itself and what arrangements best steer it toward tackling public interest needs.

Global experimental governance sets overall ambitious goals for longer-term results as targets with political (and perhaps some legal) commitments, but emphasizes bottom-up (local and national governance systems) and frontline (e.g., private sector and civil society) experimentation to figure out the means and adjust the interim performance expectations in a system of repeated feedback and sharing of best practices. Participation by a wide array of government and nongovernment actors to feed learning and build legitimacy is crucial. The evolution of these participation practices is a key part of the system. Sanctioning exists for a country falling behind on performance, but it most frequently emerges in the form of reputational costs in markets, because falling behind broadly understood feasible performance expectations weakens investor confidence.[46] Sometimes, sanctioning can take the form of the withdrawal of comity by another national regulator, which will deem the lagging country to pose higher risks on, for example, safety or technical reliability. It then imposes greater scrutiny on its products and services.

The emerging international framework for AI technology endorsed by former U.S. president Joe Biden showed some signs of experimental governance.[47] There was little sign of binding global agreements on AI governance despite the EU's internal AI rules serving as one such template. There was substantial uncertainty about what forms of regulation would prove most effective, and there were disagreements about how to balance a variety of end goals. Instead, there were promising approaches assembled into a kind of grocery cart of options to address broad baskets of necessary tasks, such as those articulated at the OECD. As a result, as two scholars argued, international regulatory diversity was high and the transactions costs imposed were considerable. Nonetheless, "what is needed far more in such a phase of regulatory uncertainty is rule diversity and the regulatory experimentation that ensues … perhaps we need different institutions altogether to aid in this."[48]

As coordination is more fragmented in its institutional formats, relies more on soft law and dips into experimental solutions, one other consequence is likely. Governments move more of the contentious market disputes from international dispute resolution mechanisms to national government and private governance arrangements. For example, judicial dispute mechanisms at the national level (or even private arbitration arrangements) become more important for sorting out heated conflicts over the financial terms for licensing key patents embedded in international digital standards (called standard-essential patents), as I discuss later.

Prior to President Trump, the global digital regime seemed headed to placing greater emphasis on sovereignty norms along with more institutional tinkering and complexity. However, there were political-economic formulas that still permited a fair amount of commonality in the government "policy guardrails" and implicit norms of the global digital market. Many of the norms would reinforce concepts of best practices. The guardrails reflecting stricter political and legal commitments seemed likely to be more selective and emphasize the leeway for bottom-up governance experiments within the guardrails. The variety of mechanisms for "enforcement" and dispute resolution were increasing. Within this mix there was a path forward that was consistent with substantial global interdependence and technological progress. It was likely to be a less economically efficient regime, but need not have been intolerably so.

This sketch of evolving dynamics included more contingent and complex forms of international governance. The Trump administration seems more interested in a rapid dramatic change in rules governing trade and investment in goods, such as semiconductors and autos. It is less geared toward rules for commerce in software, cloud computing, AI, and services, although presumably there will be strong security provisions. Its dramatic roll out is said to have led to a permanent decline in trust in American leadership in formulating rules for the world economy, an escalation of the erosion of multilateralism under Biden. What remains hard to fathom in the almost daily revisions in major parts of the policy is whether the economic pyrotechnics yield a set of settlements that "speak prose," a set of individual bargains with significantly common features in regard to the digital economy. The United States Trade Representative has identified digital economic issues as an item for all negotiations. The Trump administration's emphasis on racing to sustainable AI leadership by massive investment and technology sharing deals in Saudi Arabia and Qatar may also set

a model for incentivizing closely governed, “minilateral” investment clubs for AI. Whether accelerated investment agreements would imply some common guidelines on best practices for safety that went beyond security controls regarding China is an open question. The next section illustrates how some challenges could be addressed. Whether or not they will be is difficult to forecast.

5. Six Examples of How to Manage Challenges for the Digital Regime

To illustrate the possibilities for managing the digital ecosystem, the rest of this paper invokes precedents and examples for what might emerge. One is the construction of the global aviation regime as a precedent for creating an alternative path to reconcile sovereignty norms, technical coordination, and market interdependence. I then follow with five brief examples of possible responses to the policy challenges for the future digital regime.

A. A Precedent for Addressing Digital Sovereignty Claims: How Aviation Emphasized National Sovereignty While Permitting Technical Coordination and Market Liberalization

Even as data, software, and complex information technology systems operate pervasively on cross-border information systems, concerns about data security or privacy become more prominent. At the same time, geosecurity and industrial policy concerns reinforce demands for the right to control who enters a market and the terms on which they operate. A particular issue of deep resonance to many public officials is “data sovereignty”—who gets to control data on what terms. Those focused on data sovereignty often conclude that data must be confined to nationally located facilities. However, the adverse implications of sovereignty for regime design and interdependence are often exaggerated, as the history of international aviation demonstrates. Aviation had a far less efficient world market for a long time, but it successfully overcame acute fears about sovereignty (reinforced by industrial policy) to slowly build an interdependent global market.

The global aviation regime illustrates how market liberalization can occur in a different format than is typical for international trade. Sovereignty rights and a form of industrial policy intermingled with technical coordination globally to

produce steady growth in market interdependence combined with massive government intervention.[49] This was far from an optimal economic path, but it was a realistic political-economic compromise. This brief case study lays out lessons from the aviation regime.

As the practice of flying over countries to reach a destination started to become more pervasive, sovereignty questions escalated. The solution was simple, even if it took some time to formalize. International conventions affirmed each country had full sovereign control over the air space above its territory. However, as a practical matter of allowing international aviation, countries created a convention to grant safe passage to foreign civilian aircraft who complied with safety and security requirements, such as filing a flight plan covering their foreign passage (military aircraft were under separate rules). At first, coordination arrangements were regional with the Americas and Europe operating as separate efforts. World War I and improved aircraft technology led to the recognition that coordination had to become global.

The international air traffic control system was harmonized to make a safer system economical by having the same practices everywhere. Significantly, much of the safety work was in a delegated authority to global airline carriers' organization (the International Air Transport Association, IATA) and an international aviation safety authority (the International Civil Aviation Organization, ICAO) which had the needed expertise.

