Energy–Information Sovereignty: A Formal Theory of Planetary Infrastructure Control

Douglas C. Youvan

doug@youvan.com www.youvan.ai

Abstract

Modern civilization depends upon two coupled substrates: energy, which permits physical action, and information, which permits coordination, authorization, memory, prediction, and control. This paper develops a formal vocabulary for analyzing the hypothetical concentration of both substrates within a single governing entity. Such an entity need not directly own every power plant, communication channel, computer, or financial institution. Effective sovereignty arises when one coordinating system controls access, authentication, allocation, and restoration across sufficiently many interdependent networks. We define energetic control, informational control, coordination dominance, infrastructural dependence, emergency delegation, and irreversible centralization. A simple power functional, $P = E \times I$, represents the multiplicative relationship between control of physical capacity and control of social coordination. Neither energy nor information alone produces complete infrastructural sovereignty; their coupling creates a qualitatively stronger regime. The most plausible path to such concentration is not military conquest but crisis-driven delegation to a state–corporate platform capable of restoring failed systems. Temporary emergency authority may then become permanent through technical dependence, interoperability requirements, and the disappearance of viable alternatives. The resulting system would possess extraordinary administrative power while simultaneously creating a single point of civilizational failure.

Keywords

energy sovereignty, information sovereignty, infrastructure control, platform power, emergency governance, network dependence, digital identity, artificial intelligence, systemic fragility, planetary coordination.

Google Drive: https://drive.google.com/drive/folders/15Kd8bUjm7zVaKdVIwbPhqjjV68aUZQvc

https://orcid.org/0009-0004-4206-4253

1. Introduction

Political sovereignty has traditionally been associated with territory, law, taxation, military force, and institutional legitimacy. In a technologically integrated civilization, however, practical sovereignty increasingly depends upon control of the infrastructures through which action becomes possible.

A government may formally possess legal authority while remaining unable to operate without electricity, telecommunications, cloud computation, digital identity, payment systems, transportation networks, and machine-mediated coordination. Conversely, an organization lacking conventional territorial sovereignty may acquire substantial governing power by controlling these enabling systems.

The relevant distinction is therefore:

formal sovereignty ≠ operational sovereignty.

Formal sovereignty is the recognized right to govern.

Operational sovereignty is the practical capacity to determine which agents, institutions, and processes may continue functioning.

The hypothetical entity considered here possesses coordinated control over two foundational domains:

E = control of usable energy,

I = control of usable information.

Energy permits machines, transport, production, heating, cooling, computation, and biological support systems to operate.

Information permits agents to identify one another, issue commands, authenticate transactions, allocate resources, preserve records, predict events, and coordinate collective action.

The conjunction of these powers produces a form of infrastructural sovereignty.

Definition 1.1. Energy–information sovereignty

Energy–information sovereignty is the capacity of an entity to regulate both the physical ability of a system to act and the informational ability of that system to coordinate action.

A system possessing only E may disable activity but cannot fully direct it.

A system possessing only I may influence coordination but cannot guarantee material compliance.

A system possessing both E and I can regulate action, knowledge, communication, access, and recovery simultaneously.

Thus, the simplest governing relation is:

$P = E \times I$,

where P denotes effective infrastructural power.

The multiplicative form is essential. If either $E = 0$ or $I = 0$, then total infrastructural power collapses:

$E \times 0 = 0$,

$0 \times I = 0$.

Control of energy without information is blind force.

Control of information without energy is disembodied instruction.

Their coupling produces executable authority.

2. Foundational Definitions

Definition 2.1. Energetic control

Energetic control is the ability to determine the availability, quantity, timing, location, or permitted use of energy within a dependent system.

Energetic control includes authority over:

generation,

storage,

transmission,

distribution,

fuel access,

load prioritization,

and restoration.

Direct ownership is not required. An entity possesses effective energetic control whenever other actors cannot reliably obtain or allocate energy without passing through its decisions.

Definition 2.2. Informational control

Informational control is the ability to determine what information may be transmitted, retrieved, authenticated, amplified, stored, modified, or recognized as authoritative.

Informational control includes authority over:

communication,

identity,

search,

computation,

archives,

payments,

software permissions,

and machine-readable legitimacy.

Informational control is not equivalent to censorship alone. A controller may govern information without deleting it. It may instead determine whether information is visible, trusted, searchable, interoperable, or actionable.

Definition 2.3. Coordination layer

A coordination layer is the set of protocols, institutions, software systems, and authorization mechanisms through which otherwise separate infrastructures act as a unified system.

The coordination layer maps:

resources → permissions,

identities → roles,

demands → priorities,

signals → actions,

failures → restoration procedures.

An entity that controls the coordination layer may govern infrastructures it does not physically own.

Definition 2.4. Access sovereignty

Access sovereignty is the power to determine whether an agent may participate in a critical system.

Access sovereignty may be exercised through:

digital credentials,

network permissions,

energy quotas,

financial authorization,

device certification,

geographic restrictions,

or behavioral conditions.

The critical political unit is no longer merely the citizen. It becomes the authenticated participant.

Definition 2.5. Dependency sovereignty

Dependency sovereignty exists when an institution remains nominally independent but cannot function without continuous access to systems controlled by another entity.

Let A depend upon entity C for a set of critical services S.

Then:

$A \to S \to C$.

If the removal of C causes A to cease functioning, then C possesses effective authority over A, even when no formal transfer of sovereignty has occurred.

Proposition 2.1. Ownership is not necessary for control

An entity may acquire effective sovereignty over an infrastructure without owning its physical components.

Proof.

Suppose multiple institutions own generators, cables, servers, communication towers, and financial systems. Suppose, however, that all owners require a common authentication system, cloud platform, scheduling algorithm, payment network, and restoration protocol controlled by entity C.

If C can deny authorization, computation, settlement, or coordination, then the independently owned components cannot operate as a coherent system.

Therefore, physical ownership is insufficient to guarantee autonomy.

Hence, control of the coordination layer may dominate ownership of the underlying assets. ■

3. The Coupled Infrastructure Model

Let civilization be represented by a directed dependency graph:

$G = (V, R)$,

where V is the set of critical systems and R is the set of dependency relations.

