The Governance Stress-Test Doctrine for Internet Institutions

A model-neutral legitimacy-under-stress framework for Internet governance institutions, RIRs, IXPs, and externally influenced reform processes

Version 1.0

Amin Dayekh

Table of Contents

Abstract

The Internet is coordinated through institutions whose authority is neither purely sovereign nor purely private*. Regional Internet Registries, ICANN-related structures, Internet Exchange Points, standards communities, policy forums, national Internet councils, and externally supported digital-governance initiatives all exercise forms of authority that depend on trust, technical competence, procedural fairness, and community acceptance. They do not govern primarily through coercion. They govern because operators, members, governments, civil society, businesses, users, and technical communities accept their authority as sufficiently lawful, useful, representative, and legitimate. [1], [2], [3], [4]

The premise of this doctrine is that such institutions hold authority on behalf of, and derive authority from, the communities they coordinate. Their authority is therefore not self-validating; it must remain traceable, bounded, representative, transparent, and correctable.

This paper proposes The Governance Stress-Test Doctrine for Internet Institutions. The doctrine argues that Internet governance legitimacy must not be presumed from legal existence, technical continuity, elections, public meetings, institutional survival, or external endorsement. When an Internet institution comes under abnormal stress - through litigation, receivership, emergency administration, political pressure, contested elections, capture attempts, donor-funded reform, external intervention, or technical-continuity claims - its legitimacy must be tested through a structured review of authority, mandate, representation, capture risk, conflict disclosure, emergency limits, technical continuity, external influence, remedial capacity, procedural traceability, and community consent.

The doctrine does not claim to invent operational continuity testing for RIRs. ICP-2 and the RIR system already contain continuity, accountability, audit, operational capability, emergency continuity, rehabilitation, bottom-up governance, and anti-control concepts. The contribution here is narrower and more specific: continuity answers whether the registry can keep functioning; legitimacy-under-stress answers whether the authority by which it functions remains acceptable, bounded, representative, transparent, and correctable while pressure is applied. [7], [8], [11], [15], [16]

The doctrinal statement is therefore this: an Internet governance institution responsible for critical coordination functions must be capable of demonstrating legitimacy under stress. Where abnormal pressure alters the institution's ordinary governance environment, legitimacy cannot be presumed from legal existence, operational continuity, formal voting, or external support alone. It must be affirmatively tested, and any emergency or externally supported measure that preserves function while weakening authority, representation, remedy, or community consent must be treated as provisional, reviewable, and incapable of becoming ordinary governance without appropriate validation.

AFRINIC and APNIC are used as contrasting illustrations, not as the limits of the doctrine. AFRINIC shows late-stage institutional stress, where litigation, emergency administration, and continuity concerns affect ordinary governance. APNIC shows preventive election stress, where by-law reform addresses nominee eligibility, litigation conflicts, corporate-group influence, geographic concentration, and electoral oversight before collapse. The doctrine also applies beyond RIRs to IXPs, national councils, digital sovereignty processes, and externally funded reform projects. [19], [21], [22]

1. Introduction: Internet Governance Under Stress

The Internet's institutional achievement is not only technical. It is also constitutional in a distributed sense. The network grew without a world ministry, without a single sovereign authority, and without a central legislature capable of commanding global obedience. Its stability has depended instead on technical standards, registries, contracts, operational norms, voluntary coordination, community trust, and institutional restraint. This has allowed a global system to function across jurisdictions, markets, cultures, and political systems that often disagree. [1], [4], [5]

The premise of this doctrine is that Internet governance institutions do not possess authority for themselves. They hold authority on behalf of, and derive authority from, the communities whose coordination they enable. Their authority is therefore functional, delegated, and conditional: functional because it exists to preserve coordination; delegated because it depends on community recognition, institutional rules, and shared reliance; and conditional because it must remain bounded by mandate, procedure, transparency, and correction. When those conditions weaken, an institution may remain legally alive and technically operational, but the authority by which it acts becomes open to legitimate challenge.

