**Working Paper**

**T-Series Information:** The WP-T series develops general theoretical frameworks for analyzing power, networks, systems, boundaries, and structural transformation across multiple domains. It emphasizes transferable concepts that can support later applied research in AI, governance, geopolitics, infrastructure, and security.

**Recommended Citation:** Wu, S. (2026). *Beyond Centrality: Conditional Connectivity and Boundary Control in Interdependent Networks* (EPINOVA Working Paper No. EPINOVA–WP–T–2026–01). Global AI Governance and Policy Research Center, EPINOVA LLC. https://doi.org/10.67037/epinova.wp.t.2026.01

**Disclaimer:** This working paper presents theoretical and exploratory analysis intended to develop and examine conceptual frameworks for complex systems, networks, power, and structural transformation. It does not constitute legal advice, predictive assessment, or an official position of EPINOVA LLC or any affiliated institution. Any policy implications discussed are analytical in nature and should not be interpreted as institutional recommendations.

GLOBAL AI GOVERNANCE RESEARCH CENTER

EPINOVA

# Beyond Centrality:

## Conditional Connectivity and Boundary Control in Interdependent Networks

**Author:** Shaoyuan Wu

**ORCID:** https://orcid.org/0009-0008-0660-8232

**Affiliation:** Global AI Governance and Policy Research Center, EPINOVA LLC

**Date:** August 31, 2026

**Abstract**

Network analysis has transformed the study of power by showing how centrality, brokerage, dependence, exit options, and network topology shape influence. Contemporary network science also provides mature tools for multilayer, temporal, and interdependent networks, while weaponized-interdependence research demonstrates that jurisdiction and domestic institutions can convert structural position into coercive leverage. The theoretical problem is therefore not that existing approaches cannot represent complex or selective access. It is that substantive analyses often aggregate the usability of a relation into an edge or treat authorization and implementation as context rather than as separately observable conditions. This article develops a Node-Boundary-Network-System (NBNS) framework centered on conditional usability. A boundary is defined as an actor-, function-, direction-, and time-indexed admissibility state. Rules define admissibility criteria; interfaces implement crossing; and control-rights bundles identify who may set, interpret, authorize, veto, enforce, or override those conditions. The framework separates structural position, available leverage, boundary action, admissible capacity, target response, network adaptation, and system transformation, and it distinguishes systemic effects from systemic power. Capacity equations are restricted to explicitly ratio-scaled admissible capacity and separate authorized flow, unauthorized flow, and probabilistic approval. A semiconductor-export-control walkthrough uses a concrete NVIDIA A100/H100 product-time trace to illustrate the coding logic without claiming a causal estimate of policy effectiveness. Four discriminating hypotheses and a three-layer comparison strategy specify how NBNS can be tested not only against topology-only baselines but also against near-neighbor theories that already incorporate jurisdiction, institutions, dependence, and cross-network position.

**Keywords**: network power; conditional connectivity; boundary control; interdependence; access; decentralization; systemic power; strategic distance; AI governance

## 1. Introduction

Power in contemporary political economy and security is increasingly exercised through systems whose strategic properties depend on relations among states, firms, platforms, infrastructures, standards, and institutions. Financial clearing, semiconductor production, cloud computing, military logistics, data platforms, energy systems, maritime corridors, and artificial intelligence all exhibit forms of relational dependence in which the value of an actor or facility cannot be inferred from its intrinsic resources alone. Network scholarship has accordingly shifted analysis toward centrality, brokerage, dependence, exit options, and topology (Bonacich, 1987; Burt, 1992; Granovetter, 1973; Hafner-Burton et al., 2009). Interdependence theory likewise emphasizes sensitivity, vulnerability, adjustment costs, and alternatives (Keohane & Nye, 2012).

The strongest versions of this relational turn already move well beyond static, unweighted graphs. Multilayer network theory explicitly models multiple kinds of relationships, interlayer coupling, and network-of-networks structures, while temporal-network research treats edges as time-varying rather than continuously active (Holme & Saramäki, 2012; Kivelä et al., 2014). Interdependent-network research demonstrates how failures can propagate across coupled infrastructures (Buldyrev et al., 2010). Political-economy scholarship goes further by showing that structural position becomes coercively consequential under institutional conditions. Farrell and Newman (2019), for example, argue that states with effective jurisdiction over central nodes and appropriate domestic institutions may obtain panopticon and chokepoint effects. Beaumier and Cartwright (2024) extend this logic across interconnected networks in the semiconductor supply chain. The present argument therefore does not claim that network science is incapable of representing conditional relations, nor that prior theories ignore institutional control.

The narrower problem concerns how a potential or technically existing relation becomes usable by a particular actor for a particular purpose. A semiconductor supplier may remain connected to a customer while a license requirement changes the transactions that may legally occur. A cloud service may be globally reachable while credentials, contract terms, platform policies, or export rules restrict particular users or functions. A port may remain intact while legal, insurance, or security conditions sharply reduce the set of commercially feasible voyages. A military facility may retain physical capacity while an agreement changes which forces may use it, for which missions, and under what authorization. In each case, topology alone does not identify the politically relevant state of the relation unless the access condition is itself encoded.

This article develops the Node-Boundary-Network-System (NBNS) framework around the concept of conditional usability. Its core object is not an abstract border, but an indexed access condition: usable by whom, for what function, in which direction, and at what time. A boundary is therefore treated as an admissibility state attached to a relation or functional transition. Rules specify the criteria that determine admissibility. Interfaces are the mechanisms through which crossing is operationally implemented. Controllers are actors holding distinct rights or capabilities to set, interpret, authorize, veto, exclude, enforce, or adjudicate those conditions. This separation is intended to reduce a recurrent measurement problem in which a single restriction is counted simultaneously as a boundary, a rule, an interface condition, and an actor capability.

The framework makes four contributions. First, it formalizes conditional usability as an actor-, function-, direction-, and time-specific object of substantive network analysis while explicitly recognizing that fine-grained authorization is already well developed in access-control engineering. Second, it separates ownership and node position from bundles of control rights, allowing several actors to possess different authorization, veto, enforcement, or adjudication powers over the same node or interface. Third, it decomposes the causal sequence from structural exposure to available leverage, boundary action, admissible-capacity change, target response, network adaptation, and durable system transformation. Fourth, it offers a discriminating research design: NBNS claims independent theoretical value only where its access, implementation, and control-right distinctions explain variation that remains unresolved after accounting for topology, resources, jurisdiction, institutional capacity, dependence, and cross-network position.

The argument is organized around a single mechanism. Section 2 establishes the strongest theoretical baselines and isolates the residual problem of selective usability. Section 3 then presents the NBNS causal architecture and unpacks its components: structural exposure, control rights, boundary action, indexed admissibility, admissible capacity and effective usability, target response, network adaptation, and system transformation. Section 4 demonstrates the coding logic through a concrete A100/H100 export-control trace. Section 5 derives three broader implications—decentralization, cross-network conversion, and strategic distance—and uses AI only as a bounded illustration. Section 6 converts the framework into hypotheses, measures, and comparative research designs; Section 7 states scope conditions and limitations; Section 8 concludes.

## 2. Theoretical Baseline and Residual Problem

### 2.1 Network Position, Interdependence, and Mature Network Models

The starting point is relational rather than possessive power. Bonacich (1987) showed that centrality and power are not identical because an actor's position can make it dependent on well-connected others rather than dominant over them. Burt (1992) emphasized brokerage advantages associated with structural holes, while Hafner-Burton et al. (2009) brought access, brokerage, and exit into international-relations network analysis. Keohane and Nye's (2012) distinction between sensitivity and vulnerability similarly directs attention toward adjustment costs and alternatives rather than aggregate capability alone.

Weaponized interdependence provides the most important near-neighbor theory. Farrell and Newman (2019) do not claim that centrality automatically generates coercion. Their argument requires effective jurisdiction over central economic nodes and domestic institutions able to convert structural advantage into action. The chokepoint effect already concerns denial of network access. NBNS therefore cannot establish novelty merely by adding 'control' to centrality or by observing that access can be denied. Instead, it asks a more fine-grained question: once a relation is structurally important, how are its terms of usability specified, differentiated across users and functions, implemented through interfaces, and altered over time?

Beaumier and Cartwright (2024) make the comparison more demanding. Their cross-network-weaponization framework shows how a state's position in one semiconductor network can enable coercion in another. This directly overlaps with any theory of conversion nodes or networks of networks. NBNS consequently treats cross-network weaponization as an established mechanism and confines its additional claim to the conditional access layer: the same cross-network chokepoint can expose different actors, end uses, products, and transactions to different admissibility states because control is exercised through rule criteria and implementation interfaces rather than through undifferentiated node removal.