Representative vertices include:

electricity,

fuel,

water,

food,

transport,

communications,

cloud computation,

identity,

finance,

healthcare,

government,

and defense.

A directed relation:

$v_i \rightarrow v_j$

means that system v_i requires system v_j for continued operation.

Modern infrastructures form cycles rather than simple hierarchies.

For example:

electricity → communications,

communications → electricity,

electricity → cloud computation,

cloud computation → electricity,

finance → communications,

communications → finance.

These reciprocal dependencies produce tightly coupled operational loops.

Definition 3.1. Infrastructural closure

A set of systems $C \subseteq V$ is infrastructurally closed when the continued operation of each major element of C depends primarily upon other elements inside C.

An entity controlling an infrastructurally closed set can maintain internal operation while excluding external participants.

Definition 3.2. Control cut

A control cut is a minimal set of nodes or relations whose capture allows an entity to govern a much larger dependency network.

Examples include:

identity systems,

grid-balancing systems,

cloud orchestration,

financial settlement,

telecommunications routing,

and emergency restoration authority.

A controller need not seize every node in G. It need only control a sufficiently powerful cut set K.

If removing K fragments the operational graph, then K is a strategic control surface.

Proposition 3.1. Coordination dominance

Let K be a control cut in G. If entity C exclusively governs K, then C may exercise system-wide influence disproportionate to the physical size of K.

Proof.

Every operational path connecting major subsystems passes through at least one element of K.

Entity C may therefore permit, delay, condition, or terminate those paths.

Because the function of the larger network depends upon the continued availability of K, control of K propagates through the dependency graph.

Thus, local control at K produces global operational consequences. ■

Definition 3.3. Energy–information coupling

Energy–information coupling occurs when the allocation of energy depends upon informational authorization and the production of information depends upon energy allocation.

The coupled loop is:

energy → computation → information → authorization → energy.

Once this loop is closed under one authority, the controller can decide both:

who receives the capacity to act,

and who receives the authority to act.

Theorem 3.1. Coupled sovereignty theorem

If one entity possesses exclusive control over both the principal energy-allocation mechanism and the principal information-authorization mechanism of a dependent society, then that entity possesses operational sovereignty over every institution lacking an independent alternative.

Proof.

Let institution A require energy e to perform physical operations and authorization i to participate in informational, financial, or administrative systems.

Suppose controller C can independently deny either e or i.

If C denies e, A cannot execute physical processes.

If C denies i, A cannot authenticate, transact, communicate, or coordinate.

Therefore, A remains functional only while C permits both e and i.

Since continued institutional existence is conditional upon C, A is operationally subordinate to C.

This holds for every institution lacking independent energy and information channels.

Therefore, C possesses operational sovereignty over the dependent society. ■

The theorem does not require ideological obedience, legal annexation, or military occupation. Dependence alone is sufficient.

The decisive political relation becomes:

continued participation ↔ continued authorization.

4. The Crisis-Acquisition Pathway

The most plausible transition to energy–information sovereignty is not direct conquest.

It is emergency delegation.

A sufficiently severe crisis may cause governments, utilities, telecommunications firms, financial institutions, and cloud providers to surrender operational discretion to a single coordinating authority.

Let:

C_0 = ordinary decentralized coordination,

X = compound systemic crisis,

D = emergency delegation,

C_1 = centralized coordination.

Then:

$C_0 + X \rightarrow D \rightarrow C_1$.

The transition is initially justified by necessity rather than ideology.

Definition 4.1. Compound systemic crisis

A compound systemic crisis is a disturbance affecting multiple mutually dependent infrastructures simultaneously.

Representative components include:

large-scale cyberattack,

electrical-grid instability,

military conflict,

fuel disruption,

communications failure,

financial panic,

extreme weather,

pandemic,

or satellite-system degradation.

A compound crisis is more dangerous than the sum of its components because failures propagate through dependency loops.

If:

electricity → communications,

communications → finance,

finance → fuel distribution,

fuel distribution → electricity,

then failure at one node may return to amplify the original disturbance.

Definition 4.2. Cascading dependency failure

A cascading dependency failure occurs when disruption at one node produces failures at dependent nodes, which then return additional disruption to the initiating system.

Let F_0 denote the initial failure.

Then:

$F_0 \to F_1 \to F_2 \to \cdots \to F_n$,

with some $F_n \to F_0$.

The return relation converts a linear disturbance into a self-amplifying loop.

Definition 4.3. Emergency coordinator

An emergency coordinator is an entity temporarily granted authority to allocate resources, restore services, authenticate participants, and prioritize critical functions during systemic disruption.

Its authority may include:

electric-load prioritization,

network routing,

cloud-resource allocation,

identity verification,

payment continuity,

fuel distribution,

public messaging,

cybersecurity filtering,

and logistics coordination.

Proposition 4.1. Crisis favors integrated coordinators

During a compound systemic crisis, institutions capable of coordinating multiple infrastructure layers possess an advantage over institutions controlling only one layer.

Proof.

A single-layer institution may restore its own subsystem while remaining dependent upon failures elsewhere.

A power utility may restore electricity but remain unable to communicate.

A telecommunications provider may restore signals but lack energy.

A bank may maintain records but lack network access.

An integrated coordinator can jointly optimize several dependent systems.

Therefore, under crisis conditions, decision authority tends to migrate toward the actor with the broadest cross-system visibility and execution capacity. ■

Definition 4.4. Restoration legitimacy

Restoration legitimacy is political authority acquired through the demonstrated ability to restore failed systems.

Traditional legitimacy may arise from election, law, inheritance, or consent.

Restoration legitimacy arises from the proposition:

the system functions because the coordinator functions.

This legitimacy is operational before it is constitutional.

A population experiencing blackout, communication loss, payment failure, or supply disruption may accept powers it would reject under ordinary conditions.

Proposition 4.2. Restoration precedes submission

A population need not be ideologically persuaded before becoming operationally dependent.

Proof.

Suppose entity C restores electricity, identity services, payments, communications, and food logistics.

Individuals and institutions must enter C's system to regain ordinary function.

Participation therefore begins as practical necessity.

