THE UNIVERSITY OF CHICAGO

Incompatible Sovereignties:

Chokepoint Conflict and the Structure of Digital Governance

By

Xiaotong (Sefa) Fu

June 2026

A paper submitted in partial fulfillment of the requirements for the
Master of Arts degree in the
Master of Arts Program in the Social Sciences

Faculty Advisor: Gary Herrigel
Preceptor: Dehua Sun

Abstract

This thesis examines what happens when different types of structural digital power intersect in the same dependent actor. It argues that three forms of structural digital capability——platform (the United States), infrastructure (China), and market control (the European Union), function as governance chokepoints whose constitutive governance logics cannot be simultaneously satisfied. When these logics intersect in the same firm, state, or user, they produce compliance-priority conflicts whose recurrence is constitutive rather than incidental. The argument is developed through three conflict scenarios: U.S. platform power against EU regulatory power, U.S. platform power against Chinese infrastructure power, and Chinese infrastructure power against the U.S.-led standards coalition. South Korea's semiconductor supply chain centrality is examined as a contrasting case to establish the boundary condition of the framework. The thesis extends Farrell and Newman's chokepoint concept from coercive leverage to sustained governance authority, distinguishes two subtypes of infrastructure sovereignty chokepoint, and reveals the global digital order as a field of structural conflict among three governance logics whose authority is simultaneously real, self-reinforcing, and mutually incompatible at the political layer.

Keywords: international political economy; digital governance; chokepoints; structural power; weaponized interdependence; platform regulation; infrastructure sovereignty; compliance-priority conflict

Chapter 1. Introduction

Over the past decade, the global digital order has undergone a fundamental structural transformation. Early visions of the internet anticipated a unified, open system governed primarily by technical communities and market actors operating across borders. That vision has not materialized. Instead, a small number of actors have emerged as dominant poles within the global digital order, each exercising sustained authority over the rules, standards, and flows that define digital life for billions of users worldwide.

The empirical pattern is striking in its concentration. The United States shapes global digital exchange through the dominance of its technology platforms and the extraterritorial reach of its legal jurisdiction. China has constructed a territorially bounded digital system characterized by state authority over infrastructure, networks, and data flows. The European Union, despite lacking globally dominant technology firms, exercises regulatory authority that reshapes corporate behavior and legislative choices far beyond its borders. Most other technologically capable states, including South Korea and India, have not achieved comparable systemic influence despite significant digital investments and capable institutions.

This concentration raises a theoretically important question in international political economy and international relations: when different types of structural digital power intersect in the same dependent actor, what forms of compliance-priority conflict emerge, and what do these conflicts reveal about the internal tensions of a polarized digital order? Existing scholarship has partially addressed these dynamics. Farrell and Newman's weaponized interdependence framework, Bradford's Brussels Effect analysis, and the cyber sovereignty literature each illuminate a distinct face of digital structural power, but no unified account exists of how the

three types relate to one another, whether they are complementary, parallel, or structurally incompatible, and what happens when they intersect in the same dependent actors.

This thesis argues that the three types of structural digital capability (platform ecosystem control, infrastructure sovereignty control, and market-regulatory access control) produce structurally incompatible governance logics that compete for the compliance priority of the same dependent actors. The competition is not over market share or military influence, but over whose rules a firm, state, or user prioritizes when subjected to overlapping and contradictory governance demands. When these governance logics intersect in the same dependent actor, compliance-priority conflicts emerge whose recurrence is constitutive rather than incidental.

Chapter 2. Literature Review

This literature review situates the thesis within three intersecting bodies of scholarship: research on network power and structural interdependence, work on digital governance and internet architecture, and the political economy of regulatory authority.

2.1 Power as Position: Structural Approaches to Digital Authority

A foundational question underlies any attempt to explain the emergence of digital governance poles: where does power in digital networks come from? One answer locates power in aggregate capabilities (economy, technology, military). The other locates power in structural position, in where an actor sits within a network rather than in how much it possesses in absolute terms. This thesis adopts the second position. Three frameworks ground that claim.

Susan Strange's concept of structural power is the most general. Strange distinguished between relational power, the ability to compel another actor to do something it would not

otherwise do, and structural power, "the power to shape and determine the structures of the global political economy within which other states, their political institutions, their economic enterprises and (not least) their scientists and other professional people have to operate" (Strange, 1988, pp. 24–25). The most consequential form of international power is not the ability to win particular bargains but the ability to determine the rules of the game itself. The actor who controls one of the four primary structures (security, production, finance, knowledge) need not coerce anyone directly; dependency on the structure is sufficient to ensure that others operate within the terms it sets. Firms operating within American platform ecosystems are subject to American jurisdiction by virtue of their participation; firms that cannot forego European market access carry European regulatory requirements with them as they operate globally.

Farrell and Newman's framework of weaponized interdependence translates structural power into the specific logic of network architecture (Farrell & Newman, 2019). Global networks do not distribute power evenly. Actors positioned near the central nodes of transnational networks (financial messaging, semiconductor supply chains, internet infrastructure) can exploit the asymmetries that network architecture creates. The panopticon effect describes the informational advantage of central nodes: flows passing through a hub are visible to whoever controls that hub. The chokepoint effect describes the coercive advantage: an actor with jurisdiction over a critical hub can deny access to dependent actors who have no equivalent alternative. Two cases illustrate. In SWIFT, the United States first used the hub position for large-scale financial surveillance under the Terrorist Finance Tracking Program, then weaponized it to exclude Iran from global financial flows. In semiconductors, American restrictions on ZTE and Huawei prompted China to accelerate domestic chip development, illustrating that weaponizing chokepoints can trigger decoupling rather than compliance when

the costs of dependence become politically unacceptable to the target. The second case matters for the present thesis: it establishes that flow dependence does not automatically convert into rule acceptance.

DeNardis grounds the structural-position argument in technical artifacts: the Domain Name System, internet routing protocols, interconnection agreements, and standards bodies (DeNardis, 2014). "Arrangements of technical architecture are arrangements of power" (DeNardis, 2014, p. 7). Decisions about how the DNS is organized, who controls IP address allocation, how routing protocols are designed, and what technical standards govern device interconnection are simultaneously technical and political; the embedded politics of technical architecture constitutes a form of governance authority that operates beneath and prior to the formal legal frameworks more conventional accounts emphasize.

Together these frameworks converge on a foundation: power in digital networks is positional and structural. Yet none explains why different types of structural position produce qualitatively different forms of governance authority.

2.2 Three Faces of Digital Capability

A closer examination of three bodies of work, on platform ecosystems, on digital infrastructure and technical standards, and on regulatory market access, reveals that different types of structural capability generate different forms of governance authority through distinct mechanisms. These bodies have not previously been brought into systematic comparison.

Platform ecosystem control is the first type. Srnicek defines platforms as "digital infrastructures that enable two or more groups to interact" (Srnicek, 2017, p. 29). Two mechanisms consolidate platform position into structural power. Network effects mean that

"early advantages become solidified as permanent positions of industry leadership" (Srnicek, 2017, p. 56). Lock-in through data extraction "ties users and data to the platform" through dependency, inability to use alternatives, and lack of data portability (Srnicek, 2017, p. 63). What matters for the present thesis is the translation of this economic position into legal governance authority. Because the dominant global platforms are legally domiciled in the United States, American legal jurisdiction extends across the platform ecosystem wherever it operates. The CLOUD Act of 2018 exemplifies this mechanism, requiring firms under American jurisdiction to comply with federal data requests regardless of where data is stored.

Infrastructure sovereignty control operates through technical standards lock-in. Mattli and Büthe demonstrate that international standards are sites of distributional conflict in which first-mover advantages are decisive (Mattli & Büthe, 2003). Rühlig identifies four dimensions through which standards generate political authority: economic (standard-essential patents and adaptation costs), legal (incorporation into binding trade law via WTO TBT provisions), political (lock-in effects creating ongoing dependency on the standard-setter's supply ecosystem), and discursive (normalization of particular technical choices as universal) (Rühlig, 2021). Infrastructure standards, once embedded in deployed systems, create path dependencies extremely costly to reverse. A state that deploys infrastructure built to a particular technical standard does not merely purchase hardware; it accepts an ongoing relationship of technical dependency on the ecosystem the standard defines.

Market-regulatory access control generates governance authority through a third mechanism. Bradford's Brussels Effect "refers to the EU's unilateral power to regulate global markets … market forces alone are often sufficient to convert the EU standard into the global standard as companies voluntarily extend the EU rule to govern their worldwide operations"

(Bradford, 2020, pp. xiv–xv). The mechanism operates in two stages. In the de facto stage, multinational corporations seeking access to the European single market internalize EU standards across their global operations to achieve economies of scale; this "converts the EU rule into a global rule" (Bradford, 2012, p. 159). In the de jure stage, those firms, having borne the costs of EU compliance, lobby their home governments to adopt equivalent standards domestically (Bradford, 2012, p. 159; Bradford, 2020, p. 78). The European Union's structural power derives not from owning platforms or controlling infrastructure but from the indispensability of market access.