Liberalization of international aviation took a very different path from trade in goods and commodities. Governments saw their national airlines as a form of industrial policy (or public utility) to be zealously nurtured. National control and detailed bilateral government agreements covering which foreign airlines could land or takeoff on which terms was the baseline for market organization.[50] IATA also became the co-designer with governments of market access in order to induce similar pricing and services on any route. This protected the often precarious economics of "national flagship" carriers. It also reinforced the tendency of major aircraft supply decisions to become entangled with broader foreign policy issues.

Later, technological change compelled reforms favoring more competition and greater interdependence. The introduction of large-capacity jet transport that could fly long distances induced a revamping of interests, and thus policies, about competition. There are still many forms of government control (including safety regulation), but the terms for serving the market now allow for more

flexible service and pricing options. Governments deemed the cost of full-scale protection of flagship carriers to be unacceptable in a world of globalized commerce. Allowing for more competition, countries also permitted cross-border carrier mergers and global air carrier alliances (joining together diverse national carriers into service groupings) that compete with each other. A few of these alliances now dominate global travel. Governments monitor the alliances for many reasons, including oversight of which carriers on what terms make up the alliance.

The international aviation regime is one template of how to reconcile sovereignty and security with the advantages of relatively open global markets. The history of aviation points to the importance of dividing up the issues and their solutions very carefully in order to improve the potential for interdependence even while protecting industrial policy and security priorities. Market liberalization, security safeguards, technology coordination, and safety rules each had specialized arrangements.

We can use aviation to imagine some possibilities for a world where the diffusion of global economic power, rising geosecurity concerns, industrial and regulatory policy, and the changing technological contours of digital markets lead to more regime complexity of specialized governance, experimental governance, and reliance on "performance" standards. However, unlike aviation, such governance changes will occur in a world that is already enmeshed in the *Digital Mittelstand*. Globalization will persist but may be modified in its specific organizational modes.

As thought experiments, we can think about four challenges in global digital governance—digital service trade rules, cloud computing, cross-border privacy rules, and data security rules. Together, they show evolving responses to evolving the digital regime.

B. Trade Rules for Digital Services

Digital services weave together the *Digital Mittelstand*. Their evolution is an example of coordination based on performance standards to permit market integration. They also reflect over time the growing role of "middle powers" in creating the trade agenda in specialized governance arrangements, especially as traditional economic powers exhibit inconsistent strategies and big digital companies work to define viable expectations for the global market.

Starting with the 1997 WTO agreement on telecommunications and information services, trade negotiators joined with the national regulatory authorities of newly liberalizing markets to focus specially on regulatory principles for global communications and information services. These principles were essentially performance requirements (soft law) for national regulation.[51] Indeed, the key working party was led by the Hong Kong telecom regulator (before Hong Kong had been returned to China). For example, the regulation of telecommunications markets had to be done by a government authority independent from the market participants. The organization and scope of the authority (independent commission or government ministry, for example) was up to each country. The principles comprise a set of performance requirements for national arrangements that every party agrees is necessary for the market to work well; there are many policy paths to fulfilling the obligation, and national rules are subject to continual political economic bargaining and genuine learning about how best to regulate digital markets.

Digital service markets evolve. The more prominent role of cloud computing and big data, along with stronger attention to the digital roles of small and medium-sized firms, were key commercial factors. The need to address prominent concerns over privacy and cybersecurity also prompted interest in policy innovations. This led to innovative proposals by the United States for digital services and e-commerce initiatives in the Trans-Pacific Partnership (TPP) and later at the WTO.[52] For example, the United States proposed a trade in services agreement as a plurilateral that would dodge some of the traditional features of multilateralism (under WTO service rules a plurilateral did not require most-favored nation treatment for countries not participating).

Then, populist political decisions reversed American trade positions, beginning with the rejection of TPP and then decisions by the Biden and Trump administration on digital services trade. A policy void existed.

Similarly, while coordination incentives still drive the global work to set technical standards and achieve some degree of regulatory coordination, rising uncertainty creates stronger political oversight and potential for conflict. Because so many first-mover solutions (and their operating implications) arose from the United States, this resulted in frustrated EU regulators trying to reign in these digital technologies. The EU implemented sweeping new rules on

competition policy and other implications of digital platforms. Some of these reflected the kind of policy uncertainty created by the rapid pace and diffusion of digital innovations touching broader swaths of the economy and society.

However, many of the provisions of regulation had a penchant for sorting out penalties and obligations based on the scale of the digital firm. Skeptical U.S. officials have noted that these thresholds primarily effect American firms. The EU regulations for artificial intelligence have slowed the commercialization of rapidly changing waves of new AI capabilities in the EU. This again raised questions about whether the policy mix was implicitly designed to protect smaller European latecomers. It also garnered second thoughts among some experts about whether Europe could catch up if the AI ecosystem primarily innovated outside of the EU. The emergence of China's DeepSeek further muddled this debate.

The EU engaged in economic diplomacy to persuade other countries to follow its regulatory model. Especially given the absence of a coherent formal American model of digital regulation, this attracted great political sympathy in many countries trying to navigate the issues invoked by digital technology. This led to a strange dance—many governments broadly endorsed EU principles, but only selectively implemented them for particular security or industrial policy goals. This meant there were many national examples of taxation of foreign digital service firms and requirements for the localization of data storage and cloud computing infrastructure, which I discuss in more detail shortly.[53]

Asia-Pacific authorities also demonstrated greater deference to speeding digital innovation rather than worrying over all of the regulatory details. This reflected their interest in being stronger players in the *Digital Mittelstand*. This is why Japan, Singapore, Australia, and New Zealand have had success in rallying support for a more permissive approach to digital trade than the strictest interpretation of EU digital rules would likely support.[54] All of the proposals set up a presumption that digital markets among a minilateral group should be generally open and nondiscriminatory. But they feature detailed provisions for national regulatory exceptions. And their biggest innovations—complemented by the work of APEC on digital market principles and coordination mechanisms—are to begin applying the template of mutual recognition agreements to digital trade.

Under mutual recognition, countries can examine whether data flows meet the quality performance objectives in the trade agreement for privacy and security. But it goes one step forward by endorsing the evolution of a system where one country's system for certifying compliance can be accepted as sufficient by another country.