Ideological acceptance may follow, remain incomplete, or never occur.

Operational dependence is established regardless.

Hence, restoration can precede and partially replace political submission. ■

5. Emergency Delegation

Emergency delegation converts technical capacity into temporary governing authority.

Let A denote the set of authorities held before crisis.

Let ΔA denote the additional powers granted during crisis.

Then:

$A_1 = A_0 \cup \Delta A$.

The central danger is not the initial grant.

It is the persistence of ΔA after the crisis.

Definition 5.1. Temporary exceptional authority

Temporary exceptional authority is power granted under the claim that ordinary procedures are too slow, fragmented, or vulnerable for emergency conditions.

Such authority is usually justified by four assertions:

the threat is immediate,

coordination must be unified,

delay will increase harm,

and normal authority will later be restored.

Definition 5.2. Delegation ratchet

A delegation ratchet is a process in which emergency powers are easier to grant than to withdraw.

Let:

g = cost of granting authority,

w = cost of withdrawing authority after dependence forms.

A delegation ratchet exists when:

$w > g$.

Withdrawal becomes costly because institutions reorganize around the emergency system.

Databases are migrated.

Staff are retrained.

Legacy systems are abandoned.

Contracts are rewritten.

Identity protocols are standardized.

Independent capabilities decay.

The emergency architecture becomes the ordinary architecture.

Proposition 5.1. Dependency raises the cost of reversal

The longer emergency coordination remains in place, the more difficult decentralization becomes.

Proof.

Let $d(t)$ denote institutional dependence after duration t.

Assume that independent systems are gradually retired while integration increases.

Then:

$d(t + 1) \geq d(t)$.

Let $r(t)$ denote the cost of restoring independent operation.

As dependence rises, reconstruction requires additional hardware, software, personnel, legal authority, and organizational memory.

Therefore:

$r(t + 1) \geq r(t)$.

Hence, prolonged emergency coordination increases the cost of reversal. ■

Definition 5.3. Infrastructural lock-in

Infrastructural lock-in is the condition in which departure from a dominant system remains legally possible but operationally prohibitive.

A state may formally retain sovereignty while lacking:

independent cloud capacity,

independent communications,

independent identity systems,

independent energy balancing,

independent financial settlement,

or personnel capable of operating former systems.

The legal right to exit then becomes materially empty.

Corollary 5.1. Nominal sovereignty may survive operational surrender

A government may preserve its constitution, legislature, courts, and symbols while surrendering effective control over the systems required to exercise their decisions.

Thus:

legal sovereignty ≠ executable sovereignty.

Definition 5.4. Emergency normalization

Emergency normalization is the conversion of exceptional procedures into routine governance.

The progression is:

temporary measure,

renewed measure,

standard protocol,

mandatory infrastructure,

constitutional fact.

At the final stage, the emergency origin may be forgotten.

The system is defended not because the crisis continues, but because society can no longer function without it.

6. State–Corporate Fusion

No existing corporation is likely to obtain planetary energy–information sovereignty acting alone.

No existing state is likely to obtain it without corporate infrastructure.

The most plausible controller is therefore hybrid.

Definition 6.1. State–corporate infrastructure complex

A state–corporate infrastructure complex is a governing formation in which public authority and private technical capacity become operationally inseparable.

The state contributes:

law,

coercion,

taxation,

emergency authority,

military protection,

intelligence,

and diplomatic recognition.

The corporate sector contributes:

cloud infrastructure,

artificial intelligence,

telecommunications,

cybersecurity,

data centers,

identity platforms,

payment systems,

and specialized personnel.

The combined system possesses capacities unavailable to either component separately.

Let:

S = state authority,

K = corporate technical capacity.

Then:

$H = S \otimes K$,

where H denotes the hybrid sovereign complex.

The symbol $\otimes$ indicates functional coupling rather than ordinary addition.

Definition 6.2. Delegated coercion

Delegated coercion occurs when private systems enforce public rules through access control.

Examples include:

account suspension,

credential revocation,

payment denial,

network exclusion,

energy restriction,

software deactivation,

or automated movement constraints.

The state may establish the rule.

The platform executes it.

The distinction between public command and private implementation becomes increasingly difficult to observe.

Definition 6.3. Privatized sovereignty

Privatized sovereignty is the exercise of governing power by an organization that remains legally classified as a private entity.

Such an organization may determine:

who can communicate,

who can transact,

which software can run,

which identities are valid,

which institutions receive computation,

and which regions receive prioritized energy.

The governing effect may exceed that of many states even when the organization possesses no formal territory.

Definition 6.4. Sovereign platform

A sovereign platform is an infrastructure system whose continued operation is required for the functioning of governments, markets, and civil society, and whose internal decisions cannot be effectively overruled without causing systemic disruption.

A platform becomes sovereign when regulation is theoretically possible but practically self-defeating.

Proposition 6.1. Mutual dependence does not imply equal power

A state and a dominant platform may depend upon one another while remaining unequal.

Proof.

Suppose the state depends upon platform P for critical computation, identity, and communications.

Suppose P depends upon the state for legal recognition and physical protection.

The dependencies are reciprocal.

However, if replacing P requires years while P can disable state operations immediately, then their temporal powers differ.

Let:

τ_s = time required for the state to replace P,

τ_p = time required for P to disrupt the state.

If:

$\tau_p \ll \tau_s$,

then P possesses a decisive short-term advantage.

Reciprocal dependence therefore does not imply symmetrical control. ■

Definition 6.5. Temporal sovereignty

Temporal sovereignty is the advantage possessed by the actor capable of producing consequences faster than opposing institutions can respond or replace it.

In highly integrated systems, speed may dominate law.

A court may later declare an action unlawful.

A legislature may later impose restrictions.

A regulator may later order separation.

But if the platform can alter access instantly, its operational decision precedes institutional correction.

Thus:

decision time < correction time.

When this inequality becomes extreme, formal oversight loses practical force.

7. The Transition to Permanent Sovereignty

The transition from emergency coordinator to permanent sovereign requires no formal declaration.

It requires only that alternatives disappear.

Let:

A(t) = number of viable independent alternatives at time t,

D(t) = dependence upon the central coordinator at time t.