Each literature analyzes its respective capability type in isolation and does not ask why such capabilities concentrate in a small number of actors rather than diffusing across the many states with substantial digital investments.

2.3 Polarization or Diffusion?

Two bodies of scholarship offer competing accounts of why digital governance authority polarizes. Neither is adequate.

The power transition and digital bipolarity literature provides the most direct engagement with the polarization question. Degterev, Ramich, and Piskunov argue that the global digital order is consolidating around two competing poles, the United States and China each projecting a distinct model of internet governance (Degterev et al., 2021). This framing correctly identifies the systematic competition between American and Chinese governance models and the displacement of traditional hard-power competition into the domain of network governance. Herrera's work on technology and international systems provides a structural complement

(Herrera, 2003), and Bjola and Kornprobst situate these dynamics within digital international relations (Bjola & Kornprobst, 2023).

The framework's limitation is structural. Its explanatory logic derives from power transition theory, organized around the dyadic relationship between hegemon and challenger. This produces two poles by theoretical construction: the hegemon defends the existing order, the challenger seeks to revise it, and all other actors are positioned as aligned with or dependent upon one of the two. Within this logic, the European Union has no independent analytical standing. It appears, if at all, as a subordinate element of the American-led liberal order. This is precisely what the present thesis contests. The European Union's capacity to convert market indispensability into rule-setting authority over actors far beyond its borders is a structurally distinct form of digital governance power that cannot be collapsed into the American platform model.

Mueller's transnationalist account presents a different challenge. Mueller does not deny that state action has reshaped the internet (Great Firewalls, content regulation, ICANN politicization). His claim is that such reshaping is structurally regressive against the network's natural decentralizing logic. Internet-based networks "can easily be transnational; any attempt to make them conform to jurisdictional or organizational boundaries requires extra work and cost" (Mueller, 2010, p. 36). Yet the empirical pattern this thesis examines exhibits a feature the normative framing cannot accommodate. The European Union's GDPR has produced documented convergence in corporate data handling and third-country legislation across jurisdictions with no formal relationship with the EU. American platform ecosystems have extended American legal jurisdiction into the data practices of firms whose home governments actively contest that extension. Chinese telecommunications infrastructure has embedded

technical standards and legal obligations in network architectures of states that did not seek to adopt Chinese governance norms. These are not temporary distortions against the network's natural logic; they are durable structural outcomes that have intensified over time.

2.4 Research Gap

The gap that runs through the existing literature is theoretical, not empirical, and has three dimensions. First, why do platform ecosystem control, infrastructure sovereignty control, and market-regulatory access control produce three qualitatively distinct forms of governance pole rather than three points on a single continuum? Existing literature treats these as separate phenomena studied by separate scholarly communities. Second, under what conditions does structural capability translate into sustained governance authority rather than triggering resistance, decoupling, or the search for alternatives? Farrell and Newman's semiconductor case demonstrates that flow dependence does not automatically produce rule acceptance; South Korea generates significant dependence without producing the governance authority that characterizes the three poles. Third, what happens when these distinct governance logics operate simultaneously upon the same dependent actor? Bradford's *Digital Empires* (2023) comes closest to naming this problem, observing that tech companies "have multiple masters" and "often face conflicting demands from different governments, making it impossible for them to comply with all of those demands at the same time." Bradford treats this as one manifestation of a broader restraint dynamic. This thesis takes that observation as its point of departure, theorizing compliance-priority conflict not as a contingent byproduct of overlapping regulatory ambitions but as the predictable structural consequence of three chokepoint types whose constitutive governance logics cannot be simultaneously satisfied.

Chapter 3. Theoretical Framework

3.1 From Coercion to Governance: Extending the Chokepoint Concept

Farrell and Newman's chokepoint concept identifies a specific form of power: an actor that controls a hub through which others must pass can threaten to deny access, imposing severe costs (Farrell & Newman, 2019, pp. 42–79). This is a theory of coercive leverage. It explains how a state with jurisdiction over a critical network hub can extract concessions in discrete episodes of statecraft. It does not explain how network position generates the sustained, cross-border rule-making authority that characterizes the United States, China, and the European Union in the global digital order. The European Union does not threaten to deny market access to firms that refuse to comply with GDPR; the threat is implicit in the structure of the regulatory framework itself, and firms internalize compliance as an operating condition. The United States does not issue episode-specific demands to firms operating within American platform ecosystems; American legal jurisdiction attaches to those firms by virtue of their domicile and shapes global data governance continuously. These are instances of structural governance authority in Strange's sense (Strange, 1988, pp. 24–25).

This thesis extends the chokepoint concept to encompass this form of power. A position in a global digital network constitutes a *governance chokepoint* (as distinguished from a *coercive chokepoint*) when it satisfies two conditions. The first is flow dependence: significant digital flows must pass through or depend upon this position, and the cost of alternative routing or substitution is prohibitively high for most relevant actors. The second is rule convertibility: the occupant can translate others' flow dependence into acceptance of the occupant's rule-making

framework, not merely as a response to a specific coercive threat, but as a constitutive condition of participation in the flows the chokepoint mediates.

A practical test distinguishes rule convertibility from mere flow dependence. A dependency carries a governance logic when exiting it requires the dependent actor to renegotiate rule commitments, not only to bear economic cost. Switching cloud providers within the U.S. platform ecosystem may impose substantial commercial cost, but it does not exit the governance logic; the new provider remains within American legal jurisdiction. By contrast, switching from Korean to Taiwanese semiconductor suppliers imposes substantial commercial cost yet exits the dependency completely without renegotiating any governance framework. This distinction returns in Chapter 8.

The two categories overlap. Governance chokepoints can be weaponized when occupants choose, as the contrast between the CLOUD Act (a governance mechanism) and semiconductor export controls (a coercive one) illustrates. But conflating them obscures how governance poles sustain authority absent any specific coercive act: continuously, multilaterally, and through self-reinforcing dynamics, as more actors adapt their operations to the occupant's rule framework, exit costs increase, and the framework deepens.

This extended concept allows a precise definition of digital governance poles. A *digital governance pole* satisfies three conditions: it occupies one or more governance chokepoints; its chokepoint position generates sustained, cross-border rule acceptance by a significant and diverse population of other actors, such that its governance framework functions as a de facto or de jure standard across jurisdictions extending substantially beyond its territory; and its governance authority exhibits self-reinforcing dynamics. This definition differs from polarity in the structural realist tradition (Waltz, 1979): it is domain-specific, mechanism-based, and

constitutively relational. A digital governance pole exists only in relation to actors who accept its governance framework, and its authority is measured by the breadth and depth of that acceptance. Three actors currently satisfy this definition: the United States, China, and the European Union, each occupying a distinct chokepoint type elaborated next.

3.2 Three Chokepoints: Platforms, Infrastructure, and Regulatory Markets

Platform ecosystem control, infrastructure sovereignty control, and market-regulatory access control each generate governance authority through distinct mechanisms. The infrastructure sovereignty chokepoint, which has received the least systematic theoretical treatment, requires a further internal distinction between two subtypes that operate through different conversion pathways.

Platform ecosystem chokepoints arise from the concentration of globally dominant digital platforms within a single legal jurisdiction. Network effects and data lock-in (Srnicek, 2017, pp. 56, 63) generate flow dependence: the cost of exiting major platform ecosystems is prohibitively high for the overwhelming majority of users and firms. Rule convertibility operates through legal jurisdiction. Because dominant global platforms are legally domiciled in the United States, American law governs their operation wherever they function. The CLOUD Act exemplifies this: it extends American legal authority over data held anywhere in the world by firms subject to American law, converting platform ecosystem control into a continuous form of extraterritorial governance.

Infrastructure sovereignty chokepoints arise from state authority over the physical and logical architecture of digital networks: telecommunications infrastructure, undersea cables, routing systems, and the technical standards governing how these components interconnect. Dependence

is created not through network effects but through the embedding of state authority in deployed technical systems (Mattli & Büthe, 2003; Rühlig, 2021).