To have consequence beyond being an interesting experiment will require collaboration among national regulators on what constitutes an adequate certification process, much as has happened in pharmaceuticals among some countries. Not every country's system will be accepted by every other country. Countries who are not in the trade agreement are not even eligible for the certification option. This kind of experimentation in a new specialized agreement is exactly the type of experimental government challenge that is responsive to a broader coalition of middle-tier economies that a future digital regime should welcome. It is also most likely to emerge, if ever, in a variety of specialized agreements—not sweeping global deals.

All of the above occured before the advent of the Trump administration. Its emphasis on using tariffs to resolve all American objections to bilateral trade, investment, and regulatory disputes introduced a new dimension to the digital services negotiations. Although there is no clear official policy, early indications are that the administration will impose tariffs on, for example, European Union goods if it determines that EU digital competition rules de facto discriminate against American firms.[55] The administration would likely choose its tariff targets for maximum pain. As the discussion of the *Digital Mittelstand* showed, some prominent European suppliers of digital services and software also have manufactured products.

This would be a novel tool for addressing a nontariff barrier in a policy field (domestic competition policy) where trade policy has only very selectively been used.[56] In response, the EU has hinted that it would use its standby authority under the Anti-Coercion Instrument to impose tariffs or restrictions on operating licenses of foreign (i.e. U.S.) firms if the EU interpreted Trump tariffs as a form of illegitimate coercion.[57]

The potential U.S.-EU confrontation is important as a policy marker for its potential to set some new limits on the growing thicket of digital regulations (and taxes) that often primarily apply to foreign firms. This might nudge countries into more ambitious embraces on coordination through soft law or new institutional arrangements (such as the discussion of privacy will highlight). Of course, escalating uses of tariffs and other countermeasures could also tear the seams of digital interdependence. The next section looks at a narrower example of how the political economy of a key part of the global digital infrastructure is evolving.

C. Sovereignty, Corporate Strategy and Cloud Computing

Industrial policies often produce great political tensions even under global economic rules that seemingly guarantee nondiscrimination and market access. In an era of digital uncertainty we should expect many cases where the rules on market access and regulatory conduct are either vague or often subject to creative interpretation. Achieving some predictability at a regional or global level is a governance challenge.

A classic example of corporate strategy in managing such trade tensions occurred when demands for protection of local auto manufacturers (or assemblers) were a major political reality even during the growing tide of liberalization of trade under the 1947 General Agreement on Tariffs and Trade (GATT). This could have exploded into major trade conflicts. However, a key policy compromise—somewhat imperfect liberalization of foreign direct investment rules for auto manufacturing—intersected with sophisticated strategies by the big auto companies to parse out varying levels of local production.[58] Really big markets got more extensive auto manufacturing setups. Smaller, but not tiny, markets got some form of automotive assembly operations relying on imported content for the parts. Over the years, various cross-border joint ventures also emerged in some markets. The well-understood strategies of the big auto firms helped to stabilize fragmented governance arrangements. When Japanese auto companies finally became a major global force, they initially failed to play this strategy. As a result, the U.S. and Japanese governments got into major trade disputes until firms like Toyota conceded the need for big American production plants.

Today, the biggest cloud computing firms are incorporating somewhat similar tactics into their global strategies. Their official policy positions endorse the right to invest and operate cloud data centers according to technical efficiency and normal business criteria. They also oppose restrictions on the free flow of data among these centers—a key piece of cloud computing architecture is redundancy for resilience and distributed location for less latency in response times, and the economics of the cloud are optimal at large economies of scale. Governments, sometimes grudgingly, acknowledge the technological dynamics of the cloud. Nonetheless, for reasons of sovereignty protection (security or sensitive personal data) they may not want to commit their data to big cloud networks that distribute data collection globally. Sometimes, they emphasize cloud facilities that operate at scale and then basically wholesale space and operational support to computation and data storage equipment of smaller (often local) companies (a global firm like Equinox is good at this business). The "hyperscalers" who operate giant facilities of their own will also adapt. While offering a variety of rationales, the big cloud firms sometimes agree to put a large cloud center in a major national economy's territory and make provisions for some data to stay local. This is a strategy to reconcile the policy on paper and operations in practice.

The story of the cloud in the European Union is telling. Amazon first emerged as an e-commerce giant but makes its biggest profits from an almost accidental insight that it could create the cloud computing market. Cloud computing fundamentally changed the cost and organization of computing. A belated EU effort to create a European alternative foundered because governments could not move as decisively and private capital markets could scale up funding to amounts that were not readily available in government budgets. So, the EU had to settle on working to better unify the internal EU market for cloud computing while using R&D funds to encourage specialized innovation within the cloud ecosystem. The big cloud firms (Google, Amazon, and Microsoft primarily) were then subject to continual competition scrutiny.

The EU is belatedly trying to encourage European firms to catch up in an exploding global cloud market. The estimated number of new Cloud data centers built in Asia from 2021–24 was 500.[59] There are new data sovereignty rules of various levels of strictness in countries such as Indonesia and Vietnam. In response, not only does the exploding variety of cloud facility formats allow more flexible mixes of local control or global networking, but the cloud providers

can also customize the data flows to national rules. For example, some data will only flow within cloud facilities and users within the Association of Southeast Asian Nations (ASEAN) region. Many of the distinctions about data flows are fairly similar to the ones made in OECD and APEC privacy principles. The more significant challenges for global cloud companies do not directly involve access in most cases. They center around other types of issues, such as specialized national technical standards (an issue that arose in aviation's evolution) and the wider scope of competition scrutiny imitating the EU's digital competition rules that complicate but do not stop access.

The point here is that liberalization occurs within rules emphasizing national sovereignty in many cases. This kind of detailed oversight of technical coordination and liberalization is reminiscent of the aviation regime. It does not necessarily require a trade agreement of the traditional type. Instead, the model might look more like the one just described for trade in digital services.

D. Specialized Delegation of Dispute Settlement—National vs. International Authority

How decisions get made is a key feature, and how to resolve disputes is one key element in a regime. Digital governance is likely to require a wider variety of mechanisms than trade dispute settlement to impose penalties and settle disputes.[60] The complexity of the technical problems and caution about handing over authority to intergovernmental mechanisms has accelerated a trend that has already gained momentum in environmental governance.[61] Given the importance of standards and intellectual property in digital technology, it is worth considering how dispute settlement may evolve.