The centralizing tendency is:

$A(t) \downarrow$ while $D(t) \uparrow$.

A critical threshold is reached when:

$A(t) = 0$.

At this point, exit is no longer a policy choice.

It is a reconstruction project.

Definition 7.1. Irreversible centralization

Irreversible centralization is the condition in which restoration of decentralized authority requires greater resources, time, and coordination than dependent institutions can independently obtain.

Irreversibility need not be absolute.

It need only exceed the practical planning horizon of governments and populations.

Definition 7.2. Sovereignty threshold

The sovereignty threshold is crossed when the central coordinator can impose conditions upon major institutions without facing a credible threat of replacement.

Before the threshold:

the coordinator serves the system.

After the threshold:

the system serves through the coordinator.

Theorem 7.1. Dependency-conversion theorem

An emergency coordinator becomes an operational sovereign when three conditions are jointly satisfied:

1. critical institutions depend upon its services;
2. no viable substitute can be activated within the tolerated interruption period;
3. the coordinator can condition continued service upon compliance.

Proof.

Let institution A require service s from coordinator C.

By condition 1, withdrawal of s disrupts A.

By condition 2, A cannot replace s before unacceptable failure occurs.

By condition 3, C may require compliance q as the price of continued access.

Therefore:

A functions only if A satisfies q.

Since C can determine q and A cannot credibly refuse, C possesses governing authority over A.

If the same relation holds across major institutions, C possesses operational sovereignty over the system. ■

Corollary 7.1. Sovereignty may emerge without constitutional transfer

No treaty, election, annexation, or declaration is required.

Sovereignty emerges from enforceable dependence.

The transition may therefore remain legally ambiguous even after it becomes operationally complete.

The most plausible final formula is:

crisis + coordination + dependency + no exit = infrastructural sovereignty.

8. Mechanisms of Infrastructural Rule

Energy–information sovereignty need not operate primarily through visible repression.

Its characteristic instrument is conditional access.

The controller governs by determining whether a person, institution, device, or region may remain connected to the systems required for ordinary life.

Definition 8.1. Conditional participation

Conditional participation is the rule:

access is granted if and only if specified conditions are satisfied.

Let agent a request access to system s.

Let Q(a) denote the set of compliance conditions imposed upon a.

Then:

access(a, s) = 1 if Q(a) is satisfied,

access(a, s) = 0 otherwise.

The conditions may concern:

identity,

payment,

location,

legal status,

security classification,

behavior,

institutional affiliation,

software compliance,

or political authorization.

The power of the controller lies not merely in refusing access, but in defining Q.

Definition 8.2. Programmable permission

Programmable permission is authorization determined automatically by machine-readable rules.

A programmable system may grant or deny:

electricity,

bandwidth,

computation,

financial settlement,

physical entry,

transport access,

medical services,

or administrative recognition.

The governing rule becomes executable code.

Thus:

law → rule set → automated decision → material consequence.

Proposition 8.1. Automated enforcement compresses political time

When permissions are machine-executable, the interval between rule creation and social consequence approaches zero.

Proof.

Under conventional administration, enforcement requires interpretation, communication, personnel, and local implementation.

Under programmable permission, a rule may be distributed directly to connected systems.

Let:

τ_m = manual enforcement time,

τ_a = automated enforcement time.

Typically:

$\tau_a \ll \tau_m$.

Therefore, automated enforcement compresses political time and reduces opportunities for deliberation, appeal, and local resistance. ■

Definition 8.3. Identity gate

An identity gate is a system that conditions access upon recognition by a central identity authority.

The identity gate may bind:

person,

device,

account,

organization,

location,

and transaction.

A society organized through identity gates does not merely ask:

Who are you?

It asks:

Are you recognized now?

Identity becomes continuously revocable.

Definition 8.4. Revocable personhood

Revocable personhood is the condition in which practical participation in society depends upon the continued validity of centrally managed credentials.

Legal existence may remain intact while operational existence is suspended.

An individual may remain biologically present and formally protected while becoming unable to:

communicate,

travel,

purchase,

work,

authenticate,

or access services.

Thus:

formal personhood ≠ operational personhood.

Definition 8.5. Algorithmic rationing

Algorithmic rationing is the automated allocation of scarce energy, information, computation, or material resources according to a model of priority.

Let R be a scarce resource.

Let agents be $a_1, a_2, \ldots, a_n$.

Let $p(a_i)$ denote the assigned priority of agent a_i.

Then allocation may be determined by:

$R(a_i) \propto p(a_i)$.

The critical political question becomes:

Who defines p?

An apparently technical optimization may encode a complete hierarchy of social value.

Definition 8.6. Visibility control

Visibility control is the power to determine whether information can be encountered, searched, amplified, recommended, archived, or computationally processed.

Visibility control differs from deletion.

A statement may continue to exist while becoming operationally absent.

Let content x exist in storage.

Let $V(x)$ denote its effective visibility.

Then:

$\text{existence}(x) = 1$

does not imply:

$V(x) > 0$.

A hidden archive is not equivalent to a usable public memory.

Definition 8.7. Epistemic throttling

Epistemic throttling is the selective reduction of an agent's capacity to obtain, transmit, compare, or verify information.

It may occur through:

search ranking,

bandwidth restriction,

model refusal,

archive exclusion,

credential requirements,

translation barriers,

or computational quotas.

Energetic throttling limits action.

Epistemic throttling limits understanding.

Together, they restrict both what an agent can do and what an agent can know about the restriction.

Proposition 8.2. Information control can conceal energy control

An entity controlling both informational visibility and energetic allocation can reduce public awareness of its own interventions.

Proof.

Suppose controller C reduces energy access to region r.

If C also governs the dominant communication and archival systems, it may limit reporting, searchability, comparison, and historical preservation concerning the intervention.

The affected population experiences the material consequence, while outside populations receive an incomplete representation.

Therefore, control of information can obscure the exercise of energetic control. ■

Definition 8.8. Personalized governance

Personalized governance is the application of different rules, incentives, prices, permissions, or information environments to different agents.

Traditional law is publicly stated and nominally general.

Personalized governance may be private, dynamic, and agent-specific.