The infrastructure sovereignty chokepoint, however, operates through two analytically distinct subtypes that the existing literature has not adequately separated. The first, which may be termed *standards-export infrastructure sovereignty*, operates through the international promotion of state-favored technical standards: the standard-setter projects governance preferences by ensuring that international standards encode its preferred architectural choices, and other states that adopt those standards thereby internalize the political and architectural commitments embedded in them. China's promotion of the New IP proposal at the ITU, the international expansion of BeiDou, and the broader Digital Silk Road agenda illustrate this subtype. The second, *law-spillover infrastructure sovereignty*, operates through a different pathway. The state's legal authority attaches to its domiciled technology firms (through statutes such as China's National Intelligence Law, which obligates firms under PRC jurisdiction to cooperate with state intelligence work), and that legal obligation travels with the equipment and services those firms deploy in third-country markets. The third-country government does not adopt any Chinese standard explicitly; it incorporates into its critical infrastructure equipment whose supplier operates under Chinese legal obligations the government cannot inspect, modify, or override.

The two subtypes are analytically separable but empirically intertwined: the same infrastructure deployment can carry both effects, and the Chinese state has pursued both pathways concurrently. The distinction matters because Scenario 3 examines a case in which the law-spillover subtype is the primary mechanism. Huawei equipment deployed in Five Eyes 5G networks operated within international 3GPP standards rather than Chinese-specific architectures;

the governance logic to which dependent states objected was not the technical standard itself but the legal obligation under which the supplier operated. Recognizing this distinction explains why the coalition response was framed as a question of vendor trustworthiness rather than as an objection to Chinese standards as such.

Market-regulatory access chokepoints arise from control over access to a large, integrated, and rule-governed market for digital goods and services. Bradford's analysis specifies the mechanism. The European single market is sufficiently large that most globally operating firms cannot forego access to it; market indispensability creates flow dependence. Rule convertibility operates through the two-stage Brussels Effect described in Section 2.2. The governance authority generated by this chokepoint type is the most indirect of the three: it operates through market conditionality, corporate compliance behavior, and third-country political economy rather than through legal jurisdiction or technical architecture. Yet it is no less durable for being indirect.

The three chokepoint types share the two defining conditions but differ in the structural source of each condition and in the conversion pathway. The United States, China, and the European Union are not governance poles of the same kind that differ only in degree of influence. They are governance poles of qualitatively different kinds, each susceptible to distinct forms of challenge and erosion.

3.3 The Conversion Mechanism: Asymmetric Dependency and Rule Acceptance

The two conditions describe the structural features a position must have but do not explain the process through which those features generate governance authority. The mechanism is asymmetric dependency conversion, proceeding in three steps. First, flow dependence creates a structural asymmetry between the chokepoint occupant and dependent actors: the occupant can

set the conditions of access, while dependent actors bear the costs of compliance and face prohibitive exit costs. Second, dependent actors internalize the occupant's rule framework as a condition of participation rather than as a response to specific demands. Firms within American platform ecosystems adopt American data governance norms; states deploying Chinese telecommunications infrastructure incorporate Chinese legal obligations into their network architectures; multinational corporations operating in European markets apply EU regulatory standards globally. Third, this internalization generates self-reinforcing dynamics. As more actors adopt the framework, exit costs for remaining actors increase, and the occupant's governance authority deepens without additional coercive investment.

The mechanism is asymmetric in two senses. The distributional asymmetry: costs fall disproportionately on dependent actors. The dynamic asymmetry: the relationship deepens over time in the occupant's favor, as sunk costs in the framework increase and network externalities accumulate around it. The poles identified in this thesis are not powerful despite others' adaptation, but precisely because of it.

The mechanism has boundary conditions. Conversion produces rule acceptance rather than resistance under three conditions. First, the cost of compliance must be lower than the cost of exit. When exit costs decline because credible alternative chokepoints emerge, or because the dependent actor's own capabilities reduce switching costs, the mechanism weakens. Second, the occupant must not over-exploit the position in ways that make the political costs of dependence sufficiently salient to motivate investment in exit. American restrictions on ZTE and Huawei made the political costs of semiconductor dependence salient enough to motivate large-scale Chinese investment in domestic chip manufacturing capacity, undermining the chokepoint's long-term viability (Farrell & Newman, 2019, pp. 42–79). Third, the dependent actor must lack

the structural capabilities required to establish its own competing chokepoint. These boundary conditions provide the basis for the South Korean contrasting case in Chapter 8.

3.4 When Governance Logics Intersect: The Structural Basis of Compliance-Priority Conflict

When distinct governance logics operate simultaneously upon the same dependent actor, they do not merely produce overlapping regulatory demands that could be accommodated through careful compliance engineering. They produce a specific form of structural conflict in which the constitutive logic of each chokepoint renders the demands of the others impossible to satisfy at the same time.

The structural basis lies in the rule convertibility pathways established in Section 3.2. Each chokepoint type converts flow dependence into rule acceptance through a pathway constitutive of the chokepoint itself. Platform ecosystem chokepoints operate through legal jurisdiction; infrastructure sovereignty chokepoints, particularly in their law-spillover subtype, operate through the legal obligations of supplier firms; market-regulatory access chokepoints operate through the two-stage Brussels Effect. These pathways are not discretionary instruments the occupant could trade away; they are the mechanisms through which each chokepoint generates governance authority. When a dependent actor is positioned at the intersection of two chokepoints, the compliance demands it faces are two constitutive requirements of continued participation in two different networks, whose incompatibility is structural rather than accidental.

This incompatibility manifests on three layers. The commercial layer concerns the economic costs imposed on the dependent actor: compliance expenditure, market access restrictions, transactional friction. The technological layer concerns architectural incompatibility:

data flow requirements that cannot coexist, encryption standards that cannot interoperate, technical specifications that require divergent implementation. The political layer concerns jurisdictional and constitutive claims: sovereignty assertions, overlapping claims of regulatory authority, and conflicting articulations of the values digital systems are supposed to protect. The three layers are empirically entangled but analytically separable. The argument of this thesis is that the political layer is where compliance-priority conflict is ultimately located. Commercial and technological incompatibilities are visible surfaces, but the reason they cannot be engineered away is that each chokepoint embeds a political claim about whose rules constitute legitimate authority.

The three poles do not confront these intersections with identical regulatory styles. Bradford's (2023) typology of three regulatory models provides the appropriate starting point. The American market-driven style projects governance authority through extraterritorial jurisdictional reach: American legal authority attaches to firms by virtue of corporate domicile and ordinary legal process. The European rights-driven style projects governance authority through constitutive regulatory projection: rights-based requirements are embedded as preconditions of market access and travel with firms into third jurisdictions through the Brussels Effect. (This thesis brackets the question of whether the European style also serves digital-sovereignty objectives; the analytical claim is about the form of the governance logic projected, not the motivations underlying it.) The Chinese state-driven style projects governance authority through sovereign directive assertion: the state compels firms under its jurisdiction to cooperate with data access, content governance, and national security requirements as a matter of sovereign prerogative. These styles shape how each pole behaves within compliance-priority conflict: the

instruments deployed, the arguments offered, and the compromises proven willing or unwilling to accept.

Style and chokepoint type are analytically distinct. Chokepoint type describes the structural position that authorizes governance projection; style describes how a pole projects its governance logic in conflict situations. A single chokepoint type can be projected through different styles depending on the conflict configuration: the United States operates from the same platform ecosystem chokepoint in all three scenarios, but its style varies from extraterritorial jurisdictional projection (Scenarios 1–2) to collective standards-coalition projection (Scenario 3). Style is therefore a contingent variable shaping conflict trajectory; the structural incompatibility of governance logics is a function of chokepoint type rather than style.

Chapter 4. Research Design and Case Selection

The thesis employs a conflict-scenario comparison across three empirical cases and one contrasting case. Each conflict scenario is defined by the intersection of two distinct governance logics in the same population of dependent actors who are subject to overlapping and contradictory compliance demands. Within each scenario, the analysis traces the sequence of events and decisions through which the incompatibility became manifest, the compliance demands escalated, and dependent actors were forced to prioritize one governance logic over another. Key nodes in this causal process (legal rulings, legislative acts, corporate compliance decisions, diplomatic agreements) serve as the observable traces of the mechanism. Each scenario is anchored in a specific historical episode that allows the mechanism to be observed with sufficient documentary evidence: legislative texts, judicial rulings, regulatory decisions,

executive orders, official government statements, corporate compliance records, and multilateral statements.

The analytical questions posed to each scenario are: which governance logics are in conflict, and what specific compliance demands does each impose? What makes it structurally impossible for dependent actors to satisfy both governance logics simultaneously? Through what process did dependent actors resolve the compliance conflict, and in whose favor? What character does the conflict exhibit at the commercial, technological, and political layers, and how do the policy styles of the two poles shape the trajectory? The South Korean contrasting case is posed a related but distinct question: why does semiconductor supply chain centrality not generate compliance-priority competition despite generating significant flow dependence?