Digital technologies standardize by blending the intellectual property offerings of many stakeholders. Receiving a standard-essential patent requires the holder to grant a license for its use on terms that avoid a monopolist's temptation to require exorbitant compensation. The patent holder must agree to license the patent on fair, reasonable, and nondiscriminatory (FRAND) terms to anyone wishing to use it.

Given the potentially large economic stakes and the generality of the principles, there are often heated debates about the correct framework for implementing FRAND. For example, many scholars emphasize that fair is a difficult concept to operationalize, but nondiscrimination is a legal and economic concept that is somewhat more tractable.[62] Efforts, such as one by the EU, to create international formulas to set FRAND terms have been rejected by other governments. A similar move by China has not had far-reaching impact outside China.[63]

Instead, the FRAND system has parties rely on commercial bargaining to work out individual licensing terms. Importantly, the terms of licensing vary based on the specific assets of the parties. The deals can be complex. For example, sometimes cross-licensing of patents substitutes for a licensing fee (cross-licensing may then lead some of the biggest firms to emphasize building the biggest portfolio of "high-quality" patents to increase their bargaining position). While parties bargain carefully, most deals get settled without much drama. Sometimes, when the parties are large (so the money is big) and the precise circumstances are fairly unusual, the licensing negotiation breaks down and matters end up in courts or specialized international trade agencies of individual countries (rather than, say, the WTO). For example, if there is no licensing agreement on a U.S. patent that is incorporated in a foreign product import, the International Trade Commission can exclude the import from the U.S. market. The fact that this could happen, but might not, is an incentive for the parties to compromise.

As we shall see with privacy rules, the use of national dispute settlement systems is vital for specialized bilateral disputes. The larger lesson is that complexity and learning make the digital system more reliant on private bargaining than standard government formulas. But the means of holding the private arena in some boundaries relies on national enforcement powers, not a global institution.

E. Privacy Rules, Institutional Experimentation, Delegation to Frontline Actors, and Alternative Dispute Resolution

Divisions in regulatory approaches of privacy protection are among the most prominent points of discussion about global digital rules. This is rightly so. They speak to some fundamental disagreements over policy goals and reflect big differences in how national policy processes sort out complicated debates.

Yet, despite the splits, there is also evidence on how carefully designed delegation and institutional tinkering, even as the result of heated diplomatic clashes, can start to find solutions. These cases reflect experiments in governance, institutional specialization, delegation, and dispute resolution.[64]

The standard view of the EU's General Data Protection Regulation (GDPR) privacy is that it is more powerfully cohesive than fragmented rules of the United States and more ambitious in its goals. In rhetoric, if not fully in practice, many other countries have adopted the EU template in the absence of appealing templates from the United States or China. And the EU insists that its privacy protection has extensive overseas implications that it tries to enforce. This has led it to high-profile diplomatic disputes with the United States over the enforcement of these policies in transatlantic data flows involving U.S. firms. Thus, EU privacy policy is a strong affirmation of sovereignty rights for industrial and regulatory policies.

It is less noticed that the GDPR privacy regime for the EU coexists with massive flows of global personal data across the Atlantic under "standard commercial contracts," because both European and American companies need the data exchange.[65] For example, the OECD's privacy principles, first set in the 1980s and amended periodically, are not as extensive as the EU protections, but anticipated many of the issues on how to balance privacy and commercial functions.

As a result, GDPR has provisions to deal with commercial use of personal data in international data flows. Of course, GDPR allows for data collection to which the user explicitly consents. But beyond individual consent, GDPR allows five categories of "commonly accepted" information collection and use for firms: product fulfillment, internal operations, fraud prevention, legal compliance and public purpose, and first-party marketing. Writing detailed implementation codes for these provisions in each industry would exceed bureaucratic capacity. Therefore, the EU allowed companies in each major economic sector to create a workable template for permitting cross-Atlantic data flows consistent with GDPR. The expertise is in industry, but accountability to the EU remains. This is an instance of delegated authority.

Meanwhile, bilateral (often contentious) regulatory coordination takes the form of the United States promising that its different sets of privacy rules and practices will still support the purpose of the GDPR protections. Although disputes on business conduct have arisen under the standard commercial contracts, the highest profile cases are not about business as usual. They are mainly tied to delicate civil liberties cases, especially national security monitoring by U.S. agencies of European citizens.[66] European courts have been skeptical of various U.S. pledges of privacy protection on these cases.[67] The result is institutional innovation that is very particular to the bilateral relationship. It is contingent contracting in its highly specialized scope and the right of the EU to effectively back out. For example, the EU now has representation inside the U.S. State Department to address special cases and there are special guarantees and venues for dispute resolution.

There is still some uncertainty whether the European Court of Justice will accept even the newest bilateral arrangement even though the Commission has embraced it. Assuming that this specialized governance is sustained, the question is whether it is a working template for other conflicting privacy codes and cross-border data flows. This format really depended on a substantial level of security alliance between the two parties due to the sensitive intelligence operations involved. That security bonding is often not present. As the discussion of digital trade showed, it may be that other institutional mechanisms for reconciling variations in national policy may be more practical. One encouraging factor is that the EU rules are consistent with much of the working logic of the commercial principles for data privacy spelled out in international organizations like the OECD and APEC.[68] In its early days, the Trump administration has yet to challenge the privacy agreement and its institutional arrangement. As with digital trade in general, the question is how sweeping is the Trump ambition to curb other economic powers' domestic regulatory policies that require adjustment costs by American firms.

F. Security and Data Flows in All Digital Technology

If everything is somewhat digital, it is useful to ask how much cybersecurity protection—and of what kind—is necessary. How is it compatible with international interdependence in digital markets? The politically sensitive market for EVs provides evidence of the clashes over coordination and some hints about how the use of modularity and new forms of regulatory coordination

might address the issue. The fate of the Chinese EV industry in the United States and the EU, and that of American EV makers in China, can provide insights into the option.

As the aviation case demonstrated, it is important to recognize the difference between industrial policy and security incentives. The U.S. tariffs on Chinese vehicles appear designed to preclude all Chinese entry for industrial policy reasons. The EU has to balance protection of EU manufacturing with the massive stake of German carmakers in China. So, its tariffs may evolve to allow Chinese auto manufacturers to operate through local auto manufacturing in the EU.[69]

Even if the tariffs for industrial policy permit Chinese auto production in the EU, data security remains a crucial issue. The United States fervently raises warnings that are remarkably similar to those expressed by China about Tesla. So, it is useful to consider EV data security as a test of what might occur in the most restricted cases of data flows due to security issues. We can think of this as the "Tesla Option."[70] It developed even before the election of Donald Trump and the peculiarly prominent role of Tesla's chief executive officer Elon Musk in his administration.