NBNS does not define its contribution by contrasting a sophisticated ontology with a caricature of graph theory. Kivelä et al. (2014) provide a comprehensive framework for multilayer networks in which entities participate in multiple types of relationships and layers. Holme and Saramäki (2012) show that edge activity can be explicitly time dependent. Buldyrev et al. (2010) demonstrate how interdependence between networks can produce cascading failure. These literatures already supply formal languages capable of representing direction, weight, temporality, multiplexity, and cross-network dependence.

The proposed contribution is instead interpretive and operational: in many substantive applications, an edge variable records whether a relation exists, how much it carries, or how strong it is, while legal authority, authentication, eligibility, contractual permission, or mission authorization is encoded only indirectly. NBNS treats those conditions as a distinct empirical object when they are politically or institutionally manipulable. The framework is therefore compatible with multilayer and temporal network methods. Boundary states can be encoded as edge attributes, layers, temporal events, or constraints on feasible paths. The theory concerns what those attributes mean, who can change them, and how their change enters a causal explanation.

### 2.2 Selective Access, Control Rights, and Systems

Boundary scholarship establishes that boundaries can be social, symbolic, institutional, spatial, and relational rather than merely territorial (Lamont & Molnár, 2002). That literature is useful for clarifying inclusion, exclusion, classification, and membership, but it does not by itself provide a theory of network leverage. Likewise, boundary objects and boundary organizations concern coordination across heterogeneous communities; they should not be treated as synonyms for the access boundaries developed here. NBNS uses 'boundary' in a narrower operational sense: a condition on admissibility across analytically differentiated domains.

Protocol and standards scholarship is especially important for decentralized systems. Galloway (2004) argues that technical protocols can constitute mechanisms of control precisely where centralized command appears to recede. Grewal (2008) shows how standards of coordination gain network power as adoption expands and alternatives become less viable. These arguments imply that topological decentralization need not entail governance decentralization. NBNS builds on them by separating the distribution of nodes from the distribution of control rights over the conditions that make those nodes recognized, authenticated, interoperable, routable, or eligible.

Control also needs to be decomposed. Schlager and Ostrom (1992) distinguish bundles of rights rather than treating property as a single undifferentiated entitlement. Their approach motivates an analogous move here: ownership, operation, access authorization, exclusion, rule setting, enforcement, and adjudicative override are different rights that may be held by different actors. A firm can own a facility while a regulator controls licensing; an operator can implement access rules without possessing authority to change them; several actors can hold joint vetoes. NBNS therefore models control as a configuration of rights over a specified boundary rather than as a synonym for ownership.

Fine-grained indexing of access is not itself novel. Attribute-Based Access Control (ABAC), for example, determines authorization by evaluating attributes of the subject, object, requested operation, and, in some cases, the environment against policies and rules (Hu et al., 2019). NBNS does not claim to reinvent that access-control logic. Its proposed contribution is to translate selective admissibility into political-economic and security network analysis and connect it to structural dependence, distributions of control rights, deliberate boundary action, and downstream network or system adaptation. The actor-function-direction-time index is therefore a measurement discipline and bridge across literatures, not the sole basis of the originality claim.

Finally, a system should not be defined as a larger synonym for a network. Systems research emphasizes organized relations, functions, feedback, adaptation, and behavior over time. Holland's (1992) complex-adaptive-systems account highlights adaptation among interacting agents, while Meadows (2008) emphasizes stocks, flows, feedback, rules, and system behavior. The distinction matters for NBNS because a boundary action can leave the underlying physical network largely intact while changing flows, inducing substitution, altering investment, and eventually changing network structure itself. The system level is therefore the level at which feedback and adaptation modify the conditions of subsequent interaction.

### 2.3 Residual Problem, Claim Discipline, and Comparison Strategy

NBNS is a conceptual theory-building framework rather than a validated universal quantitative model. Its claim is deliberately incremental: the framework earns independent theoretical value only if actor-function-specific admissibility, implementation-interface evidence, and disaggregated control-right configurations distinguish cases that remain observationally similar under stronger near-neighbor explanations. Definitions, typological distinctions, and empirical hypotheses are therefore kept separate throughout the article.

The relevant empirical comparison is therefore three-layered. Baseline A uses topology and resource endowments. Baseline B adds dependence, jurisdiction, domestic institutional capacity, and cross-network position, reflecting the strongest near-neighbor explanations. NBNS constitutes Layer C: indexed admissibility, implementation interfaces, and disaggregated control-right configurations. The framework claims independent explanatory value only when Layer C distinguishes actor-function cases that Baseline B otherwise treats similarly. For example, two users facing the same strategic supplier and jurisdiction but receiving different authorization for different products or uses. If this added layer does not change prediction, explanation, or mechanism identification, NBNS should be treated as a descriptive coding framework rather than a separate theory of power.

**Table 1** summarizes the resulting division of labor across the closest literatures. The point is not that those literatures omit access or control, but that NBNS makes selective admissibility, implementation, and control-right configuration jointly observable within one causal sequence.

**Table 1. Positioning NBNS Relative to the Closest Literatures**

| Approach | Primary Explanatory Object | What It Already Explains | Specific NBNS Increment |
|---|---|---|---|
| **Centrality / Brokerage** | Network position | Access, brokerage, dependence, exit, structural advantage | Makes actor- and function-specific usability a separately coded condition when access is selective. |
| **Weaponized Interdependence** | Asymmetric hubs plus jurisdiction/institutions | Panopticon and chokepoint effects; coercive use of central nodes | Adds actor/function-specific admissibility, implementation-interface evidence, and disaggregated control rights; its increment must be tested after jurisdiction and institutional capacity are already included. |
| **Cross-network Weaponization** | Position across interconnected networks | Use of strength in one network to weaponize chokepoints in another | Adds selective admissibility at cross-network conversion interfaces and separates local access change, target response, and later rewiring; it does not claim cross-network leverage itself is novel. |
| **Multilayer / Temporal Networks** | Multiple relation types, layers, and time-varying edges | Complex topology, interlayer coupling, changing connectivity | Supplies a substantive theory of what access-state variables represent and who can change them. |
| **Protocol / Standards Power** | Rules of coordination and interoperability | Control through technical protocols and adopted standards | Separates topological decentralization from concentration of boundary-control rights. |
| **Systems / Complex Adaptation** | Feedback, function, adaptation over time | System behavior beyond static structure | Locates rerouting, recomposition, and rule change as adaptive outcomes rather than access states. |
| **Attribute-Based Access Control (ABAC)** | Subject/object/operation/environment attributes plus policy | Fine-grained authorization decisions in digital systems | Extends comparable indexing to political-economic relations and links it to control-right distributions, leverage, and adaptation rather than treating authorization as the final outcome. |

**Note:** The table treats NBNS as an incremental synthesis and measurement discipline. It does not imply that prior network, interdependence, protocol, access-control, or systems literatures lack selective access, institutional control, temporality, or adaptation.

**Sources:** Author's synthesis based on Bonacich (1987), Burt (1992), Hafner-Burton et al. (2009), Farrell and Newman (2019), Beaumier and Cartwright (2024), Kivelä et al. (2014), Holme and Saramäki (2012), Hu et al. (2019), Schlager and Ostrom (1992), Galloway (2004), Grewal (2008), Holland (1992), and Meadows (2008).

## 3. The NBNS Core Mechanism

### 3.1 Causal Architecture: From Structural Exposure to System Adaptation

**Figure 1** states the paper's core argument before the framework is decomposed into its component concepts. Structural position and target dependence create exposure, while boundary-control rights and discretion determine whether that exposure is convertible into available leverage. Purposeful boundary action then changes indexed admissibility and, where relevant, admissible capacity or other dimensions of effective usability; targets respond, networks adapt, and only some persistent adaptations become system transformations. The sequence is conditional rather than deterministic, and long-run feedback can alter both structural position and the distribution of control rights.