The three conflict scenarios are selected because they represent the clearest available cases in which structurally distinct governance logics, each rooted in a different chokepoint type, have intersected in the same dependent actors and produced compliance-priority conflicts with traceable outcomes. Each involves a different pairing of governance logic types, together covering all three bilateral combinations among the three poles. South Korea is selected as a contrasting case because it occupies a structural position of significant flow dependence in global semiconductor supply chains while failing to generate the rule acceptance pattern that the three scenarios document. The selection therefore provides the boundary-condition test that distinguishes governance chokepoints from other forms of structural centrality.

Chapter 5. U.S. Platform Power versus EU Regulatory Power

5.1 The Conflict in Outline

The first conflict scenario examines the structural incompatibility between U.S. platform governance and EU market-regulatory governance as it has materialized in transatlantic personal data transfers. The anchor episode begins with the judgment of the Court of Justice of the European Union in *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems* in July 2020 and continues through the negotiation and adoption of the EU–U.S. Data Privacy Framework (DPF) adequacy decision in July 2023.[1] The dependent actors are the multinational firms (predominantly U.S.-domiciled platform operators) that transfer the personal data of EU residents from European operations to servers and processing facilities in the United States. These firms are simultaneously subject to two constitutive governance logics. The U.S. platform logic attaches American legal authority to data held by firms under U.S. jurisdiction, most consequentially through Section 702 of the Foreign Intelligence Surveillance Act. The EU rights-driven logic treats the protection of personal data as a constitutive fundamental right under Articles 7, 8, and 47 of the Charter of Fundamental Rights, and conditions the lawful transfer of data to third countries on the existence of essentially equivalent protection in the destination jurisdiction.

The recurring character of this conflict is the first feature worth noting. *Schrems II* was the second legal declaration of incompatibility between the two logics, not the first. The Court

[1] Data Protection Commissioner v. Facebook Ireland Ltd and Schrems (Schrems II), Case C-311/18, ECLI:EU:C:2020:559 (CJEU July 16, 2020); Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 on the adequate level of protection of personal data under the EU–U.S. Data Privacy Framework, Official Journal of the European Union, L 231, 1.

had already invalidated the original Safe Harbor framework in *Schrems I* in October 2015, citing the primacy of U.S. national security requirements over privacy principles, the generalized nature of U.S. surveillance access, and the absence of effective judicial redress for EU data subjects.[2] The Privacy Shield framework that replaced Safe Harbor in 2016 was in turn invalidated by *Schrems II* on effectively the same grounds. The DPF adopted in 2023 is the third iteration of the same structural accommodation. Each political settlement addresses the symptoms of the conflict without resolving the underlying incompatibility of the two governance logics.

5.2 Two Constitutive Legal Architectures

The U.S. legal architecture rests on Section 702 of FISA, which authorizes the Attorney General and the Director of National Intelligence jointly to authorize the targeting of non-U.S. persons reasonably believed to be located outside the United States for the acquisition of foreign intelligence.[3] The targeting is carried out through directives issued to U.S. communications providers, whose compliance is compelled by statute and shielded from civil liability.[4] The operational design converts U.S. platform ecosystem control into surveillance reach: the location of companies in the United States and the routing of international communications through U.S.-based infrastructure allow intelligence agencies to collect with the assistance of providers (PCLOB, 2023, p. 172). Following *Schrems II*, the United States adopted Executive Order 14086 in October 2022, introducing additional safeguards: signals intelligence activities must be both

---

[2] Schrems v. Data Protection Commissioner (Schrems I), Case C-362/14, ECLI:EU:C:2015:650 (CJEU Oct. 6, 2015).

[3] Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1881a(a) (2018).

[4] 50 U.S.C. § 1881a(i)(4).

necessary to advance a validated intelligence priority and proportionate to that priority; targeted collection is prioritized over bulk; and a two-tier redress mechanism culminates in a Data Protection Review Court of independent legal practitioners outside the U.S. government.[5]

The EU legal architecture pivots on the essentially equivalent protection standard articulated in *Schrems II*. The Court held that neither Section 702 FISA nor Executive Order 12333 (read with Presidential Policy Directive 28) satisfied the EU principle of proportionality, with the consequence that the surveillance programmes based on those provisions could not be regarded as limited to what is strictly necessary.[6] The absence of actionable judicial remedies for EU data subjects is incompatible with the essence of the right to effective judicial protection under Article 47 of the Charter.[7] On Standard Contractual Clauses, contractual instruments cannot bind third-country public authorities; data exporters must verify case by case whether the destination country ensures adequate protection, and suspend transfers where additional safeguards cannot guarantee that level.[8] The European Data Protection Board operationalized these obligations in Recommendations 01/2020, requiring exporters to map transfers, assess effectiveness of transfer tools in light of third-country law, and adopt supplementary measures (EDPB, 2021, pp. 10–25).

The DPF adequacy decision was the political instrument that sought to reopen the transfer channel. Its reasoning rests on the EO 14086 reforms, which the Commission recognized as strengthening the conditions, limitations, and safeguards applying to signals intelligence

---

[5] Executive Order No. 14,086, 87 Fed. Reg. 62,283 (Oct. 7, 2022).

[6] Schrems II, para. 184.

[7] Schrems II, paras. 187, 192.

[8] Schrems II, paras. 132–135.

activities, and as establishing a redress mechanism through which those safeguards could be invoked by individuals.[9] On that basis, the Commission concluded that the United States ensures a level of protection essentially equivalent to that guaranteed by the GDPR. The decision's architecture is provisional: it requires continuous Commission monitoring, a first review within one year, and provides for suspension, amendment, or repeal if adequate protection is no longer ensured.[10]

5.3 Three Layers and Two Regulatory Styles

The conflict manifests on three analytically separable layers, with the political layer constituting the analytical endpoint. Commercially, the stakes are very large: the DPF decision records that data flows between the United States and the European Union are the largest in the world and underpin a $7.1 trillion economic relationship.[11] Technologically, the EDPB Recommendations reveal the depth of incompatibility. Strong encryption is effective only where the data importer does not hold the keys and the algorithm is robust against cryptanalysis by recipient-country authorities; pseudonymisation is effective only where the additional information for re-identification is held exclusively by the data exporter within the EEA (EDPB, 2021, paras. 84–85). For cloud services requiring access to data in the clear, the EDPB states that where public authority access exceeds what is necessary in a democratic society, the Board "is, considering the current state of the art, incapable of envisioning an effective technical measure to prevent that access from infringing on the data subject's fundamental rights" (EDPB, 2021, para.

[9] Commission Implementing Decision (EU) 2023/1795, recitals 6, 124, 176, 201.

[10] Commission Implementing Decision (EU) 2023/1795, art. 3(1), (5); recital 211.

[11] Commission Implementing Decision (EU) 2023/1795, Annex III.

94). For an important segment of transatlantic data processing, no technological solution can reconcile the two governance logics. Politically, the incompatibility concerns whose legal order is constitutive for the protection of EU residents' data. The Court framed the conflict in explicitly constitutional terms: access by public authorities to personal data constitutes an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter; the limitations imposed by U.S. domestic law are not circumscribed in a manner satisfying requirements essentially equivalent to those required by Article 52(1); and legislation that provides no possibility for an individual to pursue legal remedies regarding personal data does not respect the essence of the right to effective judicial protection under Article 47.[12] The U.S. position is symmetrical and opposed: EO 14086 declares that signals intelligence collection exists so that national security decisionmakers have access to timely and insightful information to advance U.S. national security interests,[13] and PCLOB has repeatedly affirmed that Section 702 is essential to U.S. national security (PCLOB, 2023).

The two poles pursue these claims through the regulatory styles identified in Section 3.4. The United States operates through extraterritorial jurisdictional projection. American authority attaches to data by virtue of corporate domicile and is asserted through compelled legal process, applied without regard to the nationality or place of residence of the data subject.[14] Section 702 itself operationalizes this pattern: targeting of non-U.S. persons abroad is accomplished through statutorily compelled cooperation of U.S. providers, protected from civil liability. The European Union operates through constitutive regulatory projection. The rights enshrined in Articles 7, 8,

[12] Schrems II, paras. 171, 185, 187.

[13] Executive Order No. 14,086, § 1.