For any EV producer, data gathering is critical for several reasons. For one, a good deal of the value added (and profit margin) in EVs is in the software and digital control stack of the car—EVs are rightly characterized as computers with wheels. Everything is monitored for performance optimization, including batteries. Therefore, EVs are sources of many forms of powerful data. Even leaving aside worries of spying or sabotage by Chinese vehicles, tensions can arise over the profits generated by digital systems and data. Automakers (like GM) and Apple can bicker about the respective roles of CarPlay and systems designed by the automaker because the software system is key to a variety of service revenues over time. (Similarly, Xiaomi of China is trying to be a new CarPlay.)[71] Yet, the fungibility of software is a feature of digital modularity and could play a key role in security policies.

Tesla has struggled with Chinese government concerns over its accumulation and use of data, with possible security implications, for several years. In spring 2024, it struck a deal to resolve the issues that deserves careful attention.[72] In May 2021, Tesla took a first step to respond to data sovereignty issues when it announced that it was building its own data center in China in order to

demonstrate that it would comply with regulations requiring local data storage. Nonetheless, even after that measure, Tesla vehicles had been restricted from entering military bases or other sensitive government locations out of security concerns and an official concern over protection of consumer privacy.

In late April 2024, Elon Musk met with Chinese Premier Li Qiang (who had championed Tesla's entry into China via foreign direct investment) to strike a deal. *Bloomberg* reported the outcome resolved the government's worries in this way: "the data security tests included how a vehicle collects "sensitive personal information" and whether a driver can easily stop a car from collecting data, the China Association of Automobile Manufacturers said in a statement late Sunday."[73] Among the specific guarantees were that Tesla would anonymize data from auto sensors that observed license plates or people's faces.

This arrangement was easier because it created a financial incentive for Tesla to adopt the use of Baidu mapping software in its vehicles. This assured Chinese regulators that the vehicle data would not only stay in China, but it would be using a complex software system that fit the country's security guidelines. The financial incentive for Tesla was straightforward. Until now, it had to rely on its cars' camera systems and use lower-quality mapping data to guide its smart vehicles. Baidu is one of 20 Chinese firms permitted by the government to use higher resolution mapping data for commercial purposes. By adopting the Baidu system, Tesla boosted Baidu as a world player in that space. In turn, the higher-quality mapping data let Tesla win approval from the government to activate its Full Self-Driving (Supervised) system. This system is offered as a $99-per-month upgrade option on a Tesla, a major boost for their profit margins just as Tesla faced much stronger competition requiring price reductions. It also meant that BYD, its biggest competitor, and NIO could not pull ahead on self-driving options.

The high level of political engagement in this negotiation also points to an experiment on using this approach as a negotiating offer for Chinese EV vehicles seeking entry into the OECD countries. One could imagine BYD, for example, seeking to open manufacturing facilities in OECD countries (a foreign direct investment strategy) and then offering to use OECD-sourced systems for mapping data and localized data storage and computing facilities in OECD countries. This offer would take advantage of the growing ability to treat software platforms (or their pieces) as modules that can (with some

cost and engineering effort) be mixed and matched. To supplement modular software swaps, Chinese firms could also offer to duplicate Tesla's commitment to anonymize license plate and facial data, and EU governments could ban the use of Chinese vehicles in government fleets plus restrict their use near security facilities.

To be sure, this approach still may not satisfy critics of personal data protection and security issues involving Chinese products. For example, TikTok offered to use Oracle cloud computing facilities to localize personal data in the United States. The offer on Oracle storage could not resolve accusations that TikTok would use its algorithms to fan disinformation and political divisions in America. However, it had some plausibility on responding to charges that it could export sensitive locational and camera data to China while also gathering data that might be used to embarrass or blackmail influential U.S. citizens. This credibility would be further enhanced if, as some think feasible, it proves possible to tag data sufficiently to allow tracing any movement outside of U.S. boundaries.[74] And, in the early Trump administration, there are strong hints that data localization along with a change in ownership to predominantly American hands might suffice, an indication that some suspicions about mysterious algorithmic threats in TikTok code might be downgraded. (Still, the Trump administration may decide that it simply doesn't want Chinese cars competing against American producers under any circumstance.)

This formula for handling data security emphasizes sovereignty security norms. It is very clumsy and cost inefficient if used for every product or service with digital data elements. Nonetheless, it might be a way of responding with more nuance to security concerns on products where there are many benefits of interdependence even if security controls are stringent. It would be a form of "small yard, high fence" for technology security that did not rely on banning the technology products in question.

Efforts for products with real, but lower, risks might be subject to security best practices organized on the format of the GDPR and its delegation of compliance to standard commercial contracts for industries.[75] One could imagine diplomacy to announce parallel unilateral national criteria for such standard contracts on some products. Each party would retain the power to enforce (or abandon) the contract terms. But some level of parallelism would permit market integration to a certain degree even under security norms.

Conclusion

These examples of possible evolutions in digital governance are not a surrender to wild fragmentation in rules, norms, and decision channels. There may be gains from more innovations in governing ideas and mechanisms. But there is also a price to pay for these changes. More generally, focusing on the implications of the *Digital Mittelstand* should make us aware that there is more order buried under the tensions and disputes than commonly recognized. It is just a somewhat different kind of order and it could use some imaginative nurturing to help us achieve the best of the potential of digital technology. Whether the United States will pursue policies that nurture these possibilities is a central question for the Trump administration.

Endnotes

[1] The standard array of early papers on regime theory is Stephen Krasner, ed., *International Regimes*, Cornell University Press, 1983.

[2] These are semiconductors, software (platforms and specialized applications), Cloud computing, big data, big data broadband network delivery systems, e-services (ranging from financial through entertainment and logistics), and AI. Complementing these functions are the specialized suppliers to these products and the sprawling next generation of creators such as additive manufacturing, sensors, and the creation of digital twins.