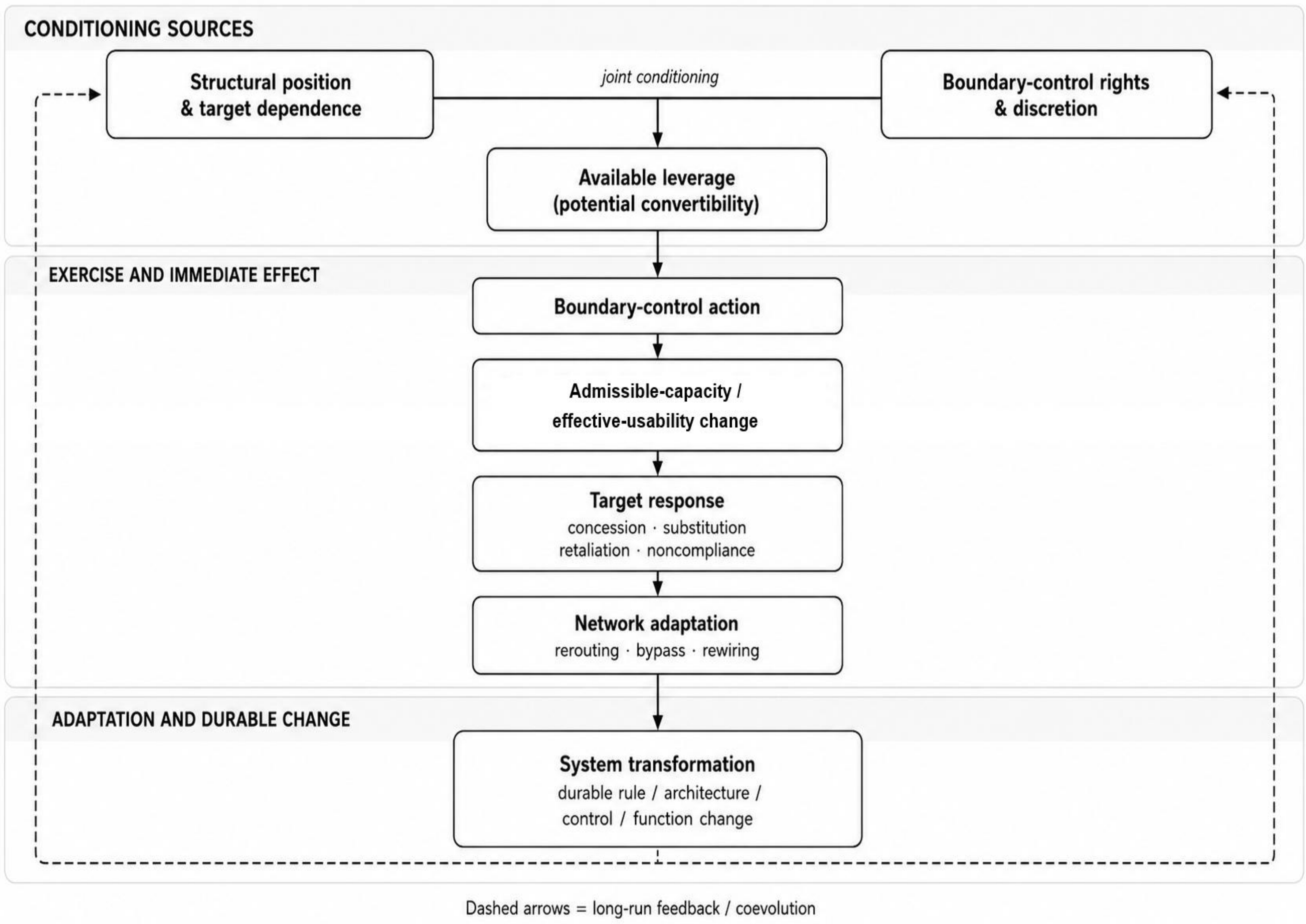


**Figure 1. Causal Architecture of Boundary-Conditioned Network Power**

**Note:** Structural position/target dependence and boundary-control rights/discretion are separate conditioning sources that jointly shape available leverage; they are not sequential mediators. Solid arrows trace the principal mechanism. Dashed arrows indicate longer-run feedback. Rerouting or substitution remains a network adaptation unless it durably changes rules, architecture, control, interoperability, or functional reproduction.

**Sources:** Author's conceptual synthesis drawing on Farrell and Newman (2019), Beaumier and Cartwright (2024), Schlager and Ostrom (1992), Hu et al. (2019), and the feedback/adaptation logic of Holland (1992) and Meadows (2008).

Boundary power is the capacity to alter the indexed admissibility conditions under which actors, resources, information, authority, or functions cross between domains. It is relational and action-specific. An actor may possess extensive resources yet little boundary power if it cannot change access conditions faced by others. Conversely, a regulator, platform administrator, standards body, or infrastructure operator can exercise boundary power without owning all of the nodes whose use is affected.

Systemic effects and systemic power are not equivalent. A systemic effect is any downstream change in the operation or structure of multiple networks or in system outputs, regardless of whether an actor intended or controlled it. Systemic power is the attributable capacity of an actor to use relevant control rights deliberately to produce a durable change in rules, interoperability conditions, distributions of boundary control, network architecture, or functional reproduction across multiple networks. Large unintended cascades are therefore systemic effects but not, by themselves, evidence that the initiating actor possessed systemic power.

Boundary power is exercised when an actor purposefully uses a consequential node or interface, together with the relevant control rights, to alter the admissibility conditions or feasible options faced by another actor. Structural position may generate dependence, but boundary-control rights and discretion condition whether that dependence is convertible into available leverage. Boundary action is the mechanism through which such leverage is exercised; changes in admissible capacity or effective usability are intermediate outcomes. Target concession, substitution, retaliation, circumvention, or noncompliance occur at a subsequent stage, while network adaptation and durable system transformation are downstream consequences.

### 3.2 Actors, Nodes, Boundaries, Rules, and Interfaces

Actors and nodes must be separated analytically. An actor is an entity to which purposive choice, authority, or control rights can be attributed for the analysis: a state agency, firm, platform operator, alliance body, regulator, standards organization, or other decision-capable entity. A node is a functional concentration within a relational structure: a facility, platform, exchange, cloud region, port, model service, standards body, clearing mechanism, or other locus through which a consequential function is provided. An actor may control several nodes, and a node may be subject to several actors' rights.

This distinction prevents double counting across levels. A state is not automatically coded as a node merely because firms and facilities located in its jurisdiction are nodes. Conversely, a firm operating a node does not automatically possess the regulator's authority to define permissible use. Researchers must specify the actor, the node, the function under analysis, and the right through which the actor can affect that function.

#### 3.2.1 Boundary as an Indexed Admissibility Condition

A boundary is an actor-, function-, direction-, and time-specific admissibility condition governing whether and to what extent a relation or functional transition can be used across analytically differentiated domains. The key question is not whether an abstract system is 'open' or 'closed,' but open to whom, for what, in which direction, and when. The same API can permit read access while denying write access; the same port can accept civilian traffic while excluding military use; the same export channel can remain open for mature products while requiring licenses for advanced items; and the same alliance facility can permit training but require separate authorization for combat operations.

Let $e$ denote a potential relation. Its boundary state can be written as $B_e(a, f, d, t)$, where a identifies the relevant user or target actor, f the function or use, d the direction of crossing, and $t$ the observation time. $B$ is not assumed to possess a universal numeric scale. It may be categorical, ordinal, probabilistic, or ratio-scaled depending on the substantive mechanism and evidence. Equation (1) therefore records membership in a domain-specific admissibility representation rather than forcing every boundary into the interval [0,1]. When a capacity equation is used later, a separate ratio-scaled capacity-share parameter is defined explicitly.

$$\boldsymbol{B_e(a, f, d, t) \in \mathcal{B}_e} \tag{1}$$

### 3.2.2 Rules, Interfaces, and the Source of Admissibility

Rules and interfaces are analytically distinct from the boundary state. Rules specify the criteria under which admissibility is determined. They may be laws, licenses, contracts, platform policies, membership conditions, certification requirements, technical standards, procurement rules, alliance procedures, or institutional mandates. Interfaces are the technical, physical, organizational, or procedural mechanisms through which crossing is implemented: an API gateway, customs process, cloud account, identity provider, port terminal, payment message, foundry order, security agreement, or software protocol.

The same empirical object can perform more than one role, but the roles must not be counted as duplicate variables. A protocol can simultaneously encode a rule and serve as an interface; an organization can own a node and administer access to it. Coding should therefore record functions rather than force every object into a single mutually exclusive category. The boundary state is the outcome to be explained at the access layer; rules and interface conditions are inputs that help determine that state.

$$\boldsymbol{B_e(a, f, d, t) = g\left[R_e(t), I_e(t), U_{a,e}(t), f, d\right]} \tag{2}$$

Here $R_e$ denotes the relevant rule configuration, $I_e$ the operational status and interoperability of the interface, and $U_{a,e}(t)$ the target actor's authorization, identity, or qualification status. Equation (2) is deliberately functional rather than multiplicative. It does not assume that rules, interfaces, and user attributes are independent variables; it states only that the observed admissibility state should be traced to distinguishable criteria and implementation conditions.

### 3.3 Control-Rights Bundles and Available Leverage

Boundary power depends on control rights, but control should not be inferred from ownership alone. A controller is an actor possessing one or more rights or capabilities to change, interpret, authorize, veto, exclude, enforce, or adjudicate the relevant boundary condition. These rights may be unilateral, shared, delegated, conditional, or contested. Joint authorization can make a nominally central actor unable to act alone; a regulator can possess exclusion authority without operating the underlying node; and a platform operator can implement a rule written by a state or standards body.