[14] Commission Implementing Decision (EU) 2023/1795, Annex VI.

and 47 of the Charter are treated not as policy preferences to be balanced against competing objectives but as preconditions of any lawful data processing. The EDPB articulates the stance directly: an essentially equivalent level of protection must accompany the data when it travels to third countries (EDPB, 2021, paras. 1–2), and obligations are ex ante and preventative.[15]

The two styles generate a predictable dynamic. The U.S. style responds to inter-jurisdictional tension by offering procedural safeguards, oversight mechanisms, and redress architecture (EO 14086 and the Data Protection Review Court). The EU style evaluates those procedural additions against the substantive rights test in its own constitutional order (the adequacy determination process and the one-year monitoring review). The DPF is the product of this interaction. Its durability depends on whether the procedural instruments introduced on the U.S. side prove substantively equivalent, in European evaluation, to the rights-equivalence the EU order demands. Two questions about durability lie beyond this analysis: whether the DPF's adequacy determination will survive judicial challenge before the Court of Justice, and whether the EO 14086 safeguards will be sustained through subsequent U.S. political cycles. The chapter's analytical claim is the prior structural one. The two governance logics remain incompatible at the political layer, and the DPF is best understood as the third in a recurring sequence of political accommodations rather than as a terminal resolution.

[15] Schrems II, paras. 135, 142.

Chapter 6. U.S. Platform Power versus Chinese Infrastructure Power

6.1 The Episode in Outline

The second conflict scenario examines the structural incompatibility between U.S. platform ecosystem governance and Chinese infrastructure sovereignty governance (specifically the law-spillover subtype) as it materialized in the TikTok divestiture episode. ByteDance Ltd., a Cayman-incorporated holding company with its operational center in China and with TikTok Inc. as its U.S.-incorporated platform subsidiary, was simultaneously subject to two governance logics imposing mutually incompatible compliance demands. The U.S. platform logic asserted that continued operation within the American platform ecosystem required severance from foreign adversary control, operationalized through the Protecting Americans from Foreign Adversary Controlled Applications Act (PAFACA) of April 2024.[16] The Chinese infrastructure logic asserted state authority over ByteDance as a firm under PRC jurisdiction, operationalized through the National Intelligence Law of 2017, the Data Security Law of 2021, and Document 79 of 2022.[17]

The episode spans four and a half years, from Executive Order 13942 in August 2020 through the Supreme Court's per curiam judgment on January 17, 2025, passing through three phases that progressively expose the incompatibility.[18] In the first phase, the Trump

---

[16] Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, div. H (2024) [hereinafter PAFACA].

[17] National Intelligence Law of the People's Republic of China, arts. 7, 14 (2017); Data Security Law of the People's Republic of China, arts. 31, 36 (2021); State-owned Assets Supervision and Administration Commission, Document 79 (Sept. 2022).

[18] Executive Order No. 13,942, 85 Fed. Reg. 48,637 (Aug. 6, 2020); TikTok Inc. v. Garland, No. 24-656, slip op. (U.S. Jan. 17, 2025).

administration attempted divestiture through Executive Order 13942 under the International Emergency Economic Powers Act (IEEPA). The District Court for the District of Columbia blocked this approach in *TikTok Inc. v. Trump*, holding that IEEPA's Berman Amendment prohibits the regulation of informational materials.[19] In the second phase, after the Biden administration replaced the original order with Executive Order 14034 in June 2021, ByteDance negotiated with the Committee on Foreign Investment in the United States (CFIUS) to construct Project Texas, a technical and organizational proposal that sought to quarantine U.S. user data and platform operations within an Oracle-hosted infrastructure managed by TikTok U.S. Data Security (TTUSDS).[20] In the third phase, the United States government concluded that no such arrangement could substitute for ownership divestiture; Congress enacted PAFACA in April 2024; the D.C. Circuit upheld the statute against First Amendment challenge on December 6, 2024; and the Supreme Court affirmed on January 17, 2025.[21]

6.2 Project Texas and the Symmetrical Sovereignty Claims

Project Texas was the most elaborate attempt to engineer around governance logic incompatibility ever undertaken by a private firm in the global digital order. Its core elements established TTUSDS as a separate Delaware subsidiary with government-approvable management; migrated U.S. user data into an Oracle-hosted cloud environment; provided for Oracle as a "trusted third party" to inspect the recommendation engine source code; and included

---

[19] TikTok Inc. v. Trump, No. 1:20-cv-02658 (D.D.C. 2020).

[20] Executive Order No. 14,034, 86 Fed. Reg. 31,423 (June 9, 2021).

[21] PAFACA, Pub. L. No. 118-50, div. H (2024); TikTok Inc. v. Garland, No. 24-1113 (D.C. Cir. Dec. 6, 2024); TikTok Inc. v. Garland, No. 24-656, slip op. (U.S. Jan. 17, 2025).

a government-operated kill switch.[22] The proposal addressed each surface manifestation of the conflict: data location, source code visibility, organizational independence, and emergency authority.

The government's rejection identifies the mechanism through which structural incompatibility resists technical resolution. First, the recommendation engine remained inseparable from ByteDance's continuous global development cycle. The D.C. Circuit documented that the engine "was originally developed by ByteDance" and that the global TikTok team, including Chinese engineers, continually develops the recommendation engine and platform source code; even under ByteDance's most ambitious voluntary mitigation, source code supporting the platform would continue to be developed and maintained by ByteDance subsidiary employees in both the United States and China.[23] Second, source code review proved incapable of detecting the channels through which influence might be exerted. The Executive concluded that even under the assumption that every line could be monitored and verified, the PRC could exert malign influence through commercial features that source code review could not detect.[24] Third, the trustworthiness of the proposed compliance regime depended on continuing reliance on the entity it was designed to constrain.[25] The court's summary is direct: acceptance of Project Texas would have ultimately relied on the Executive Branch trusting ByteDance to comply, which the government understandably judged it could not do; in the

---

[22] TikTok Inc. v. Garland, D.C. Cir., slip op. at 13–14.

[23] TikTok Inc. v. Garland, D.C. Cir., slip op. at 11, 23.

[24] TikTok Inc. v. Garland, D.C. Cir., slip op. at 23.

[25] TikTok Inc. v. Garland, D.C. Cir., slip op. at 22–23.

Executive's view, divestment was the only solution.[26] The technical failure is not contingent. It is the predictable consequence of attempting to engineer around a structural incompatibility located at the political layer.

The political incompatibility operates through symmetrical and opposed sovereignty claims over ByteDance. The U.S. claim was that firms operating within the American platform ecosystem are subject to American legal authority regarding foreign adversary control, operationalized not through content regulation but through structural divestiture. PAFACA designates TikTok and ByteDance by name as a "foreign adversary controlled application" and makes it unlawful for an entity to distribute, maintain, or update such an application through a marketplace or internet hosting service.[27] The statute defines the sole escape path through a "qualified divestiture," a transaction that would result in the application no longer being controlled by a foreign adversary, precluding the establishment or maintenance of any operational relationship, including any cooperation on a content recommendation algorithm or any agreement on data sharing.[28] The statute's legal form is precise about what is being regulated: not the content of speech on TikTok, but the jurisdictional nexus between the platform and the foreign adversary. The D.C. Circuit assumed strict scrutiny and upheld the statute as the least restrictive means of advancing compelling national security interests; the Supreme Court affirmed.[29]

---

[26] TikTok Inc. v. Garland, D.C. Cir., slip op. at 23.

[27] PAFACA § 2(a)(1), (g)(3).

[28] PAFACA § 2(g)(6).

[29] TikTok Inc. v. Garland, D.C. Cir., slip op. at 57; TikTok Inc. v. Garland, U.S., slip op. at 1.

The Chinese claim is symmetrically opposed: firms under PRC jurisdiction are subject to state authority over intelligence cooperation, data export, and strategically significant technology. The National Intelligence Law of 2017 (Articles 7 and 14) obligates organizations and citizens to support, assist, and cooperate with state intelligence work, and authorizes intelligence institutions to demand such cooperation, without provision for refusal based on conflicting foreign law.[30] The Data Security Law of 2021 prohibits cross-border data transfer to foreign judicial or law enforcement agencies without PRC approval, and subjects "important data" to additional export controls.[31] The 2020 revision of China's export control catalog, which classified content recommendation algorithms as export-controlled technology, gave the Chinese state direct authority to block any sale of TikTok whose terms included algorithm transfer.[32] The D.C. Circuit accepted that even putatively "private" companies based in China do not operate with independence from the government, and that through its control over Chinese parent companies, the PRC can access information from and about U.S. subsidiaries and compel their cooperation.[33] Document 79 codifies the broader expectation that firms under PRC jurisdiction align their technical architectures with state sovereignty objectives rather than with foreign regulatory accommodation.[34]

---

[30] National Intelligence Law of the People's Republic of China, arts. 7, 14 (2017).

[31] Data Security Law of the People's Republic of China, arts. 31, 36 (2021).

[32] Ministry of Commerce of the People's Republic of China, Catalogue of Technologies Prohibited or Restricted from Export (rev. Aug. 28, 2020).

[33] TikTok Inc. v. Garland, D.C. Cir., slip op. at 35–36.