[3] A good overview of the changing priorities and the policy tradeoffs from a U.S. leader is Michael G. Froman, "The Next President and the Tradeoffs in U.S. Economic Policy," *Foreign Affairs*, October 3, 2024.

[4] A gloomier forecast is "The New Economic Order," The Economist, May 11, 2024, p. 7. Another pessimistic view is Dani Rodrik and Stephen Walt, "How to construct a new global order," *Oxford Review of Economic Policy*, Vol. 40, 2024, pp. 256-268.

[5] Brian Schwartz, Gavin Bade, and Josh Dawsey, "Trump's Economic Messaging Is Spooking Some of His Own Advisers," The Wall Street Journal, March 11, 2025; Matina Stevis-Gridneff, "Tariff Pain First, Deals Later, U.S. Tells Canada," New York Times, March 15, 2025, p. A9.

[6] Scott Galloway, "Online/Offline," *No Mercy / No Malice*, September 20, 2024.

[7] This was a major observation of Mario Draghi's 2024 report to the European Commission. Three EU economists also note that the United States left big-bet research in the hands of science leaders who were not biased toward incumbent firms. Philippe Aghion, Mathias Dewatripont and Jean Tirole, "Can Europe Create an Innovation Economy?" Project Syndicate, October 7, 2024.

[8] Suzanne Vranica and Miles Kruppa, "Google's Grip on Search Slips as TikTok and AI Startup Mount Challenge," *The Wall Street Journal*, October 5, 2024.

[9] For an explanation of the limits of the power of digital platform companies see Jonathan A. Knee, *The Platform Delusion,* Penguin Portfolio Press, 2021.

[10] Kevin Roos, "Shutting out Social Apps?" *New York Times*, October 7, 2024, p. B1.

[11] Eric Thun, Daria Taglioni, Timothy Sturgeon, and Mark Dallas, "The emergence of 'massive modularity' as a new form of industrial organisation and what it means for decoupling and international trade policy," Centre for Economic Policy Research, March 17, 2023.

[12] Microsoft stumbled despite its advantages until a new chief executive officer shifted the business model away from being Windows centric. On the decisions on what to integrate as a core technology and the dangers of not reinventing business models regularly, see An Interview with Google SVP Rick Osterloh About Pixel, Android, and Smartphone History, *Stratechery*, Thursday, August 15, 2024.

[13] A clear exposition of modular design in software is Sanjoy Kumar Malik, "A Gentle Guide to Modular Software Design," LinkedIn, posted October 12, 2024.

[14] Peter F. Cowhey and Jonathan D. Aronson, Transforming Global Information and Communication Markets: The Political Economy of Innovation, MIT Press, 2009 and Peter F. Cowhey and Jonathan D. Aronson, Digital DNA: Disruption and the Challenges for Global Governance, Oxford University Press, 2017 detail the cases.

[15] For one sophisticated analysis of the complexities of the app store competition case and proposed remedy involving Google, see "Google's Play Store Remedies, The Injunction, The Power of Network Effects," *Stratechery*, posted October 8, 2024.

[16] Daniel Drezner, "How Everything Became National Security," *Foreign Affairs*, September/October 2024 has observed the tendency for everything to become security questions. He urges various methods to prioritize among them.

[17] Mark MacCarthy, *Regulating Digital Industries*, Brookings Institution Press, 2023.

[18] "The Top 100 'Mittelstand' companies 2018," Munich Strategy, February 2019.

[19] Siemens spent $10 billion to purchase Altair, a software design firm specializing in simulation to upgrade manufacturing processes and products (after spending another $10 billion on smaller software firms) with the ambition to increase profit margins and differentiate its offerings. Information from Bloomberg Industrial Strength, quoted in Adam Tooze, "Top Links 552 Nasty bonds on underwater office buildings. Indian top earners in Germany. Avian flu & U.S. military food insecurity," Chartbook newsletter, November 5, 2024. Other scholars note that robotics are a key factor that differentiates firm productivity gains in the EU. Joel Stiebale, Jens Suedekum, and Nicole Woessner, "Robots and the rise of European superstar firms," International Journal of Industrial Organization, Vol 97 (2024) 10385.

[20] "America's internet giants are being outplayed in the global south," The Economist, January 9, 2025.

[21] "Cross-Border Data Flows: A Review of the Regulatory Enablers, Blockers and Key Sectoral Opportunities in Five Asian Economies: India, Indonesia, Japan, the Philippines, and Vietnam," Asia Cloud Computing Association, 2018.

[22] Eric Flaningam, Substack August 18, 2024, https://substack.com/@ericflaningam/note/c-65871271?r=1y2s6&utm_medium=ios&utm_source=notes-share-action.

[23] Cowhey and Aronson, *Digital DNA*. *Digital Twins: The Foundation of the Enterprise Metaverse*, McKinsey Digital, October 2022. "Off to the Races," *The Economist*, August 31, 2024, pp.63-66.

[24] This is the implication of the work on transatlantic technology relations of Henry Farrell and Abraham Newman, *Of Privacy and Power: The Transatlantic Fight over Freedom and Security*, Princeton University Press, 2019.

[25] While my interpretation is somewhat different, Dan Breznitz and John Zysman offered similar thinking about technology parameters embodied in code in John Zysman and Dan Breznitz (eds.), *The Third Globalization: Can Wealthy Nations Stay Rich in the Twenty-First Century?* Oxford University Press, 2013.

[26] Jonathan Hillman, *The Digital Silk Road: China's Quest to Wire the World and Win the Future*, Harper Business, 2021, Chapter 6, estimated the EU share of the market capitalization of the 70 largest digital firms at less than 5 percent. This overlooks other EU digital strengths but it is a politically important symbol in Europe.

[27] This is a finding of Mario Draghi's influential report to the EU Commission, *The future of European competitiveness*, European Commission, September 2024.

[28] A good example is Cristina Caffarra, "Europe Must Break Free from Its Digital Dependence," Project Syndicate, posted March 12, 2025.

[29] Susan Shirk, *Overreach: How China Derailed Its Peaceful Rise,* Oxford University Press, 2022.

[30] Rush Doshi, *The Long Game: China's Grand Strategy to Displace American Order,* Oxford University Press, 2021. Barry Naughton and Briana Boland, *CCP inc.: The Reshaping of China's State Capitalist System*, Center for Strategic and International Studies Report, January 31, 2023. Barry Naughton (ed.), "Re-Engineeering China's Innovation Machine," Supplemental Issue of *Current History*, Vol. 123, 2024.