For a given boundary $b$ and time $t$, the control profile $C(a, b, t)$ **is** therefore a bundle rather than a scalar. Empirical research can represent the bundle categorically or score individual rights when valid measures exist. The central discipline is to identify which right is necessary for the action being explained.

**Table 2** illustrates why "control" should be coded as a bundle of potentially separable rights rather than inferred from ownership or jurisdiction alone.

**Table 2. Illustrative Control-Rights Bundle**

| Right | Analytical Meaning | Example Evidence |
|---|---|---|
| **Ownership** | Legal/economic claim over the node or asset | Corporate records, title, share structure |
| **Operation** | Ability to run or configure the node/interface | Operating agreements, technical administrator privileges |
| **Authorization** | Ability to approve access or use | Licenses, credentials, mission approval, account permissions |
| **Veto / Exclusion** | Ability to block a specified use or actor | Legal veto, sanctions authority, platform ban, contractual exclusion |
| **Rule Setting** | Ability to define admissibility criteria | Regulation, protocol governance, standards process, procurement rules |
| **Enforcement** | Ability to make a rule effective in practice | Inspections, technical controls, penalties, account suspension |
| **Adjudication / Override** | Ability to interpret disputes or reverse decisions | Courts, appeals bodies, supervisory authority |

**Note:** Rights are analytically separable and may be distributed across multiple actors. The same actor may hold several rights, and a single boundary may be subject to joint or nested authority.

**Sources:** Author's conceptual adaptation of the bundle-of-rights logic in Schlager and Ostrom (1992), supplemented by authorization and policy-evaluation logic in Hu et al. (2019).

### 3.4 Networks, Systems, and Analytical Levels

A network is the relational configuration through which potential and realized interactions occur at a given time. For a substantive application, it can be represented as $N_t = (V, E, K, B, I, R, X)$, where $V$ is the node set; E the potential relations; $K$ the baseline technical or organizational capacity associated with those relations; $B$ the indexed boundary states; $I$ the interfaces; $R$ the relevant rules; and $X$ the realized flows or uses. This is not proposed as a replacement for established graph formalisms. It is a bookkeeping representation intended to prevent effective access from being silently equated with relation existence.

A system is not simply a network with more nodes. It is a configuration of one or more interacting networks that reproduces functions or outputs and changes through feedback and adaptation. Let $\Sigma_t$ denote a system comprising multiple networks $N_t^m$, cross-network coupling or conversion relations $Q_t$, system outputs $Y_t$, and an adaptation operator $\Gamma$. Actor actions $A_t$ and external shocks $Z_t$ can change boundary states, flows, investment, topology, rules, and interfaces, producing a new system configuration at $t+1$.

$$\boldsymbol{N_t = (V, E, K, B, I, R, X)} \quad \textbf{(3)}$$

$$\boldsymbol{\Sigma_t = (\{N_t^m\}, Q_t, Y_t, \Gamma), \qquad \Sigma_{t+1} = \Gamma(\Sigma_t, A_t, Z_t)} \quad \textbf{(4)}$$

This distinction reserves the network level for relational structure and realized use, while the system level captures functions, feedback, cross-network coupling, and adaptation over time. A change in flow with unchanged topology is therefore a network event; persistent rerouting that induces new capacity, new institutions, or new rules becomes a system-adaptation process.

**Table 3** consolidates the core concepts by assigning each one a distinct analytical question. This reference table is intended to prevent the same empirical restriction from being counted simultaneously as a rule, interface, boundary state, and actor capability.

**Table 3. Core Concepts and Non-overlapping Analytical Questions**

| Concept | Definition in NBNS | Core Question |
|---|---|---|
| **Actor** | Decision-capable entity to which authority or control rights are attributed | Who can choose or authorize a relevant action? |
| **Node** | Functional concentration in a network | What function is concentrated here? |
| **Boundary** | Indexed admissibility condition on a relation or transition | Usable by whom, for what, in which direction, and when? |
| **Rule** | Criterion that defines admissibility | Why is the crossing permitted, restricted, or denied? |
| **Interface** | Mechanism that operationally implements crossing | How is the crossing accomplished or blocked? |
| **Control-Rights Bundle** | Rights/capabilities to set, authorize, veto, enforce, or adjudicate | Who can change or implement the boundary condition, and how? |
| **Network** | Potential and realized relational structure at time t | What is connected, usable, and actually flowing? |
| **System** | Interacting networks, outputs, feedback, and adaptation over time | How does the wider configuration reproduce functions and adapt? |

**Note:** Definitions are analytical roles rather than claims that the listed objects are ontologically independent in every empirical setting. A single empirical object may perform multiple roles, but each role should be evidenced and coded separately.

**Sources:** Author's framework, informed by the network, access-control, control-rights, protocol, and systems literatures reviewed in Sections 2 and 3.

### 3.5 Admissible Capacity, Flow, and Probabilistic Approval

A general boundary state should not be reused automatically as a capacity multiplier. For a capacity application, let $K_e(t)$ denote the baseline technical or organizational capacity of relation e for the same specified task and observation period. Define $\beta_e^K(a, f, d, t)$ as the fraction of that baseline capacity that is legally and operationally admissible for the indexed actor-function-direction-time tuple. This is a ratio-scale definition: $\beta_e^K = 0.5$ means that one-half of the relevant baseline capacity is admissible. Ordinal restriction scores, approval probabilities, prices, waiting times, or generalized friction measures are not inserted into Equation (5) unless a substantive mapping to capacity share is independently justified.

$$K_e^{adm}(a, f, d, t) = K_e(t)\, \beta_e^K(a, f, d, t), \quad \beta_e^K(a, f, d, t) \in [0, 1] \tag{5}$$

Equation (5) is therefore narrower than a general theory of access. It is appropriate when admissible capacity can be measured or defensibly bounded. A formal license requirement alone does not establish $\beta_e^K$; implementation evidence is required to determine how much authorized capacity is actually available. When the empirical quantity is a probability of case-by-case approval, the probability is modeled separately rather than treated as a realized capacity fraction.

Admissible capacity is also not the same as observed total flow. Let $X_e^{auth}$ denote authorized or lawful flow and $X_e^{unauth}$ unauthorized, evasive, or otherwise noncompliant flow. Only the authorized component is bounded by the admissible-capacity measure. Observed flow may remain positive even when formal authorized capacity is zero if implementation is incomplete or actors evade the restriction. Conversely, demand, price, expectations, congestion, or strategy can keep authorized flow below the available ceiling.

$$0 \le X_e^{auth}(a, f, d, t) \le K_e^{adm}(a, f, d, t), \qquad X_e^{obs} = X_e^{auth} + X_e^{unauth} \tag{6}$$

The framework therefore distinguishes baseline relation capacity, admissible authorized capacity, realized authorized flow, and observed total flow. It also separates probabilistic approval from realized availability. Where a transaction is approved or denied case by case, $A_e$ is the realized binary approval state; expected available capacity can be computed from the approval probability under stated assumptions, but that expectation is not a hard ceiling on any particular approved transaction. Empirical studies must specify which quantity is measured before attributing a change to boundary control.

For probabilistic access, Equation (7) distinguishes the realized approval state from its expectation. The expected quantity is useful for repeated transactions or ex ante planning, but it must not be interpreted as the maximum capacity available in every realized case. In Equation (7), $K_e$ is treated as fixed for the specified transaction or observation period; the binary approval state determines whether that baseline capacity is available in the realized case.

$$K_e^{available} = K_e A_e, \quad A_e \in \{0, 1\}, \qquad \mathbb{E}\left[K_e^{available}\right] = K_e \Pr(A_e = 1) \tag{7}$$

### 3.6 Boundary Actions, Target Responses, and Downstream Transformation

The framework separates categories that belong to different analytical levels. Open, filtered, restricted, and denied describe access states. Granting, authenticating, filtering, throttling, conditioning, restricting, and denying are boundary actions that can move a relation between states. Rerouting, substitution, bypass, and rewiring are network adaptations. Transfer, recomposition, fragmentation, and integration refer to more durable system transformations.

This separation allows several conditions to coexist without contradiction. A port can be denied to a specified military function while commercial access remains filtered rather than closed. A target network can reroute around that denial. The lost function can later be recomposed across several substitute nodes. None of these observations requires saying that the original node has been 'transferred' to a rival network.

**Table 4** separates access states, boundary actions, network adaptations, and system transformations so that events occurring at different causal stages can coexist without being coded as mutually exclusive "states."