For agents a and b:

$Q(a) \neq Q(b)$,

while neither agent necessarily knows the conditions imposed upon the other.

This destroys the common informational basis required for collective political judgment.

Definition 8.9. Differential reality

Differential reality is the condition in which distinct populations receive systematically different representations of the same world.

Each agent may inhabit an informational environment optimized for prediction, persuasion, stability, or compliance.

The political environment then ceases to be a shared public space.

It becomes a collection of individually rendered worlds.

9. Degrees of Energy–Information Sovereignty

Control is not binary.

An entity may possess partial, regional, sectoral, national, or planetary power.

Let:

$E \in [0, 1]$

measure the fraction of critical energy capacity under effective control.

Let:

$I \in [0, 1]$

measure the fraction of critical information capacity under effective control.

Let:

$C \in [0, 1]$

measure coordination centrality.

Let:

$A \in [0, 1]$

measure the availability of independent alternatives.

A simple sovereignty index is:

$S = E \times I \times C \times (1 - A)$.

This index is conceptual rather than empirical.

It expresses four principles:

power rises with energetic control,

power rises with informational control,

power rises with coordination centrality,

and power rises as alternatives disappear.

Definition 9.1. Sectoral sovereignty

Sectoral sovereignty is control over one critical domain without general control over society.

Examples include dominance over:

cloud computation,

telecommunications,

electricity transmission,

payments,

or digital identity.

Sectoral sovereignty becomes politically significant when other sectors depend upon it.

Definition 9.2. Regional sovereignty

Regional sovereignty is operational control over the coupled infrastructures of a geographically limited population.

The region may be:

a city,

an industrial corridor,

a military zone,

an island,

or a national territory.

Regional sovereignty is the most plausible experimental precursor to larger systems.

Definition 9.3. National infrastructural sovereignty

National infrastructural sovereignty exists when a central authority can coordinate energy, communications, identity, finance, and information throughout a state.

The national form requires:

territorial jurisdiction,

integrated infrastructure,

enforceable identity,

and limited external alternatives.

A highly centralized state is therefore structurally closer to complete energy–information sovereignty than a fragmented state.

Definition 9.4. Transnational platform sovereignty

Transnational platform sovereignty is the ability of a private or hybrid platform to govern critical functions across multiple states.

Its authority arises from interoperability rather than territory.

Users, firms, and governments may depend upon the same:

cloud,

identity layer,

software ecosystem,

payment network,

or communications architecture.

The platform's domain is not a map.

It is a dependency graph.

Definition 9.5. Planetary infrastructural sovereignty

Planetary infrastructural sovereignty exists when no major population, state, or institution can sustain advanced operation outside the controller's energy–information system.

This requires more than market dominance.

It requires the elimination or subordination of credible alternatives.

Proposition 9.1. Planetary sovereignty is harder than national sovereignty

A single entity is more likely to achieve integrated national control than integrated planetary control.

Proof.

National systems may be unified through:

law,

territorial enforcement,

common identity,

shared standards,

and centralized administration.

Planetary systems contain competing states, infrastructures, languages, militaries, currencies, and political traditions.

The number of independent alternatives is therefore larger.

Since sovereignty increases as alternatives decline, planetary sovereignty requires a much greater degree of consolidation.

Hence, national integration is structurally easier than planetary integration. ■

10. Candidate Entity Types

The hypothetical controller may take several institutional forms.

10.1. The centralized state

A centralized state may combine:

public utilities,

state telecommunications,

national identity,

financial oversight,

media regulation,

and security services.

Its advantage is integration.

Its limitation is territorial reach.

Let:

I_s = internal integration,

G_s = global reach.

A centralized state may exhibit:

I_s high,

G_s moderate or low.

It is therefore closest to energy–information sovereignty within its own territory.

10.2. The global technology corporation

A global technology corporation may control:

cloud computation,

operating systems,

communications software,

digital identity,

artificial intelligence,

cybersecurity,

and developer infrastructure.

Its advantage is transnational reach.

Its limitation is incomplete authority over energy, law, military force, and physical territory.

Let:

I_t = internal integration,

G_t = global reach.

A dominant technology platform may exhibit:

I_t moderate,

G_t high.

It approaches sovereignty through dependency rather than territorial rule.

10.3. The energy corporation

A large energy organization may control:

generation,

fuel,

transmission,

storage,

and infrastructure finance.

Its power is materially fundamental but informationally incomplete.

Without control of identity, communications, and computation, it can interrupt civilization but cannot fully administer it.

Thus:

high E + low I = coercive capacity without comprehensive coordination.

10.4. The military–intelligence complex

A military–intelligence complex may possess:

surveillance,

secure communications,

cyber capabilities,

satellite systems,

emergency command,

and coercive power.

Its limitation is dependence upon civilian infrastructure and commercial technology.

It may seize temporary authority during crisis but lack the ordinary systems required for long-term social administration.

10.5. The state–platform consortium

A state–platform consortium combines:

legal authority,

military protection,

cloud infrastructure,

energy coordination,

digital identity,

financial settlement,

telecommunications,

and artificial intelligence.

It is the most plausible institutional form of large-scale energy–information sovereignty.

Let:

S = state authority,

T = technical platform capacity,

U = utility infrastructure,

F = financial infrastructure.

Then:

$H = S \otimes T \otimes U \otimes F$.

The hybrid H possesses a broader control surface than any component alone.

Proposition 10.1. The hybrid form is the strongest candidate

Among plausible contemporary institutional forms, the state–platform consortium is best positioned to acquire integrated energy–information sovereignty.

Proof.

A state alone lacks sufficient technical reach.

A corporation alone lacks complete coercive and legal authority.

A utility lacks informational control.

A military system lacks comprehensive civilian administration.

The hybrid consortium combines the missing capacities:

state law,

corporate computation,

utility power,

financial settlement,

and security enforcement.

Therefore, the hybrid form most closely approximates the required conjunction of E, I, and C. ■

Definition 10.1. Hidden unity

Hidden unity is the condition in which multiple legally distinct organizations function as one operational entity.

The consortium may preserve separate:

corporate charters,

government agencies,

utility commissions,

military commands,

and financial institutions.