[34] State-owned Assets Supervision and Administration Commission, Document 79 (Sept. 2022).

The two legal regimes stand in direct opposition on the precise question that defines the conflict. PAFACA requires ByteDance to sever any operational relationship with PRC-controlled entities, including cooperation on the algorithm and data sharing. The National Intelligence Law requires ByteDance to cooperate with PRC intelligence activities and prohibits refusal. The Data Security Law prohibits cross-border data transfer to foreign law enforcement without PRC approval, and the export control revision prohibits the sale of the recommendation algorithm without Chinese government authorization. No compliance posture available to ByteDance can satisfy both regimes simultaneously. The D.C. Circuit captured the confrontation directly when ByteDance argued that divestiture was impractical: the impracticality, the court observed, derived from Chinese sovereign action, namely export prohibitions that the PRC had erected to make a forced divestiture more difficult if not impossible.[35]

6.3 Policy Styles and the Absence of a Negotiating Instrument

The United States operated through the market-driven extraterritorial style. Authority was projected through legal control over market intermediaries (the app stores and hosting services named in PAFACA) rather than through any attempt to regulate content or block traffic at the network level. The remedy selected was divestiture rather than prohibition: a structural ownership intervention designed to sever the operational relationship without purporting to regulate speech. The adaptive trajectory from Executive Order 13942 in 2020 to PAFACA in 2024 documents how the U.S. system generated the governance instrument through ordinary legal process. When the initial IEEPA-based action failed because the Berman Amendment

[35] TikTok Inc. v. Garland, D.C. Cir., slip op. at 68–69.

protected informational materials, the state adapted by codifying a new statutory basis precisely tailored to survive First Amendment review.

The Chinese state operated through the state-driven sovereign-directive style. The legal foundation rests on categorical provisions (National Intelligence Law Article 7) that permit no refusal, and on administrative instruments, including the 2020 export control revision, that the state deployed directly into the negotiation. When the United States first sought a sale in 2020, China's Ministry of Commerce added content recommendation algorithms to the export control list, effectively requiring Chinese government approval for any sale whose terms transferred the algorithm.

The interaction in Scenario Two produced a different trajectory than in Scenario One. Where the U.S.–EU conflict generated a political settlement in the DPF, the U.S.–China conflict generated a terminal legal ruling with no political settlement. The American style pursued the conflict to the fullest constitutional elaboration available, and the Chinese style pursued it through direct administrative obstruction. No mediating instrument comparable to an adequacy decision was available, because neither pole was willing to articulate a framework within which the other's constitutive claims could be recognized. The actual implementation status of PAFACA after January 17, 2025 remains politically unsettled: the Supreme Court itself acknowledged that divestiture within the statutory 270-day timeframe is "commercially infeasible," and subsequent executive non-enforcement raises questions about whether the structural incompatibility is being resolved, deferred, or quietly absorbed into a regime of selective enforcement.[36] The two governance logics in Scenario Two remain incompatible at the

[36] TikTok Inc. v. Garland, U.S., slip op. at 3.

political layer, and the episode's resolution at the U.S. judicial level has not dissolved that incompatibility.

Chapter 7. Chinese Infrastructure Power versus the U.S.-Led Coalition

7.1 The Cascading Exclusions, 2018–2021

The third conflict scenario examines the structural incompatibility between Chinese infrastructure sovereignty governance and a U.S.-led coalition of security-alliance states as it materialized in the 5G infrastructure exclusion decisions of 2018 to 2021. This scenario differs from the preceding two in two significant respects. First, the dependent actors are sovereign states rather than firms. The United Kingdom, Australia, and Sweden were each required to choose between two mutually exclusive configurations of telecommunications infrastructure, each carrying a governance logic that could not be accommodated alongside the other. Second, the incompatibility is expressed primarily at the level of technical architecture rather than through competing legal demands directed at the dependent states themselves. The U.S.-led coalition logic does not assert direct legal jurisdiction over foreign 5G procurement; it operates through collective security standards and intelligence-sharing architectures that treat certain infrastructure configurations as constitutively incompatible with continued participation in the alliance's information environment.

The anchor episodes span three years and four jurisdictions. Australia was the first Five Eyes member to act, announcing in August 2018 that companies likely subject to extrajudicial directions from a foreign government that conflict with Australian law would be excluded from participation in its 5G network infrastructure: a determination whose principal effect was the

exclusion of Huawei Technologies and ZTE Corporation.[37] The Five Eyes Interior Ministers' communiqué, issued in London in July 2019, provided the collective articulation of the governance logic motivating the Australian decision, recognizing the need for risk-based vendor evaluation that could include assessment of "control by foreign governments" as a disqualifying factor.[38] Sweden's Post and Telecom Authority issued its determination in October 2020, conditioning the award of 5G spectrum licenses on the exclusion of equipment from vendors designated as security risks. The UK enacted the Telecoms Security Act 2021, providing the legislative framework for designating "high-risk vendors" and requiring operators to remove designated equipment from their networks by specified deadlines.[39] These decisions document the process by which a governance logic incompatibility initially stated as a security assessment became progressively institutionalized as binding legal obligation across multiple sovereign jurisdictions.

Australia's 2018 determination preceded the Five Eyes collective articulation by nearly a year. The collective articulation in the 2019 communiqué preceded the legislative formalization in the United Kingdom by two years. The sequence reveals that the structural incompatibility existed prior to any of its legal expressions: governments were already acting on the recognition that Chinese infrastructure sovereignty and Five Eyes intelligence architecture could not coexist before they had codified the terms of that incompatibility into statute.

---

[37] Department of Home Affairs (Australia), 5G Security Guidance: Protecting Australia's 5G Network (2018).

[38] Five Country Ministerial Communiqué: Emerging Threats, London 2019 (July 30, 2019).

[39] Telecoms Security Act 2021, c. 31 (UK).

7.2 The Latent Governance Logic: Law-Spillover Infrastructure Sovereignty

The Chinese governance logic operative in this scenario is the law-spillover subtype identified in Section 3.2. Precision on this point matters, because the scenario has sometimes been read as a conflict over Chinese-specific technical standards, and the case material does not support that reading. Huawei equipment deployed in Five Eyes 5G networks operated within international 3GPP standards rather than Chinese-specific architectures. The objection on the coalition side was not to a Chinese standard but to a Chinese supplier whose legal obligations under PRC law were considered architecturally inseparable from the equipment it deployed.

The Chinese governance logic in this scenario does not manifest through a specific statute directed at third-country 5G procurement. It manifests through the legal framework that governs Huawei as a firm under Chinese jurisdiction: Articles 7 and 14 of the National Intelligence Law, which require firms under PRC jurisdiction to support, assist, and cooperate with state intelligence work and prohibit refusal.[40] The governance logic is not communicated to dependent states through legal demands; it is embedded in the supplier-firm relationship itself. A state that deploys Huawei telecommunications infrastructure does not receive a directive from the Chinese government; it enters an ongoing technical and supply relationship with a firm operating under a legal obligation to cooperate with Chinese intelligence authorities when directed to do so. The governance logic travels with the equipment.

This is the analytically distinctive feature of Scenario Three. In Scenarios One and Two, the competing governance logics confronted dependent actors through identifiable legal instruments: FISA Section 702 and the GDPR created direct legal obligations on data-processing

[40] National Intelligence Law of the People's Republic of China, arts. 7, 14 (2017).

firms; the National Intelligence Law and PAFACA created direct legal obligations on ByteDance. In Scenario Three, the Chinese governance logic does not create any direct legal obligation on the sovereign states choosing their 5G infrastructure. Its claim over those states is structural and architectural: by deploying infrastructure built and maintained within the Chinese legal ecosystem, a state incorporates into its critical communications architecture a dependency on a firm whose cooperation with Chinese state authority is legally mandated. The governance logic is latent rather than explicit, but it is no less real.