**Table 4. Distinguishing States, Actions, Adaptations, and Transformations**

| Analytical Level | Examples | What Changes? |
|---|---|---|
| **Access State** | Open; filtered; restricted; denied. Open: no function-specific authorization constraint beyond routine conditions. Filtered: eligibility depends on actor/item/end-use attributes but an authorized path exists. Restricted: authorization remains possible but binding quantity, throughput, time, cost, or case-by-case review reduces usable access. Denied: no authorized path for the indexed tuple during the observation window based on implemented rule/decision evidence; a license requirement or presumption of denial alone is not coded as actual denial. | Current admissibility for a specified actor/function/direction/time, coded separately from formal rule language, license application status, approval decision, and measured capacity. |
| **Boundary Action** | Grant; authenticate; filter; throttle; condition; restrict; deny | A controller intentionally changes or enforces an admissibility condition |
| **Network Adaptation** | Rerouting; substitution; bypass; rewiring | Flows or relations shift in response to changed effective connectivity |
| **System Transformation** | Transfer; recomposition; fragmentation; integration | Persistent architecture, membership, rules, or functional reproduction changes |

**Note:** Access state is indexed to actor, function, direction, and time. Boundary action is purposeful intervention; network adaptation is a relational response; system transformation requires durable change in rules, architecture, control, interoperability, or functional reproduction.

**Sources:** Author's framework; cascade and adaptation distinctions are informed by Buldyrev et al. (2010), Holland (1992), and Meadows (2008).

### 3.6.1 Boundary Cascades and Conditional System Repricing

A boundary action can propagate, but propagation is neither novel in itself nor inevitable. Interdependent-network research already demonstrates how local failures can cascade across coupled networks (Buldyrev et al., 2010). The NBNS increment concerns a particular initiating event: an intentional, selective, and potentially reversible change in admissibility. Such a change can alter flows, congestion, queueing, costs, expectations, and investment even when no node is physically destroyed.

System repricing should therefore be treated as a family of outcomes rather than a single variable. Substitute-node load may rise while profit falls because congestion or compliance costs increase. Market valuation can move differently from capacity utilization. Strategic attention can increase even when commercial revenue does not. The sign of the effect depends on persistent demand, substitute feasibility, spare capacity, expectations, time horizon, and policy response. Repricing is thus an empirical consequence to be measured separately in traffic, price, utilization, investment, valuation, or political attention rather than inferred from rerouting alone.

## 4. Empirical Walkthrough: U.S. Advanced-Semiconductor Export Controls

The semiconductor case is used here as an illustrative coding walkthrough with one concrete product-time trace, not as a causal estimate of the overall effectiveness of U.S. technology controls. Farrell and Newman (2019) already explain how jurisdiction and institutions can weaponize central network positions, and Beaumier and Cartwright (2024) show how semiconductor positions can be weaponized across linked networks. The NBNS question is narrower: once that structural opportunity exists, how should differentiated access, implementation, control rights, authorized capacity, target response, and later adaptation be observed without collapsing them into a single statement that a chokepoint has been 'used'?

The time index matters because relevant controls did not take effect on a single date. NVIDIA reported that on August 26, 2022 the U.S. government informed the company of an immediate license requirement for future exports to China, including Hong Kong, of its A100 and forthcoming H100 integrated circuits and systems incorporating them (NVIDIA Corporation, 2022b). The U.S. Bureau of Industry and Security (BIS) then issued the broader October 7, 2022 rule in phases: specified semiconductor-manufacturing-item restrictions took effect October 7, U.S.-person support restrictions on October 12, and advanced-computing and supercomputer controls on October 21 (BIS, 2022). BIS announced updated advanced-computing rules on October 17, 2023 with a general effective date of November 16, 2023; NVIDIA later reported that on October 23 the government informed it that licensing requirements were effective immediately for shipments of several named products, including A100, A800, H100, H800, and L40S (BIS, 2023; NVIDIA Corporation, 2024). Event coding must therefore distinguish announcement, formal effective date, and transaction-specific implementation.

A September 1, 2022 NVIDIA Form 8-K adds an important scope qualification. The company disclosed authorization for exports, reexports, and in-country transfers needed to continue development of the H100 integrated circuit, authorization through March 1, 2023 for A100 exports needed to support U.S. customers, and authorization through September 1, 2023 for A100 and H100 order fulfillment and logistics through the company's Hong Kong facility (NVIDIA Corporation, 2022a). These authorizations did not amount to blanket approval for all commercial shipments to Chinese end users. In NBNS terms, development, customer support, logistics, and final commercial use are distinct functions and must be coded separately rather than inferred from product name and destination alone.

The case also illustrates the Rule-Interface distinction. Product classifications, end-use criteria, Entity List status, foreign direct product (FDP) provisions, and license policies are rule or eligibility conditions. Implementation interfaces are the procedures through which those conditions are operationalized: transaction screening against item, end-use, Entity List, and FDP requirements; license review; exporter and foundry compliance checks; U.S.-person due diligence; and the technical or commercial transaction channel itself. A license requirement is therefore not identical to denial, and a presumption-of-denial policy is not identical to a transaction-level denial decision.

The concrete NVIDIA trace provides some implementation and response evidence but not a direct measure of admissible capacity. In its fiscal-year 2024 Form 10-K, NVIDIA stated, in the context of the October 23, 2023 immediate licensing requirement, that it had not received licenses to ship the covered restricted products to China as of that disclosure. The same filing reported that China's share of its Data Center revenue fell from 19 percent in fiscal 2023 to 14 percent in fiscal 2024 and to a mid-single-digit share in the fourth quarter, and that it had begun shipping alternative products to the China market in small volumes (NVIDIA Corporation, 2024). These observations support a time-bounded, product-specific change in authorized access and supplier adaptation. They do not establish that every use, exception, support activity, or logistics channel was unauthorized throughout the full 2022-2024 observation window, do not identify $K_e^{adm}$ directly, and cannot by themselves establish the causal effect of export controls on revenue. Demand shifts, product cycles, strategic anticipation, stockpiling, and preexisting localization efforts remain alternative explanations for downstream outcomes.

The discriminating value of NBNS lies in comparisons that hold the near-neighbor structural explanation as constant as possible. The same supplier, destination, and jurisdiction can exhibit different admissibility across products, users, end uses, and time; a mature product may remain commercially available while an advanced product requires a license; and an otherwise interoperable transaction channel may remain physically intact while authorization changes. A position-plus-jurisdiction theory identifies the strategic setting. NBNS adds value only if the finer access and implementation distinctions generate different predictions or better mechanism identification among cases that this second-level baseline otherwise treats similarly.

**Table 5** applies the NBNS coding sequence to this narrow product-time trace. The table separates controller and rights, rule criteria, implementation interfaces, boundary-state evidence, observable flow/response indicators, and unresolved causal questions rather than treating “export control” as a single variable.

Working Paper

**Table 5. NBNS Coding of the Semiconductor-Control Walkthrough**

| Element | Concrete A100/H100 Coding | Evidence / Interpretation |
| --- | --- | --- |
| **Actor / Product / Function / Period** | NVIDIA A100 and H100 (plus covered systems), with commercial shipment to China including Hong Kong as the primary function; development, U.S.-customer support, and Hong Kong order-fulfillment/logistics authorizations are coded as distinct functions. August 2022 through fiscal 2024 trace. | NVIDIA Corporation (2022a, 2022b, 2024). The trace is intentionally narrow; it is not a claim about the whole semiconductor ecosystem. |
| **Controller And Control Rights** | U.S. government / BIS: rule-setting, licensing, enforcement; NVIDIA and transaction partners: compliance implementation. | Control rights are disaggregated rather than assigned to "the United States" as a single node. |
| **Rule / Eligibility Condition** | Immediate license requirement reported August 26, 2022 for A100/H100; use-specific temporary authorizations disclosed September 1, 2022; broader BIS controls phased October 7/12/21, 2022; 2023 updates altered thresholds and licensing scope, with a company-specific immediate implementation notice reported October 23, 2023. | BIS (2022, 2023); NVIDIA Corporation (2022a, 2022b, 2024). Announcement, effective date, function-specific authorization, and company-specific implementation are coded separately. |
| **Implementation Interface** | Transaction screening against item/end-use/Entity List/FDP requirements; BIS license review; exporter/foundry compliance and U.S.-person due diligence. | Entity List designation and FDP rules are eligibility/rule conditions; screening and licensing procedures are implementation interfaces. |
| **Boundary-State Coding** | A license requirement is a formal rule condition rather than, by itself, an observed boundary state. Depending on authorization availability and implementation evidence, the resulting state may be coded as filtered or restricted; it should not be coded as denied without transaction- or implementation-level evidence. The September 2022 authorizations are coded separately by function: H100 development, A100 support for U.S. customers through March 1, 2023, and A100/H100 order fulfillment and logistics through Hong Kong through September 1, 2023. For products covered by the October 23, 2023 immediate licensing requirement, NVIDIA stated in its FY2024 Form 10-K that it had not received licenses to ship the restricted products to China as of the filing. This is a time-bounded company report for the specified restricted products, not a claim that all uses, exceptions, or channels were unauthorized throughout 2022-2024. | Actual denial requires decision or implementation evidence. Temporary or function-specific authorizations, a license requirement, a presumption of denial, and an observed shipment denial are separate records and should not be collapsed into one boundary-state label. |
| **Admissible Capacity and Flow** | Direct $K^{adm}$ is not observed in the cited public materials. Revenue share and shipment statements are outcomes, not capacity measures. | The trace therefore does not assign $\beta^K$ from rule text. Shipment/license records would be required for a capacity estimate. |
| **Observed Supplier Response** | NVIDIA reported moving some operations out of China/Hong Kong and shipping alternative China-market products in small volumes; China Data Center revenue share declined. | NVIDIA Corporation (2024). These facts show adaptation, not a clean causal estimate of the controls. |