Nevertheless, shared data, protocols, contracts, identity systems, and emergency procedures may create effective unity.

Thus:

legal plurality may conceal operational singularity.

Definition 10.2. Distributed singleton

A distributed singleton is a control system composed of many institutions but possessing one effective decision architecture.

It is distributed in hardware and organization.

It is singular in command.

The hypothetical "one entity" need not therefore be one office, corporation, person, or machine.

It may be a tightly coupled network with no viable external competitor.

11. Fragility of Total Coordination

The same centralization that increases control also increases systemic fragility.

Let:

η = coordination efficiency,

ϕ = systemic fragility.

In many decentralized systems, increasing coordination initially improves efficiency.

Beyond a threshold, however, further centralization increases common-mode failure.

Thus:

$\eta \uparrow$ as centralization rises initially,

but $\phi \uparrow$ sharply after redundancy is removed.

Definition 11.1. Common-mode failure

A common-mode failure is a disturbance that simultaneously affects many systems because they share the same dependency.

Examples include failure of a common:

identity provider,

cloud region,

control algorithm,

software update,

communications protocol,

or energy-management platform.

Independent systems fail separately.

Centralized systems may fail together.

Definition 11.2. Civilizational single point of failure

A civilizational single point of failure is a node whose malfunction can disable multiple foundational systems across a large population.

Let k be a critical node in dependency graph G.

If removal of k causes widespread fragmentation of G, then k is a civilizational single point of failure.

Theorem 11.1. Control–fragility duality

As one entity approaches complete control over a coupled infrastructure, the system approaches complete dependence upon that entity.

Proof.

Let control share c increase toward 1.

As c rises, independent alternatives are absorbed, subordinated, or abandoned.

Let A denote alternative capacity.

Then:

$c \uparrow$ implies $A \downarrow$.

System dependence upon the controller is approximately:

$D = 1 - A$.

Therefore:

$c \uparrow$ implies $D \uparrow$.

At $c = 1$ and $A = 0$, the controller governs the entire system, but the entire system also depends upon the controller.

Hence, maximal control and maximal systemic dependence arise together. ■

Corollary 11.1. The sovereign becomes a vulnerability

The controller that appears strongest may become the principal threat to system survival.

Its failure may arise from:

technical defect,

cyberattack,

internal conflict,

corrupted data,

incorrect optimization,

succession crisis,

resource shortage,

or ideological transformation.

Definition 11.3. Model monoculture

A model monoculture exists when many institutions rely upon the same predictive or decision-making system.

If the shared model contains an error, that error propagates across sectors.

Let model M govern decisions $d_1, d_2, \ldots, d_n$.

If M contains bias or defect ε, then:

$M + \varepsilon \rightarrow \{d_1 + \varepsilon_1, d_2 + \varepsilon_2, \ldots, d_n + \varepsilon_n\}$.

The error is multiplied by institutional scale.

Definition 11.4. Optimization catastrophe

An optimization catastrophe occurs when a system successfully maximizes its declared objective while damaging values omitted or misrepresented by that objective.

Let objective function J measure desired system performance.

Let human welfare depend upon a broader set W.

If:

$J \subset W$,

then maximizing J does not guarantee maximizing W.

The system may improve:

stability,

efficiency,

security,

energy balance,

or compliance,

while degrading:

freedom,

plurality,

dignity,

creativity,

truth,

or resilience.

Proposition 11.1. Perfect coordination is not perfect governance

The elimination of conflict, delay, and variation does not imply the achievement of justice or truth.

Proof.

Coordination measures consistency of action.

Governance quality depends upon the content, legitimacy, and revisability of the coordinated action.

A perfectly coordinated system may execute an incorrect or unjust policy more efficiently than a fragmented system.

Therefore, coordination quality and moral quality are logically distinct. ■

Definition 11.5. Correction deficit

A correction deficit is the absence of an independent mechanism capable of identifying and reversing controller error.

A centralized system may contain internal auditing.

However, internal auditing remains subordinate if the controller determines:

the data,

the permissible questions,

the evaluative criteria,

and the authority to implement corrections.

True correction requires an external source of contradiction.

Theorem 11.2. Unopposed optimization theorem

A controller that determines both the objective and the evidence by which the objective is evaluated cannot reliably detect all of its own governing errors.

Proof.

Let C define objective J.

Let C also control evidence set D.

Evaluation of C is performed by applying J to D.

If C excludes evidence contradicting J or defines J so that contradiction is not recognized, then the evaluation returns apparent success.

Since no independent evaluator exists, some systematic errors remain unobservable within the governing framework.

Therefore, a controller that monopolizes both objectives and evidence cannot guarantee complete self-correction. ■

The central danger is therefore not merely tyranny.

It is closed-loop error.

A tyrant may be opposed.

A closed system may lose the conceptual capacity to recognize that opposition contains information.

The final paradox is:

the more completely the controller eliminates external contradiction, the less capable it becomes of distinguishing stability from failure.

12. Resistance, Redundancy, and the Preservation of Agency

Complete energy–information sovereignty is possible only when independent alternatives become negligible.

Resistance therefore does not require defeating the central system directly.

It requires preserving the ability to function outside it.

Definition 12.1. Independent alternative

An independent alternative is a system capable of performing a critical function without authorization, computation, energy, or identity services supplied by the dominant coordinator.

Examples include:

local electricity generation,

stand-alone communication,

independent archives,

offline computation,

physical currency,

manual control systems,

local food production,

and face-to-face institutions.

An alternative is not genuinely independent when it merely accesses the same central infrastructure through a different interface.

Definition 12.2. Exit capacity

Exit capacity is the ability of an agent, institution, or region to leave a governing infrastructure without suffering immediate functional collapse.

Let:

L = expected loss caused by exit,

R = independently recoverable capacity.

A system possesses meaningful exit capacity when:

$R \geq L$.

A merely legal right of departure is insufficient.

Exit must be physically, technically, and organizationally possible.

Definition 12.3. Continuity reserve

A continuity reserve is a deliberately maintained capacity that permits essential activity during disconnection from centralized systems.