The coalition response addressed this latent logic by treating vendor identity (specifically, the legal jurisdiction under which a vendor operates) as a security-relevant attribute of telecommunications infrastructure. The Australian determination's framing of the conflict as a question of whether infrastructure is "likely subject to extrajudicial directions from a foreign government that conflict with Australian law" identifies the political-layer incompatibility with precision. The vendor-identity criterion was elevated to collective articulation in the Five Eyes communiqué's recognition that "control by foreign governments" was a legitimate factor in vendor risk assessment, and operationalized as binding domestic law in the United Kingdom's high-risk vendor designation framework under the Telecoms Security Act 2021.[41] The Prague Proposals (May 2019), published following a conference of officials from more than thirty countries, established that vendor trustworthiness assessments should encompass political, economic, and technical factors, including the legal environment of the vendor's home country and its susceptibility to direction by a state that does not share the procuring country's values. The U.S. Clean Network initiative, announced in April 2020, operationalized the coalition logic

[41] Telecoms Security Act 2021, c. 31, pt. 4.

across multiple infrastructure domains, establishing that 5G network traffic entering or exiting U.S. diplomatic facilities must travel via a "clean path" that did not use any equipment from untrusted IT vendors such as Huawei and ZTE.[42]

7.3 The Engineering Limit: HCSEC Findings

The technological layer is where Scenario Three's distinctive character is most clearly expressed. The Huawei Cyber Security Evaluation Centre (HCSEC), established in 2010 as a joint arrangement between Huawei and the UK government, was the most elaborate attempt to engineer around the law-spillover incompatibility through technical oversight. The HCSEC Oversight Board's annual reports therefore provide the evidentiary basis for assessing whether technical review could substitute for structural exclusion. Their conclusion is the closest parallel in Scenario Three to the EDPB's paragraph 94 in Scenario One and the rejection of Project Texas in Scenario Two: the Oversight Board could provide only "limited assurance" that the long-term security risks could be managed in the Huawei equipment currently deployed in the United Kingdom.[43] The reports documented systemic failures across configuration management, third-party software components carrying publicly documented vulnerabilities, and basic security coding practices, and concluded that the defects reflected systemic organizational and technical practices that the HCSEC program could document but could not correct.[44] No technical architecture of oversight, however elaborate, could substitute for the organizational reforms required, and those reforms lay beyond the reach of any bilateral monitoring arrangement.

---

[42] U.S. Department of State, The Clean Network (2020).

[43] HCSEC Oversight Board, Annual Report 2019, p. 4.

[44] HCSEC Oversight Board, Annual Report 2019, pp. 18–32.

Two distinct impossibilities operate in this scenario, and they should not be conflated. The HCSEC findings establish a *technical* impossibility: even setting aside Chinese law, the cybersecurity quality of Huawei equipment is such that external review cannot provide the assurance that critical infrastructure procurement requires. The law-spillover analysis (Section 7.2) establishes a *structural* impossibility: even if Huawei's code quality were exemplary, the legal obligations under the National Intelligence Law would still travel with the equipment. Each impossibility independently grounds the coalition's exclusion logic; together they establish that no plausible reform path could have produced a settlement compatible with both governance logics. Improving Huawei's software engineering practices would not have dissolved the law-spillover problem; renegotiating Chinese intelligence law would not have dissolved the engineering quality problem. The two are jointly sufficient and individually irreducible. In all three scenarios, the technological-layer finding establishes the same structural conclusion: the incompatibility cannot be engineered away.

7.4 Coalition Style and the Political Layer

In Scenarios One and Two, the United States projected governance authority through legal architecture governing firms within American platform ecosystems. In Scenario Three, the United States has no comparable basis for direct legal authority over the 5G procurement decisions of the United Kingdom, Australia, or Sweden. The coalition governance logic is instead projected through a collective standards-setting style, in which bilateral security relationships, shared intelligence architectures, and multilateral fora (the Five Eyes ministerial process, the Prague conference, and the Clean Network initiative) establish a definition of trusted infrastructure that effectively excludes Chinese vendors without requiring any unilateral legal assertion of American jurisdiction. The Chinese governance logic is projected through the state-

driven sovereign directive style, but in a form that is architecturally embedded rather than actively asserted: the National Intelligence Law's cooperation obligations attach to Huawei as a matter of Chinese law regardless of what any third-country government decides about its own 5G network. This is the purest expression of law-spillover infrastructure sovereignty.

The political-layer incompatibility operates through opposed sovereignty claims over the same infrastructure. The coalition claims that the procuring state's security interests legitimately determine what infrastructure is permissible within its critical communications architecture, including consideration of the supplier's home-state legal obligations as a security-relevant factor. The Chinese logic claims that the supplier's legal obligations under PRC law are a matter of Chinese sovereignty that third-country security frameworks have no legitimate authority to second-guess. Neither claim can accommodate the other without abandoning the foundational principle from which it derives. The two governance logics in Scenario Three remain incompatible at the political layer, and the cascading exclusion decisions are best understood as the progressive institutionalization of that incompatibility rather than as terminal resolutions.

Chapter 8. South Korea as Contrasting Case

8.1 The Negative Prediction

The three preceding chapters traced compliance-priority conflicts through which the structural incompatibility of three governance logics became visible. This chapter examines a case in which the framework predicts that no such conflict will occur. The negative prediction is theoretically productive because the framework's explanatory force depends on identifying not only when compliance-priority conflicts arise but also when they do not, even in the presence of substantial flow dependence.

South Korea provides the appropriate test. As the producer of a dominant share of the world's memory semiconductors, with Samsung Electronics and SK Hynix together accounting for the majority of global DRAM and NAND production, South Korea occupies a structural position in the global semiconductor supply chain that generates substantial flow dependence among consuming states and firms. Yet this dependence has not produced compliance-priority conflicts of the kind documented in the three preceding chapters. The framework explains this absence through the second condition required for a governance chokepoint: rule convertibility. Without a constitutive linkage between the dependency and a governance framework that dependent actors must accept as a condition of continued participation, dependence does not convert into rule acceptance.

8.2 Flow Dependence Without a Governance Framework

The flow dependence is significant: memory semiconductors are essential components in nearly all consumer electronics, data center infrastructure, automotive electronics, and military systems, and the alternative supply pathways available to consuming states and firms are limited.

What South Korea's position lacks is a governance framework that travels with the dependency. Adopting Korean memory semiconductors does not require importing states or firms to comply with Korean regulatory frameworks, content governance rules, data protection standards, or any other dimension of Korean digital governance. Switching from Samsung or SK Hynix to alternative suppliers imposes substantial commercial cost (capital expenditure, supply chain reorganization, qualification cycles), but exiting the dependency does not require renegotiating any rule commitment. The dependency carries no governance logic, and consequently the operational test from Section 3.1 is not satisfied. The South Korean state has

not articulated a governance framework attached to its semiconductor production that other states or firms could be required to accept. Korean export control practice operates within multilateral arrangements rather than asserting independent extraterritorial reach. Korean regulatory frameworks for the semiconductor industry are oriented toward domestic industrial policy, environmental compliance, and labor regulation, not toward establishing rules that apply to consuming jurisdictions as a condition of participation in Korean supply.

8.3 Diversification, Not Rule Acceptance

The empirical record of how major consuming states have responded to semiconductor flow dependence demonstrates the framework's prediction. Three legislative-policy responses, enacted within a fourteen-month window in 2022–2023, document the dominant pattern: substantial state investment in reducing dependence rather than acceptance of any governance framework attached to the dependency. The U.S. CHIPS and Science Act of August 2022 authorized approximately $52 billion in federal investment in domestic semiconductor manufacturing capacity and research, with explicit framing as a measure to reduce U.S. dependence on foreign sources, and imposed restrictions on the establishment of advanced semiconductor manufacturing facilities in foreign countries of concern by recipients of funding for ten years.[45] The European Chips Act, adopted as Regulation (EU) 2023/1781 in September 2023, mobilized more than €43 billion toward doubling the EU's share of global semiconductor production, framing the goal as a matter of strategic autonomy.[46] Japan's Economic Security

[45] CHIPS and Science Act, Pub. L. No. 117-167, 136 Stat. 1366 (2022), §§ 102, 103, 107.

[46] European Chips Act, Regulation (EU) 2023/1781, recitals 1, 4, 7.

Promotion Act of May 2022 established the legislative framework for Japanese state action to secure supply chains for strategically critical goods, including semiconductors.[47]

Three features are significant. All three were enacted within a fourteen-month window, indicating coordinated rather than independent strategic adaptation. All three frame semiconductor dependence in the language of strategic vulnerability rather than in the language of governance norms: the policy problem is not that Korean rules are objectionable, but that dependence on Korean production constitutes a supply chain risk. All three deploy substantial public investment to develop alternative production capacity. Substantial flow dependence has produced diversification investment, not rule acceptance.

8.4 Why Semiconductor Dependence Carries No Governance Logic

The framework's explanation rests on the rule convertibility condition. The three chokepoint types identified each link dependency to rule acceptance constitutively: platform jurisdiction attaches to ecosystem participation; infrastructure obligations travel with deployed equipment; regulatory compliance is built into market access. Semiconductor dependence is a discrete-input dependency: chips can be replaced with chips from alternative producers without renegotiating any governance framework attached to the original supplier. Several features of the industry combine to produce this outcome. The product is a commoditized component that operates within technical specifications established by international standards bodies and does not carry embedded governance requirements that propagate to the systems in which it is integrated. Korean firms supply globally but do not host platforms, control infrastructure, or

[47] Japan, Keizai Anzen Hoshō Suishin Hō [Economic Security Promotion Act], Law No. 43 of 2022.

regulate markets in ways that would generate rule convertibility. The Korean state does not articulate the export of semiconductors as the export of a governance model; it treats semiconductor production as industrial policy rather than as a vehicle for projecting regulatory authority.