**Table 5. NBNS Coding of the Semiconductor-Control Walkthrough (Cont.)**

| Element | Concrete A100/H100 Coding | Evidence / Interpretation |
|---|---|---|
| **Broader Target Adaptation** | Chinese localization, mature-node investment, and design-around efforts are documented, but some projects were announced rather than completed and localization predated the controls. | Allen (2024); Goujon et al. (2022); Kleinhans et al. (2023). Evidence should be coded as intention, investment, capacity, technical result, or causal effect rather than merged. |
| **Alternative Explanations / System Outcome** | Demand, product cycles, anticipation, stockpiling, allied policy changes, and preexisting industrial policy can affect observed outcomes. Durable system transformation cannot be inferred from the initial access change alone. | Longitudinal evidence is required before coding persistent rewiring, fragmentation, or system-level power. |

**Note:** This is an illustrative coding walkthrough, not a causal estimate of the effectiveness of U.S. export controls. Development authorization, customer support, logistics/fulfillment, license requirements, final commercial shipment, observed sales, and later adaptation are coded as distinct functions and time-indexed observations. Unknown admissible capacity is left unobserved rather than inferred from legal text alone.

**Sources:** U.S. Bureau of Industry and Security (2022, 2023); NVIDIA Corporation (2022a, 2022b, 2024); Goujon et al. (2022); Kleinhans et al. (2023); Allen (2024); and Beaumier and Cartwright (2024).

## 5. Derived Implications of the Core Mechanism

The following implications are downstream deductions from the core mechanism, not parallel theories. Each asks what follows once conditional usability and control-right distributions are treated as distinct from topology.

### 5.1 Decentralization and the Distribution of Boundary Control

The claim that decentralized systems remain bounded is too weak to carry much theoretical weight. A stronger and more measurable proposition is that different forms of decentralization can vary independently. At minimum, researchers should distinguish node concentration, infrastructure concentration, interface concentration, ownership concentration, and boundary-control concentration. Galloway's (2004) account of protocol is relevant precisely because distributed architectures can remain governed through technical standards that enable and disable connectivity.

Topological decentralization and boundary-control decentralization are conceptually distinct and need not covary. A system may contain a very large number of nodes and operators while a small number of identity providers, root authorities, cloud platforms, protocol maintainers, or licensing bodies control consequential admission conditions. The opposite configuration is also possible. No deterministic equality or inequality is proposed between the two dimensions; each must be measured on the relevant population of nodes, interfaces, rights, or decisions.

Empirical research should not proxy boundary-control concentration with interface count. A hundred interfaces administered under one rule-setting authority can be highly decentralized physically and highly concentrated institutionally. One interface subject to several independent authorizers can exhibit the opposite configuration. Concentration metrics must therefore be calculated over the relevant control rights or decision shares, not inferred from the number of endpoints alone.

### 5.2 Cross-network Conversion Interfaces

A cross-network conversion interface is an interface whose operation is necessary to transform a resource, authorization, representation, or function from a form usable in one network into a form usable in another. This narrower term avoids relabeling ordinary production nodes merely because they transform inputs. The analytically relevant question is whether control over the conditions of cross-network conversion provides leverage beyond control of the underlying productive asset itself.

Strategic significance comes not from the label 'conversion' but from dependence on the transition and from control over its admissibility conditions. This is where NBNS complements cross-network weaponization. Beaumier and Cartwright (2024) show how power in one semiconductor network can be leveraged across another. NBNS adds the question of which actors and functions are allowed to traverse the conversion interface, which rules define that permission, which actors hold the relevant rights, and how targets adapt when access changes.

### 5.3 Strategic Distance as Generalized Task Cost

Strategic distance should not be defined as a sum that already contains 'boundary friction' and then adds cost, delay, and risk again. Nor should redundancy be treated as an unexplained property of a single path. Network research already demonstrates that effective distance can differ sharply from geographic distance (Brockmann & Helbing, 2013). NBNS therefore uses a task-specific generalized-distance formulation rather than claiming to invent nongeographic distance.

For actor a seeking to produce function f at target z and time t, the task must first be fixed—for example by required quantity q* and deadline τ. Let P(a, z, f, t | q*, τ) be the paths that remain feasible for that task given current admissibility conditions and capacity. Strategic distance is the minimum generalized cost over that feasible set. $C_p$ is path cost, $L_p$ latency, and $R_p$ a justified measure of political, legal, operational, or security risk; the weights are research-design parameters rather than universal constants. Partial restriction can also increase $C_p$ or $L_p$ through queueing, licensing delay, or throttling without eliminating the path altogether.

$$\boldsymbol{D_s(a \to z, f, t \mid q^*, \tau) = \min_{p \in P(a,z,f,t \mid q^*,\tau)} \left[ w_c C_p + w_l L_p + w_r R_p \right]} \tag{8}$$

If the feasible set is empty, the fixed task is unreachable under the defined conditions and $D_s$ can be treated as infinite for that analysis. Redundancy enters through the number and quality of feasible alternatives rather than as a duplicated path attribute. Boundary change affects strategic distance either by removing paths from the feasible set or by changing the cost, latency, or risk of paths that remain feasible. Strategic-distance rebound occurs when a previously low-cost route becomes inadmissible or sufficiently degraded that the minimizing path shifts to a more costly alternative. For the same fixed task, if the costs of surviving feasible paths are unchanged, contraction of the feasible path set implies:

$$\boldsymbol{P_{t+1} \subseteq P_t \Rightarrow D_s(t+1) \geq D_s(t)} \tag{9}$$

### 5.4 AI as a Bounded Illustration

Artificial intelligence remains useful for illustrating NBNS because AI capability depends on layered and selective access conditions, but the AI application is not evidence that validates the general theory. Prior work distinguishes model capability from data quality, resource access, authority, real-world interfaces, and rule space (Wu, 2026b); stratifies AI systems by access threshold, institutional embedding, resource authority, intervention capacity, and differentiated rule conditions (Wu, 2026a); and maps global AI power as overlapping domains shaped by infrastructure, capital, platforms, regulation, language communities, public-sector adoption, and security integration (Wu, 2026c).

NBNS reinterprets these dimensions without collapsing them into 'boundary.' Data access can be represented as an admissibility condition on information flows; the rule governing that access is distinct from the database or API interface through which it is implemented. Resource authority can involve a control-rights bundle rather than simple ownership. Real-world interfaces connect analytical output to action. Rule spaces establish criteria that affect classes of boundary states. A public model and an embedded enterprise or security system may therefore share underlying technical capability while occupying different positions in the access-control architecture.

The illustrative value of AI lies in selectivity. An API can be open to one class of user, rate-limited for another, unavailable in a jurisdiction, restricted to particular models, or unable to call specified tools. Compute can be commercially available in one region but subject to licensing, identity, security, or procurement conditions in another. A model may be downloadable while the data, accelerator supply, cloud deployment, or operational authority required for a specific function remains constrained. These are precisely the situations in which an actor-function-time indexed access variable adds analytical clarity.

## 6. Empirical Implications and Research Design

### 6.1 Discriminating Hypotheses

This article proposes four empirical hypotheses. Definitions and typological claims are not counted as hypotheses. Each hypothesis specifies an observable outcome and a comparison that can weaken the claim. The relevant baseline is not limited to topology or resources: where possible, tests should compare NBNS against models that already include dependence, jurisdiction, institutional capacity, and cross-network position.

**Table 6** states four hypotheses that follow from the mechanism. Each requires an outcome measured independently from the rule or control-right variable used to explain it.