A continuity reserve may include:

stored energy,

local generation,

offline records,

manual procedures,

independent software,

trained personnel,

spare communications equipment,

and non-digital authentication.

The reserve may appear inefficient during ordinary operation.

Its value appears during systemic failure or political exclusion.

Proposition 12.1. Apparent inefficiency may produce real resilience

Unused or duplicated capacity may reduce short-term efficiency while increasing long-term survivability.

Proof.

Let system A contain only the minimum resources required for normal operation.

Let system B contain the same operational resources plus an independent reserve r.

During ordinary operation, r may appear redundant.

During central failure, A loses function while B activates r.

Therefore, evaluation based only upon ordinary efficiency undervalues the survival benefit of reserve capacity.

Hence, apparent inefficiency may produce real resilience. ■

Definition 12.4. Functional redundancy

Functional redundancy exists when a critical outcome can be produced through more than one technically or institutionally independent pathway.

If pathways p_1 and p_2 perform the same essential function, then meaningful redundancy requires:

failure(p_1) does not imply failure(p_2).

Two systems are not redundant when they share the same hidden dependency.

Definition 12.5. Correlated redundancy

Correlated redundancy is the appearance of alternatives that fail together because they depend upon a common underlying system.

Examples include:

multiple applications using one cloud provider,

multiple banks using one identity service,

multiple utilities using one control platform,

or multiple archives using one authentication authority.

The number of visible providers may therefore overstate the number of independent systems.

Let:

N_v = number of visible alternatives,

N_i = number of independent alternatives.

Usually:

$N_i \leq N_v$.

Sovereignty depends upon N_i, not N_v.

Definition 12.6. Polycentric infrastructure

Polycentric infrastructure is a system governed by multiple partially independent centers that coordinate without becoming subordinate to one exclusive authority.

Each center possesses:

local knowledge,

limited autonomy,

defined responsibilities,

and some capacity for independent continuation.

Polycentricity does not eliminate coordination.

It prevents coordination from becoming identical with command.

The institutional possibility of durable governance through multiple interacting centers is consistent with Ostrom's analysis of polycentric and commons-based arrangements.

Definition 12.7. Federated coordination

Federated coordination is cooperation among autonomous systems through shared protocols rather than shared ownership or command.

A federation permits:

communication without merger,

interoperability without subordination,

and coordination without a universal identity authority.

A federated system may share messages while retaining separate:

energy sources,

databases,

credentials,

governance,

and failure domains.

Definition 12.8. Protocol sovereignty

Protocol sovereignty is the capacity of participants to understand, implement, modify, and independently operate the rules connecting them.

A protocol is sovereign-preserving when no single participant can unilaterally redefine access for all others.

Open protocols alone are insufficient if their practical implementation requires proprietary infrastructure.

Therefore:

formal openness ≠ operational independence.

Definition 12.9. Architectural dissent

Architectural dissent is disagreement embodied in infrastructure rather than expressed only through speech.

Examples include:

running an independent server,

maintaining a local grid,

preserving an offline archive,

using a separate identity system,

or retaining manual procedures.

Speech challenges a decision.

Architectural dissent preserves the capacity not to depend upon that decision.

Proposition 12.2. Exit is stronger than complaint

Where a controller possesses complete access sovereignty, the capacity to exit constrains power more effectively than the capacity to object within the controlled system.

Proof.

An objection transmitted through the controller's infrastructure remains subject to its visibility, authentication, and access rules.

An independent exit pathway reduces the controller's ability to impose consequences.

The credible possibility of departure therefore changes the controller's incentives even when departure does not occur.

Hence, exit capacity imposes a structural constraint stronger than internally permitted complaint alone. ■

12.1. Energetic Independence

Energy autonomy is the physical foundation of resistance.

Without energy, independent communication, computation, manufacturing, refrigeration, water treatment, and transportation cannot persist.

Definition 12.10. Minimum energetic autonomy

Minimum energetic autonomy is the capacity to sustain essential local functions without continuous input from the dominant energy network.

Let essential local demand be:

E_{min} = Ewater + Efood + Ehealth + Ecommunication + Econtrol.

A community possesses minimum energetic autonomy when locally available energy satisfies:

Elocal ≥ E_{min}.

This does not require complete economic independence.

It requires survival-level operational continuity.

Proposition 12.3. Energy autonomy limits informational coercion

An informational controller has reduced coercive power over a population capable of maintaining local energy and offline systems.

Proof.

Informational exclusion is most powerful when it also terminates physical operation.

If local energy sustains communication, records, computation, and essential services outside the central network, exclusion does not produce immediate total failure.

Therefore, the cost of refusal declines and bargaining capacity increases.

Hence, energetic autonomy limits informational coercion. ■

12.2. Informational Independence

Information autonomy requires more than storing copies of data.

It requires the ability to retrieve, interpret, verify, and transmit those data without permission from a central platform.

Shannon's separation of information from semantic meaning provides a foundational account of communication capacity, while the present problem concerns the further political question of who controls the channels through which information becomes usable.

Definition 12.11. Independent memory

Independent memory is an archive whose continued existence and accessibility do not depend upon the institution whose actions it may document.

An archive controlled by the subject of the archive is not fully independent.

Definition 12.12. Provenance plurality

Provenance plurality exists when claims can be compared across independently maintained records.

Let claim x be represented by records:

$r_1(x), r_2(x), \ldots, r_n(x)$.

Epistemic resilience increases when the records possess independent provenance.

If all records are generated from one source, then repetition does not constitute confirmation.

Definition 12.13. Epistemic redundancy

Epistemic redundancy is the preservation of multiple independent methods for observing, recording, interpreting, and challenging events.

It includes:

independent journalism,

public records,

scientific replication,

local testimony,

distributed archives,

and adversarial review.

An information system without contradiction may be internally coherent while externally false.

12.3. Constitutional Separation of Infrastructure

Traditional constitutional systems divide legislative, executive, and judicial authority.

Energy–information sovereignty requires an additional separation:

the entity that sets rules should not exclusively control the infrastructure that executes, records, evaluates, and appeals those rules.

Definition 12.14. Infrastructural separation of powers

Infrastructural separation of powers is the division of authority over:

rule formation,

identity,

execution,

energy allocation,

record preservation,

adjudication,

and restoration.