This explanation generates a counterfactual. If South Korea were to articulate a governance framework attached to its semiconductor production (a regulatory regime that required consuming firms or states to comply with Korean data localization rules, content governance standards, or technology-transfer restrictions as a condition of continued supply), the framework predicts that the response among consuming jurisdictions would shift. The contrast establishes the boundary condition: flow dependence produces governance authority only when the dependency is constitutively linked to a governance framework that dependent actors must accept as a condition of continued participation.

8.5 Implications for Emerging Candidates

The framework's analytical move is to ask whether a candidate's structural position carries a governance logic that dependent actors must accept as a condition of continued participation. India occupies a position of substantial flow dependence as a destination market for global digital services. Indian regulatory authorities have begun to articulate a governance framework imposing data localization and content moderation obligations on foreign firms. Whether this framework will generate the de facto and de jure compliance pattern characteristic of the Brussels Effect is an open question the framework can evaluate but does not predict. India is the most plausible candidate for emergence as a fourth governance pole, but the prediction is conditional on the development of rule convertibility rather than on the size of the Indian market

alone. Russia, by contrast, has developed substantial digital sovereignty infrastructure but has primarily turned that capability inward, insulating Russian networks from external influence rather than projecting Russian governance rules onto dependent actors abroad. The framework predicts that Russia will not become a governance pole in the absence of outward governance projection.

Chapter 9. Conclusion

The three scenarios converge on a common structural pattern. Each conflict reaches the political layer regardless of the surface manifestation through which it first becomes visible. Each generates a political settlement that addresses commercial and technological incompatibilities without dissolving the political-layer incompatibility. The South Korean case confirms the boundary condition: flow dependence converts into governance authority only when the dependency is constitutively linked to a governance framework. The negative observation is theoretically productive because it specifies the analytical procedure for evaluating other candidates: not size, capability, or even centrality, but whether the structural position carries a governance logic that dependent actors must accept as a condition of continued participation.

The thesis makes three theoretical contributions. First, the chokepoint concept is extended from coercive leverage to sustained governance authority that operates continuously through the ordinary functioning of the chokepoint position rather than through episodic coercive acts. Second, the typology of three structurally distinct chokepoint types provides a basis for analyzing the U.S., China, and the EU as different expressions of a common structural logic; the further distinction between standards-export and law-spillover subtypes of infrastructure

sovereignty resolves an ambiguity in the existing literature and is the framework's most original contribution at the level of internal typology. Third, the structural account of compliance-priority conflict identifies a distinctive analytical object: when chokepoint types whose constitutive governance logics cannot be simultaneously satisfied intersect in the same dependent actor, compliance-priority conflict is the predictable consequence rather than a contingent outcome.

Several limitations should be acknowledged. The framework did not provide a comprehensive account of each pole's governance logic in isolation. The empirical analysis relies primarily on publicly available primary documents; some aspects of the causal processes, particularly internal deliberations of governments, corporations, and intelligence communities, are not accessible through public sources. The framework analyzes the digital order as it exists in the current period; the configuration may shift as new capabilities emerge, as dependent actors develop exit options, or as inter-pole negotiations produce durable agreements that modify the terms of compliance-priority competition.

In conclusion, this thesis suggests that the global digital order is a field of structural conflict among three governance logics whose authority is simultaneously real, self-reinforcing, and mutually incompatible at the political layer. The poles do not converge toward a common framework, because their governance logics rest on constitutive claims that cannot be reconciled without abandoning the foundational principles from which they derive. The poles do not separate into hermetic spheres, because the same dependent actors remain entangled in flows that cross all three jurisdictions and carry all three governance logics with them. If the framework is correct, governance harmonization in the global digital order is not a matter of finding the right institutional design or the right diplomatic instrument; it is structurally limited by the constitutive incompatibility of the three governance logics. Conversely, states that seek to establish digital

governance frameworks distinct from those of the three established poles face a structural test rather than a capability-based one: whether their dependencies carry governance logics that other actors must accept as conditions of continued participation. That specification is what this thesis offers to the analysis of a global digital order whose deep architecture, this thesis argues, is now visible.

References

Bjola, C., & Kornprobst, M. (2023). *Digital international relations*. Routledge. https://doi.org/10.4324/9781003437963

Bradford, A. (2012). Exporting standards: The externalization of the EU's regulatory power via markets. *International Review of Law and Economics*, *42*, 158–173.

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Columbia University Press.

Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press.

Degterev, D., Ramich, M., & Piskunov, D. (2021). U.S. & China approaches to global internet governance: "New bipolarity" in terms of "the network society." *International Organisations Research Journal*, *16*(3), 7–33. https://doi.org/10.17323/1996-7845-2021-03-01

DeNardis, L. (2014). *The global war for internet governance*. Yale University Press.

European Data Protection Board. (2021). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* (Version 2.0). https://edpb.europa.eu

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, *44*(1), 42–79. https://doi.org/10.1162/ISEC_a_00351

Herrera, G. L. (2003). Technology and international systems. *Millennium: Journal of International Studies*, *32*(3), 559–593. https://doi.org/10.1177/03058298030320031001

Mattli, W., & Büthe, T. (2003). Setting international standards: Technological rationality or primacy of power? *World Politics*, *56*(1), 1–42. https://doi.org/10.1353/wp.2004.0006

Mueller, M. L. (2010). *Networks and states: The global politics of internet governance*. MIT Press. https://doi.org/10.7551/mitpress/9780262014595.001.0001

Privacy and Civil Liberties Oversight Board. (2023). *Report on the surveillance program operated pursuant to Section 702 of the Foreign Intelligence Surveillance Act*.

Rühlig, T. (2021). *China, Europe and the new power competition over technical standards* (UI Brief No. 1). Swedish Institute of International Affairs.

Srnicek, N. (2017). *Platform capitalism*. Polity Press.

Strange, S. (1988). *States and markets*. Blackwell.

Waltz, K. N. (1979). *Theory of international politics*. Addison-Wesley.

Legal and Policy Sources

CHIPS and Science Act, Pub. L. No. 117-167, 136 Stat. 1366 (2022).

Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Pub. L. No. 115-141, 132 Stat. 1213 (2018).

Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 on the adequate level of protection of personal data under the EU–U.S. Data Privacy Framework. *Official Journal of the European Union*, L 231, 1.

Data Protection Commissioner v. Facebook Ireland Ltd and Schrems (*Schrems II*), Case C-311/18, ECLI:EU:C:2020:559 (CJEU July 16, 2020).

Data Security Law of the People's Republic of China (2021).

Department of Home Affairs (Australia). (2018). *5G security guidance: Protecting Australia's 5G network*. Australian Government.

European Chips Act, Regulation (EU) 2023/1781. *Official Journal of the European Union*, L 229, 1.

Executive Order No. 13,942, 85 Fed. Reg. 48,637 (Aug. 6, 2020).

Executive Order No. 14,034, 86 Fed. Reg. 31,423 (June 9, 2021).

Executive Order No. 14,086, 87 Fed. Reg. 62,283 (Oct. 7, 2022).

Five Country Ministerial. (2019, July 30). *Five Country Ministerial communiqué: Emerging threats, London 2019*.

Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1881a (2018).

Huawei Cyber Security Evaluation Centre Oversight Board. (2019). *Annual report 2019: A report to the National Security Adviser of the United Kingdom*.

Japan, *Keizai Anzen Hoshō Suishin Hō* [Economic Security Promotion Act], Law No. 43 of 2022.

Ministry of Commerce of the People's Republic of China. (2020). *Catalogue of technologies prohibited or restricted from export* (rev. Aug. 28, 2020).

National Intelligence Law of the People's Republic of China (2017).

Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, div. H (2024).

Schrems v. Data Protection Commissioner (*Schrems I*), Case C-362/14, ECLI:EU:C:2015:650 (CJEU Oct. 6, 2015).

State-owned Assets Supervision and Administration Commission. (2022, September). *Document 79: Notice on accelerating digital transformation of state-owned enterprises*.

Telecoms Security Act 2021, c. 31 (UK).

TikTok Inc. v. Garland, No. 24-1113 (D.C. Cir. Dec. 6, 2024).

TikTok Inc. v. Garland, No. 24-656, slip op. (U.S. Jan. 17, 2025).

TikTok Inc. v. Trump, No. 1:20-cv-02658 (D.D.C. 2020).

U.S. Department of State. (2020). *The Clean Network*.