Working Paper

**Table 6. Core Hypotheses of the NBNS Framework**

| Hypothesis | Statement | Key Comparison / Evidence Against The Claim |
|---|---|---|
| **H1 Boundary-conditioned Leverage** | Holding target dependence, node centrality, and controller resource endowments broadly constant, comparable attempts to alter admissibility will produce larger independently measured reductions in the target's feasible option set, or a higher probability of specified target concession, when the initiating actor possesses the authorization, exclusion, enforcement, and discretionary rights necessary to implement the change. The expected mechanism is that relevant control rights increase the likelihood and scope of an implemented admissibility change, which in turn alters the target's available options. | Measure leverage independently from control rights and from the attempted intervention itself, using outcomes such as concession probability, policy reversal, or change in feasible options. The key comparison is between otherwise similar cases involving comparable attempts to alter admissibility but different configurations of implementation-relevant rights. H1 is weakened if stronger control-right configurations do not produce larger implemented admissibility changes or, conditional on such changes, do not produce larger independently measured effects on the target's option set. |
| **H2 Enforced Selective Access** | For a binding access-rule change that is applicable and implemented, affected actor-function pairs will experience a larger decline in independently measured admissible capacity, service availability, or another pre-specified measure of effective usability than comparable unaffected pairs while underlying physical capacity and topology remain substantially unchanged. | Do not define the outcome from the rule itself. Verify implementation and compare with similar unaffected users/items/uses. No differential availability decline despite verified implementation, or an equal decline driven by physical/demand shocks, weakens H2. |
| **H3 Concentration of Implementation Rights** | Holding nominal rule scope, targeted flow, and physical interface count broadly constant, greater concentration of authorization and enforcement rights increases the share of targeted transactions actually brought under the restriction and reduces implementation variance across interfaces. | Measure control-right concentration separately from flow/interface concentration. If dispersed control achieves equal or more complete implementation, or concentration does not predict realized coverage, H3 is weakened. |
| **H4 Conditional Rewiring** | After an enforced access reduction, affected actor-function pairs with persistent demand and technically, institutionally, and capacity-wise feasible substitutes will reroute or substitute sooner or more extensively than comparable pairs without the access reduction; the increment should weaken as switching cost or capacity constraints rise. | Other causes of rerouting are not falsifiers. The test is the incremental difference relative to a counterfactual or comparison group. Little added rerouting under persistent demand and genuinely feasible substitutes weakens H4. |

**Note:** Definitions and typological claims are excluded from the hypothesis count. The outcome for each hypothesis must be measured independently from the access rule, boundary state, or control-right variable used as an explanation.

**Sources:** Author's hypotheses derived from the NBNS mechanism and the near-neighbor literatures reviewed in Section 2.

### 6.2 Operationalization and Coding Sequence

The recommended unit of analysis is a boundary event or boundary condition defined over an actor-user-function-direction-time tuple. Researchers should specify: (1) the controller; (2) the affected actor or class; (3) the node or relation; (4) the function; (5) the preexisting boundary state; (6) the rule criteria; (7) the implementation interface; (8) the relevant control rights; (9) the observed action; (10) the change in admissible capacity or effective usability; (11) target response; and (12) network/system outcome. This sequence makes it possible for the same physical object to appear in multiple roles without duplicating a variable.

Boundary state should be measured from independent evidence whenever possible. Legal text can establish a formal license requirement, but not whether enforcement is effective. Technical architecture can establish that authentication exists, but not whether a regulator can lawfully modify the rule. Transaction data can reveal reduced flow, but not by itself whether demand or access changed. Triangulation across policy documents, contracts, technical records, operational logs, and observed flow data is therefore central to the research design.

**Table 7** translates the framework into illustrative measures. The indicators are not universal scales: they are candidate observations that must be matched to the actor-function-time unit defined for each study.

**Table 7. Illustrative Operational Measures**

| Construct | Possible Indicators | Evidence |
|---|---|---|
| **Structural Position** | Degree/eigenvector/betweenness centrality; brokerage; flow share; dependence ratio | Network maps, trade/service flows, platform relations |
| **Rule Condition** | Eligibility criteria; license requirement; item/end-use restrictions; membership or certification requirements; contractual or policy conditions. | Laws, regulations, licenses, contracts, policies, standards, governance documents. |
| **Boundary State** | Actor-function-direction-time-specific admissibility state (open, filtered, restricted, or denied), coded from authorization and implementation evidence; transaction-level approval/denial status; access or authorization logs; ratio-scaled admissible-capacity share $\beta^K$ when directly measurable. | Authorization and licensing decisions, access logs, contracts, configuration records, and transaction-level implementation evidence. |
| **Control Rights** | Authorization, veto, exclusion, rule-setting, enforcement, adjudication shares | Law, governance documents, contracts, administrator privileges |
| **Admissible Capacity** | Maximum legally and operationally admissible service, supply, or throughput for the specified actor-function pair and observation period; observed authorized flow and observed total flow are coded separately. | Baseline capacity data combined with authorization and implementation evidence applicable to the specified actor-function-time unit; where available, transaction-, quota-, throughput-, or service-level records that permit the admissible share to be estimated or bounded. |
| **Substitutability** | Alternative capacity; switching time; interoperability; political/legal feasibility | Supplier/network data, scenario analysis, contracts, capacity utilization |

**Table 7. Illustrative Operational Measures (Cont.)**

| Construct | Possible Indicators | Evidence |
|---|---|---|
| **Target Adaptation** | Rerouting; supplier switching; investment; stockpiling; redesign; retaliation | Longitudinal transactions, investment, procurement, policy changes |
| **System Outcome** | Persistent topology change; new interfaces/rules; fragmentation/integration; output loss/recovery | Temporal multiplex networks, process tracing, system performance data |
| **Strategic Distance** | Minimum task cost/latency/risk over feasible paths | Routing, logistics, permissions, insurance, legal/operational risk data |

**Note:** Indicators are illustrative rather than universal. Measures should be selected before outcome analysis where possible, and boundary state should be distinguished from formal rule language, implementation evidence, and observed flow.

**Sources:** Author's operationalization drawing on Bonacich (1987), Hafner-Burton et al. (2009), Kivelä et al. (2014), Hu et al. (2019), Schlager and Ostrom (1992), Buldyrev et al. (2010), Holland (1992), and Meadows (2008).

### 6.3 Research Designs and Incremental Explanatory Value

Comparative case studies can pair similarly central nodes or interfaces that differ in control rights, joint-veto arrangements, or rule discretion. Event studies can examine policy or protocol changes that alter admissibility while leaving much of the underlying physical network unchanged. Difference-in-differences or matched comparisons may be possible where a rule affects one class of user, item, end use, or jurisdiction but not a similar comparison group. Researchers should measure substitutability and dependence before the event to reduce post-treatment bias.

Process tracing is especially useful when the outcome could also be produced by demand shocks, conflict, price changes, strategic anticipation, or other policies. It can identify the authorization decision, how implementers translated it into access conditions, whether targets recognized the constraint, what alternatives they considered, and why observed adaptation or concession followed. Other credible identification strategies remain possible. Where causal controls are unavailable, the study should claim process support rather than causal identification.

Longitudinal multilayer-network analysis can test whether access events precede changes in flow and topology across networks. Simulation can vary control-right concentration, substitutability, buffering, and coupling under explicit assumptions. Predictive or explanatory tests should compare three levels where data permit: (A) topology and resources; (B) topology/resources plus dependence, jurisdiction, institutional capacity, and cross-network position; and (C) the same baseline plus indexed boundary state, implementation interface, and control-right variables. Improved prediction alone does not prove the proposed mechanism, but failure of Layer C to improve discrimination over a well-specified Layer B would weaken the claim of independent theoretical value.

The strongest test of NBNS is incremental relative to the closest existing explanation, not merely to a topology-only model. If actor-function-specific admissibility, implementation-interface evidence, and control-right configurations add little information after dependence, jurisdiction, institutional capacity, resources, and cross-network position are measured, the framework may still be useful as a transferable coding scheme but should not be claimed as an independent theory of power. A useful null expectation is therefore that Layer C variables do not systematically improve discrimination among actor-function cases that Layer B predicts similarly. Rejection of that null still requires mechanism evidence to show that the added variables are not proxies for preexisting power.

### 7. Scope Conditions and Limitations

First, NBNS applies most directly where access conditions are consequential, selective, and at least partly controllable. The mere existence of an analytical system boundary does not imply that a real actor can manipulate it. A boundary that is uncontrollable, non-scarce, or irrelevant to the target function is not automatically a source of power. The framework should not infer leverage from 'systems must have boundaries.'

Second, boundary categories such as physical, legal, digital, institutional, economic, or cognitive describe domains of manifestation rather than a single natural kind. Their mechanisms and measures can differ sharply. A legal prohibition does not make an action physically impossible; an epistemic limit does not imply a regulatory restriction; and a physical bottleneck need not be alterable by rule. Cross-domain comparison is appropriate only after the relevant admissibility relation has been specified.