[31] *The Economist* has noted that the shares of big data centers globally divide up to 52 percent in the Americas, 28 percent in the Asia-Pacific, and 20 percent in Europe, the Middle East, and Africa. "Splashing the Cache," *The Economist,* February 8, 2025, pp. 51-52.

[32] On U.S. trade reversals on digital tech see Michael L. Beeman, *Walking Out: America's New Trade Policy in the Asia-Pacific and Beyond,* Walter H. Shorenstein Asia-Pacific Research Center, 2024. On credibility and its implications for regimes, see Peter F. Cowhey, "Domestic Institutions and the Credibility of International Commitments: The Cases of Japan and the United States." *International Organization,* 47 no. 2 (1993) 299-326.

[33] David Kreps, "Corporate Culture and Economic Theory," in James Alt and Kenneth Shepsle, eds., *Rational Perspectives on Positive Political Economy*, Cambridge University Press, 1990, pp. 90-143.

[34] John Gerard Ruggie, "Multilateralism: The Anatomy of an Institution," in J.G. Ruggie (ed.) *Multilateralism Matters*, Columbia University Press, 1993, pp. 3-47.

[35] Kal Raustiala and David Victor, "The Regime Complex for Plant Genetic Resources," *International Organization*, Vol 58, No. 2, Spring 2004. Charles F. Sabel and David G. Victor, *Fixing the Climate—Strategies for an Uncertain World,* Princeton University Press, 2023. Cowhey and Aronson, *Digital DNA*, Chs. 4-5.

[36] Peter F. Cowhey and Milton Mueller, "Delegation, Networks, and Internet Governance" in Miles Kahler ed., *Network Politics: Agency, Power, and Governance*, Cornell University Press, 2009. Cowhey and Aronson, *Digital DNA*.

[37] Beeman, *Walking Out.*

[38] And national security concerns tend to creep beyond the "high walls, narrow gardens" metaphor often invoked to say industrial policy will be very selective. For example, once governments begin to restructure supply chains, there are many temptations to add just one more item to the security exception list. Even the existing digital infrastructure became contested, as illustrated by Hillman, *The Digital Silk Road*.

[39] Stephen D. Krasner, "Global Communications and National Power: Life on the Pareto Frontier," *World Politics 43*, No. 3, April 1991, pp. 336-366. In contrast, cooperation game logic, like the prisoner's dilemma, suggests that actors have mixed motives because they may most benefit from not joining others in regime support. Theories of hegemonic leadership (by a single or small group of market leaders) relied on observable and persistent predictability of strategic focal points of behavior by the leaders.

[40] Cowhey, Peter F. and Aronson, J.D. (1985) The Great Satellite Shootout. *Regulation: AEI Journal on Government and Society.* 27-36.

[41] Christina Cottiero, Emilie Hafner-Burton, Stephan Haggard, Lauren Prather, and Christina Schneider, "Illiberal Regimes and International Organizations," *The Review of International Organizations*, 2024. Christina Cottiero and Stephan Haggard, "Stabilizing Authoritarian Rule: The Role of International Organizations," *International Studies Quarterly*, Vol. 67, 2023.

[42] See Cowhey and Aronson, *Digital DNA*, on the "3G" standard setting. Nigel Corey, "Europe Goes Protectionist on Global Technical Standards: The Example of "Common Specifications"," Information Technology and Information Foundation (ITIF), posted February 24, 2023. Nigel Corey, **"**France's "Sovereignty Requirements" for Cybersecurity Services Violate WTO Trade Law and Undermine Transatlantic Digital Trade and Cybersecurity Cooperation," ITIF, May 10, 2022. Foo Yun Chee, "EU cybersecurity label should not discriminate against Big Tech, European groups say," *Reuters*, June 17, 2024, 2:21 PM PDT.

[43] The Digital Silk Road, Ch. 6.

[44] Kenneth Abbott and Duncan Snidal, "Hard and Soft Law in International Governance," International Organization, 54, no. 3, Summer 2000.

[45] The United Nations (UN) is also trying to play a role in AI by stressing issues of equity, inclusion, and diverse participation in decision-making in the global community. "Global Digital Compact," A/79/L.2., United Nations, https://www.un.org/global-digital-compact/sites/default/files/2024-09/Global%20Digital%20Compact%20-%20English_0.pdf.

[46] The architecture described here is much messier than the ideal set forward by Stephen Weymouth, Digital Globalization, Cambridge University Press, 2023. Weymouth believes that digital platforms pose problems in privacy, taxation, and competition that can only be addressed by strong multilateral governance measures. My approach expects much looser coordination at the global level and more selective coordination in smaller governance arrangements at the regional or plurilateral levels.

[47] "AI Principles," OECD, https://www.oecd.org/en/topics/sub-issues/ai-principles.html. "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," The White House, 2023. Mia Hoffman, "The EU AI Act: A Primer," Center for Security and Emerging Technology, September 26, 2023. "ASEAN Guide on AI Governance and Ethics," 2023, https://asean.org/wp-content/uploads/2024/02/ASEAN-Guide-on-AI-Governance-and-Ethics_beautified_201223_v2.pdf. Steven Feldstein, "Global Struggle Over AI Surveillance," Carnegie Endowment for International Peace, 2024. Erin Lockwood, "Economic International Organizations' Perceptions of and Responses to Artificial Intelligence Risk," University of California Irvine, 2024.

[48] Viktor Mayer-Schonberger and Urs Gasser, "A Realist Perspective on AI Regulation," Foreign Policy, September 16, 2024. For experimental learning see Holden Karnofsky, "If-Then Commitments for AI Risk Reduction," Carnegie Endowment for International Peace, 2024.

[49] To be clear, no international regime denied that countries had sovereign rights. But the degree to which sovereignty was emphasized as a building block for the regime varied throughout history.

[50] Peter F. Cowhey and John Richards, "Building Global Service Markets: Economic Structure and State Capacity" in Jonah D. Levy ed., *The State After Statism: New State Activities in the Age of Liberalization*, Harvard University Press, 2006. For a deft treatment relying on ideas similar to regime complex and delegation arguments, see Mette Eilstrup-Sangiovanni, "Ordering global governance complexes: The evolution of the governance complex for international civil aviation," *Review of International Organizations*, Volume 17, Spring, 2022, pp. 293-222.