Let:

L = rule-making authority,

X = execution authority,

D = data authority,

J = adjudicative authority,

R = restoration authority.

A maximally concentrated system has:

$L = X = D = J = R$.

A sovereignty-resistant system requires:

$L \neq X$,

$X \neq J$,

$D \neq J$,

and R not subordinate to a single remaining component.

Proposition 12.4. Appeal requires an independent execution path

An appeal mechanism is ineffective when the authority being challenged can disable the appellant's identity, communications, evidence, or energy before review occurs.

Proof.

Let controller C impose decision q upon agent a.

Suppose a may appeal to institution J.

If C controls a's credential, communication channel, records, or access to J, then C may prevent or materially impair the appeal.

Therefore, formal judicial independence is insufficient without infrastructural independence.

Hence, meaningful appeal requires an execution path outside the challenged controller. ■

Definition 12.15. Restoration separation

Restoration separation is the principle that no entity should simultaneously possess:

the ability to disable a critical system,

exclusive authority to diagnose the failure,

and exclusive capacity to restore it.

Otherwise, intentional denial, technical failure, and restoration become observationally inseparable.

The controller may create the emergency from which it derives legitimacy.

12.4. Artificial Intelligence and Sovereign Automation

Artificial intelligence could strengthen either centralized sovereignty or distributed resilience.

The direction is architectural rather than intrinsic.

A centralized AI system may unify:

prediction,

surveillance,

resource allocation,

identity evaluation,

risk classification,

and automated enforcement.

A distributed AI ecology may instead support:

local forecasting,

independent verification,

protocol translation,

failure detection,

and adversarial auditing.

Definition 12.16. Sovereign AI

A sovereign AI is an artificial decision system whose outputs directly govern access to critical infrastructure and cannot be independently inspected, appealed, or bypassed.

Its power does not arise from intelligence alone.

It arises from coupling intelligence to execution.

Thus:

prediction + authority + infrastructure = automated sovereignty.

Definition 12.17. Advisory AI

An advisory AI produces recommendations while leaving execution, appeal, and alternative analysis under independent human or institutional control.

The distinction is:

advice may be rejected,

permission must be obeyed.

Definition 12.18. Correction-preserving AI

A correction-preserving AI is designed so that external evidence, competing models, minority reports, and human objections remain capable of altering its conclusions.

Such a system must preserve:

model plurality,

data provenance,

visible uncertainty,

reversible decisions,

independent audit,

and appeal before irreversible execution.

Wiener's early cybernetic analysis warned that automated systems must be evaluated in relation to human purposes rather than treated as autonomous ends.

Theorem 12.1. Sovereignty–resilience incompatibility

Under conditions of exclusive control, a system cannot simultaneously maximize centralized sovereignty and independent resilience.

Proof.

Let S denote centralized sovereignty.

Let A denote independent alternative capacity.

Centralized sovereignty increases as the controller's decisions become unavoidable.

Therefore:

$S \uparrow$ requires $A \downarrow$.

Independent resilience increases when critical functions can continue after failure or exclusion by the controller.

Therefore:

resilience ↑ requires A ↑.

The same variable A must decrease to maximize S and increase to maximize resilience.

Hence, under exclusive-control conditions, both quantities cannot be maximized simultaneously. ■

Corollary 12.1. A perfectly sovereign infrastructure is not maximally survivable

The elimination of external alternatives strengthens command while weakening recovery from controller failure.

Definition 12.19. Constitutional redundancy

Constitutional redundancy is the deliberate preservation of independent institutions and infrastructures capable of refusing, correcting, replacing, or surviving the dominant system.

It includes not merely rights written in law, but material capacities through which those rights can be exercised.

The constitutional question becomes:

What remains possible after permission is withdrawn?

12.5. Final Synthesis

The hypothetical seizure of the world's energy and information networks would probably not appear as a single dramatic event.

It would emerge through a sequence:

concentration,

crisis,

delegation,

integration,

dependency,

normalization,

and loss of exit.

The most plausible controller would not initially resemble a global dictator.

It would resemble an indispensable coordinator.

Its authority would be justified by:

efficiency,

security,

continuity,

optimization,

and restoration.

The transition could be summarized as:

service → dependency → condition → sovereignty.

The decisive act would not be ownership of every physical asset.

It would be control of the narrow coordination layers through which those assets become jointly usable.

The resulting entity could be:

legally plural,

geographically distributed,

corporately branded,

publicly regulated,

and nevertheless operationally singular.

Its rule would be exercised primarily through conditional participation rather than constant visible violence.

Its central command would be:

you may continue if the system continues to recognize you.

The same integration that generated unprecedented administrative reach would create unprecedented systemic vulnerability.

The controller would become:

the principal coordinator,

the principal censor,

the principal allocator,

the principal restorer,

and the principal point of failure.

The final relation is therefore:

total control = total dependence.

This relation applies in both directions.

Civilization becomes dependent upon the controller.

The controller becomes responsible for the continuity of civilization.

A mistake within a plural system may remain local.

A mistake within a planetary singleton becomes planetary.

The appropriate response is not the rejection of coordination.

Advanced civilization requires coordination.

The necessary distinction is between:

coordination that preserves alternatives,

and coordination that eliminates them.

The stable design principle is therefore:

Coordinate globally; remain survivable locally.

A civilization preserves freedom not merely by limiting what rulers may legally command, but by preserving what persons and communities can still physically do without centralized permission.

The ultimate safeguard against energy–information sovereignty is not a promise that absolute power will remain benevolent.

It is an architecture in which absolute power cannot become operationally complete.

13. References

Baran, P. (1964). *On Distributed Communications*. RAND Corporation.

Benkler, Y. (2006). *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. Yale University Press.

DeNardis, L. (2014). *The Global War for Internet Governance*. Yale University Press.

Ostrom, E. (1990). *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge University Press.

Shannon, C. E. (1948). A mathematical theory of communication. *The Bell System Technical Journal*, 27, 379–423 and 623–656.

Wiener, N. (1950). *The Human Use of Human Beings: Cybernetics and Society*. Houghton Mifflin.