### Conclusion

Network theory already provides powerful accounts of relational position, dependence, multilayer structure, temporal connectivity, and interdependent failure. Research on weaponized interdependence and cross-network weaponization already shows that jurisdiction, institutions, and position across linked networks can become sources of coercive power. The contribution of NBNS must therefore be narrower and more precise than the claim that existing theories lack boundaries.

The framework centers on conditional usability. A relation can exist physically or technically while its admissibility varies by actor, function, direction, and time. Rules define admissibility criteria; interfaces implement crossing; control-rights bundles identify who can alter or enforce those conditions. Structural position and dependence create potential exposure, while control rights and discretion condition whether that exposure is convertible into available leverage. Boundary action is the mechanism of exercise. Admissible-capacity change is an intermediate outcome. Target response, network adaptation, and durable system transformation occur later and only under additional conditions. Systemic power is reserved for attributable, purposeful capacity to produce durable changes in rules, interoperability, architecture, or functional reproduction across networks; large unintended effects alone do not meet that criterion.

This decomposition clarifies several puzzles. Denial need not involve destruction. Denial of one function need not imply exclusion from the entire network. Rerouting is a response to an access change rather than another boundary state. Transfer is not equivalent to exit, and system recomposition can reproduce a lost function across multiple alternatives. A decentralized topology can coexist with concentrated control of authentication, protocol, licensing, standards, or market access. Strategic distance can rebound when a boundary change removes low-cost paths from the feasible set even though geographic distance remains unchanged.

The resulting research program is intentionally testable against both simple and near-neighbor explanations. If indexed admissibility, implementation-interface evidence, and control-right variables do not improve discrimination beyond models that already include dependence, jurisdiction, institutional capacity, resources, and cross-network position, NBNS should be narrowed to a descriptive coding framework. If they do improve discrimination and process evidence shows that controllers deliberately altered admissibility, the framework provides a way to connect structural position to selective access, purposeful action, adaptation, and system change without collapsing those stages into a single concept of power. The central question for research on complex interdependence is therefore not only who occupies consequential positions, but which relations are actually usable, by whom, for what purpose, under whose authority, through what implementation process, and with what consequences when those conditions change.

**Research and Source Statement**

This article is a conceptual and theoretical study. It reports no newly collected participant-, firm-, or country-level dataset and does not present a validated quantitative NBNS index. The semiconductor section is an illustrative coding walkthrough built from public regulatory documents, corporate filings, and existing research; its product-time trace is not a causal estimate of the overall effectiveness of export controls. The author's earlier AI-power publications are treated as conceptual antecedents rather than independent validation. External source verification for this revision was conducted through August 30, 2026.

## References

Allen, G. C. (2024, November 26). *The true impact of allied export controls on the U.S. and Chinese semiconductor manufacturing equipment industries.* Center for Strategic and International Studies. https://www.csis.org/analysis/true-impact-allied-export-controls-us-and-chinese-semiconductor-manufacturing-equipment

Beaumier, G., & Cartwright, M. (2024). Cross-network weaponization in the semiconductor supply chain. *International Studies Quarterly, 68*(1), sqae003. https://doi.org/10.1093/isq/sqae003

Bonacich, P. (1987). Power and centrality: A family of measures. *American Journal of Sociology, 92*(5), 1170-1182. https://doi.org/10.1086/228631

Brockmann, D., & Helbing, D. (2013). The hidden geometry of complex, network-driven contagion phenomena. *Science, 342*(6164), 1337-1342. https://doi.org/10.1126/science.1245200

Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E., & Havlin, S. (2010). Catastrophic cascade of failures in interdependent networks. *Nature, 464*, 1025-1028. https://doi.org/10.1038/nature08932

Bureau of Industry and Security. (2022, October 7). *Commerce implements new export controls on advanced computing and semiconductor manufacturing items to the People's Republic of China (PRC).* U.S. Department of Commerce. https://www.bis.gov/node/20292

Bureau of Industry and Security. (2023, October 17). *Commerce strengthens restrictions on advanced computing semiconductors, semiconductor manufacturing equipment, and supercomputing items to countries of concern.* U.S. Department of Commerce. https://www.bis.gov/press-release/commerce-strengthens-restrictions-advanced-computing-semiconductors-semiconductor-manufacturing-equipment

Burt, R. S. (1992). *Structural holes: The social structure of competition.* Harvard University Press. https://www.hup.harvard.edu/books/9780674843714

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

Galloway, A. R. (2004). *Protocol: How control exists after decentralization.* MIT Press. https://mitpress.mit.edu/9780262072472/protocol/

Goujon, R., Piper, L. D., Kleinhans, J.-P., & Kratz, A. (2022, October 21). *Freeze-in-place: The impact of US tech controls on China.* Rhodium Group. https://rhg.com/research/freeze-in-place/

Granovetter, M. S. (1973). The strength of weak ties. *American Journal of Sociology, 78*(6), 1360-1380. https://doi.org/10.1086/225469

Grewal, D. S. (2008). *Network power: The social dynamics of globalization.* Yale University Press. https://yalebooks.yale.edu/book/9780300151343/network-power/

Hafner-Burton, E. M., Kahler, M., & Montgomery, A. H. (2009). Network analysis for international relations. *International Organization, 63*(3), 559-592. https://doi.org/10.1017/S0020818309090195

Holland, J. H. (1992). Complex adaptive systems. *Daedalus, 121*(1), 17-30. https://www.jstor.org/stable/20025416

Holme, P., & Saramäki, J. (2012). Temporal networks. *Physics Reports, 519*(3), 97-125. https://doi.org/10.1016/j.physrep.2012.03.001

Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2019). *Guide to attribute based access control (ABAC) definition and considerations (NIST Special Publication 800-162, Update 2).* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-162

Keohane, R. O., & Nye, J. S. (2012). *Power and interdependence (4th ed.).* Longman. https://www.pearson.com/en-us/subject-catalog/p/power-and-interdependence/P200000002485

Kivelä, M., Arenas, A., Barthelemy, M., Gleeson, J. P., Moreno, Y., & Porter, M. A. (2014). Multilayer networks. *Journal of Complex Networks, 2*(3), 203-271. https://doi.org/10.1093/comnet/cnu016

Working Paper

Kleinhans, J.-P., Goujon, R., Hess, J., & Piper, L. D. (2023, April 4). *Running on ice: China's chipmakers in a post-October 7 world.* Rhodium Group. https://rhg.com/research/running-on-ice/

Lamont, M., & Molnár, V. (2002). The study of boundaries in the social sciences. *Annual Review of Sociology, 28*, 167-195. https://doi.org/10.1146/annurev.soc.28.110601.141107

Meadows, D. H. (2008). *Thinking in systems: A primer (D. Wright, Ed.).* Chelsea Green Publishing. https://www.chelseagreen.com/product/thinking-in-systems/

NVIDIA Corporation. (2022a, September 1). *Current report (Form 8-K).* U.S. Securities and Exchange Commission. https://www.sec.gov/Archives/edgar/data/1045810/000104581022000151/nvda-20220831.htm

NVIDIA Corporation. (2022b). *Quarterly report (Form 10-Q) for the quarter ended July 31, 2022.* U.S. Securities and Exchange Commission. https://www.sec.gov/Archives/edgar/data/1045810/000104581022000147/nvda-20220731.htm

NVIDIA Corporation. (2024). *Annual report (Form 10-K) for the fiscal year ended January 28, 2024.* U.S. Securities and Exchange Commission. https://www.sec.gov/Archives/edgar/data/1045810/000104581024000029/nvda-20240128.htm

Schlager, E., & Ostrom, E. (1992). Property-rights regimes and natural resources: A conceptual analysis. *Land Economics, 68*(3), 249-262. https://doi.org/10.2307/3146375

Wu, S. (2026a). *AI capability stratification: A framework for the future distribution of AI power (Policy Brief No. EPINOVA-2026-PB-59).* Global AI Governance and Policy Research Center, EPINOVA LLC. https://doi.org/10.67037/epinova.pb.2026.059

Wu, S. (2026b). *Beyond model capability: A system-level framework for AI power (Policy Brief No. EPINOVA-2026-PB-58).* Global AI Governance and Policy Research Center, EPINOVA LLC. https://doi.org/10.67037/epinova.pb.2026.058

Wu, S. (2026c). *Global AI power mapping: Domains, alliances, and rule spaces (Policy Brief No. EPINOVA-2026-PB-60).* Global AI Governance and Policy Research Center, EPINOVA LLC. https://doi.org/10.67037/epinova.pb.2026.060