[51] Cowhey and Aronson, *Digital DNA.*

[52] Cowhey and Aronson, Digital DNA and Beeman, Walking Out, esp. pp. 114-123 and 252-255. "APEC Digital Economy and Trade: Outcomes in 2023 and Prospects for 2024 and Beyond," The National Bureau of Asian Research (NBR), February 17, 2024.

[53] A standard list of these regulations and tax schemes can be found in the 2025 trade policy white paper of the Coalition of Service Industries, *Services and Digital Trade are Key to American Technological Innovation and Competitiveness*.

[54] The WTO Initiative on Electronic Commerce, from which the United States suddenly withdrew its endorsement, also had Brazil, Colombia, Indonesia, Taiwan, and Turkey, among others, as supportive participants. Joint Statement Initiative on Electronic Commerce, INF/ECOM/87, WTO, July 26, 2024.

[55] "Defending American Companies and Innovators From Overseas Extortion and Unfair Fines and Penalties," The White House, February 21, 2025. For a critique: Tom Wheeler, "Trump's tech tariffs: From protecting production to protecting Big Tech's profits," Brookings Instiution, March 10, 2025.

[56] For example, the Federal Communications Commission in the 1990s, with the support of the Office of the U.S. Trade Representative, created a policy limiting foreign investment in American communications networks to countries who met a "checklist" of competition policy requirements. Later, this rule was abnegated because the new WTO agreement on telecommunications liberalization covered investment.

[57] Jeanna Smialek, "Europe Expected Some Give-and-Take from Trump. It was Mistaken," *New York Times*, March 14, 2025, p. A8. The international law firm, Crowell, has a succinct review of the EU policy, "The Anti-Coercion Instrument: What Is It and How Europe Might Use It Over the Next Four Years," Crowell, February 4, 2025.

[58] Peter F. Cowhey and Jonathan D. Aronson, *Managing the World's Economy: The Consequences of Corporate Alliances*, Council on Foreign Relations Press, 1993.

[59] "Money Talks: How the data-centre boom became a political battleground," *The Economist*, October 10, 2024.

[60] Critics of international trade and investment often oppose the provisions in bilateral investment treaties that allow parties in a dispute to go to private arbitration. This is happening even as private or nongovernmental dispute settlement rises in other fora.

[61] See, for example, the cyanide code's nongovernmental enforcement mechanism under the UN Environmental Program . Governments reserve the right to impose alternative regulations. Also see Jessica Green, *Rethinking Private Authority, Agents and Entrepreneurs in Global Environmental Governance*, Princeton University Press, 2014.

[62] Dennis W. Carlton and Allen L. Shampine, "An Economic Interpretation of FRAND," *Journal of Competition Law and Economics*, Vol 9 No. 3, September 2013, pp 531-552. Herbert Hovenkamp, "FRAND and Antitrust," *Cornell Law Review*, Vol. 105, 2019-2020.

[63] The EU has recently initiated consideration of a bureaucracy that would dictate these terms in the name of competition. This account relies heavily on the observations of another FRAND policy expert that fit my own experience in the field. Jordan Schneider and Lily Ottinger, "History and Future of Global Patent Policy," *China Talk* Substack, August 19, 2024.

[64] This account draws on Cowhey and Aronson, *Digital DNA*, Chapter 7. Martina Francesca Ferracane, Data governance models and geopolitics : Insights from the Indo-Pacific region, European Institute University policy brief 48, 2022. Peter Swire, "A guide to the attorney general's finding of 'reciprocal' privacy protections in EU," Cross-Border Data Forum, July 25, 2023.

[65] For example, contemporary autos are all networked and auto companies monitor their use and performance routinely, including components like batteries in EVs.

[66] Even in the U.S.-EU standard commercial contracts, the question of government surveillance occasionally emerged. Meta was fined by the EU for not sufficiently protecting private European data from U.S. government surveillance.

[67] One irony is that EU national intelligence services enjoy substantial discretion under the terms of GDPR.

[68] Kenneth Propp has demonstrated that GDPR has not impeded the flow of personal data to China in any major way for commercial purposes: "#AtlanticDebrief – How can policymakers navigate between data war and peace? | A debrief from Kenneth Propp" Atlantic Council, October 7, 2024.

[69] Alan Beattie, "A Divided EU Presents China with Easy Targets, Trade Secrets, *Financial Times*, October 7, 2024. "The Call of Duties," *The Economist*, June 15, 2024, p. 55.

[70] Peter Cowhey, "Strategic Autonomy and Green Supply Interdependence: The Role of Foreign Direct Investment," in Gerard Pogorel and Francesco Cappelletti (eds), *Sustainable Development and EU Industrial Sovereignty: Challenges and Conditions for Success*, European Liberal Forum, 2024.

[71] Volkswagen has stumbled on its efforts to build its own software platform while Renault has partnered with Google and Qualcomm. “French Correction,” *The Economist*, August 31, 2024, p. 52. “Volkswagen—No Quick Fix,” *The Economist*, September 7, 2024, p. 56. David J. Lynch, “U.S. pitches ban on Chinese tech in driverless and connected vehicles,” *Washington Post*, September 24, 2024**.** Adam Tooze, “Chartbook 309 Can Western carmakers derisk in China? The unreality of geoeconomic realism.” *Chartbook* Substack, August 14, 2024.

[72] Sources for this account include: "Tesla clears China’s data security requirements, moves closer to self-driving tech rollout," EFE, April 29, 2024. "As Musk Visits China, Tesla Wins Key Data Security Clearance," Bloomberg, April 28, 2024. Dan Swinhoe, “Tesla says it has established a data center in China,” Data Centre Dynamics, May 26, 2021. “Elon Musk Reaches Deals in China on Self-Driving Teslas,” New York Times, April 29, 2024.

[73] “As Musk Visits China, Tesla Wins Key Data Security Clearance,” Bloomberg.

[74] I am not trying to resolve the heated claims about TikTok. I am illustrating the complexities in the United States.

[75] One obstacle to the use of standard commercial contracts with China is that it does not belong to the global NGO that works on cybersecurity certification criteria. “Common Criteria,” Common Criteria Portal (commoncriteriaportal.org).