Two distinctions anchor this doctrine. First, continuity is not legitimacy. Continuity asks whether the institution or service can keep functioning; legitimacy asks whether the authority by which it functions remains justified, bounded, representative, transparent, and correctable. Second, assistance is not substitution. Assistance supports the community's own authority; substitution occurs when an external actor becomes the practical source of direction while the community remains only formally visible. These two distinctions are essential because stressed institutions often survive operationally while their authority, mandate, representation, or community acceptance deteriorates.

That achievement is now under pressure. Internet institutions are being pulled into litigation, emergency administration, state ambition, digital sovereignty agendas, donor-funded reform, cybersecurity politics, resource scarcity, contested elections, and geopolitical competition. These pressures do not always break an institution visibly. The website may remain online. Services may continue. Meetings may be held. Elections may take place. Public statements may invoke stability, accountability, and reform. But institutional movement is not institutional legitimacy. [31]

A registry can remain technically functional while its governance authority becomes disputed. A court may preserve a company while community legitimacy remains unsettled. An election may produce officers while the authority convening the election remains contested. External actors may provide useful assistance while gradually becoming the practical source of direction. Technical continuity is necessary, but it cannot become a universal excuse for governance opacity.

The doctrine begins from this distinction. Internet governance already has principles for ordinary times: openness, transparency, accountability, multistakeholder participation, bottom-up policy development, technical stability, and community responsiveness. The harder question is what happens when those principles are tested by abnormal institutional pressure. The purpose of this doctrine is to provide a model-neutral legitimacy test for that moment. [2], [3], [17]

2. Relationship to ICP-2 and the RIR Governance Document

This doctrine should not be read as a substitute for ICP-2 or for the current RIR Governance Document process. The current draft proposed as the successor to ICP-2 already moves the RIR system into a lifecycle-governance framework. It addresses recognition, operation, derecognition, operational obligations, service continuity, emergency continuity, audit, rehabilitation, bottom-up policy development, transparency, independence, and safeguards against undue control. It also reflects a continuing consultation process rather than an already completed final settlement. [7], [8], [9], [10]

The doctrine does not claim that the RIR system lacks continuity testing or accountability mechanisms. In 2015, as part of the IANA Stewardship Transition, each RIR completed a review of its governance policies and procedures with special focus on multistakeholder governance, policymaking mechanisms, and capture risk. AFRINIC's accountability assessment was conducted through an independent review process, and AFRINIC Board records show that a public summary was approved for publication in May 2016. The IANA Numbering Services SLA and the Joint RIR Stability Fund also show that the number-resource system already contains continuity-oriented mechanisms. [11], [12], [13], [14], [15], [16]

The contribution of this doctrine is different. It addresses the legitimacy layer that can remain unresolved even where operational continuity exists and even where lifecycle criteria are being developed. It asks what happens when an Internet institution is still alive, still functioning, and still legally present, but its authority is contested, its emergency mandate is unclear, its election process is vulnerable, its candidates or supporters are entangled with legal conflicts, its reform process is externally shaped, its reviewers may themselves have institutional interests, or its community no longer accepts the process as legitimate.

The doctrine therefore complements, rather than repeats, the RIR Governance Document. Continuity keeps the registry alive. Legitimacy keeps it accepted. The first question is whether services can continue; the second is whether the authority by which they continue remains bounded, representative, transparent, and correctable.

3. Doctrinal Statement

An Internet governance institution responsible for critical coordination functions must be capable of demonstrating legitimacy under stress. Where litigation, receivership, political pressure, emergency administration, capture attempts, external reform, disputed elections, donor influence, candidate support by conflicted actors, or technical-continuity claims alter the institution's ordinary governance environment, legitimacy cannot be presumed from legal existence, operational continuity, formal voting, or external support alone. It must be affirmatively tested through a structured review of authority, mandate, representation, capture risk, conflict disclosure, emergency limits, technical continuity, external influence, remedial capacity, procedural traceability, reviewer legitimacy, affected-community support, and the evidence of sustained community acceptance. Any emergency or externally supported measure that preserves function while weakening these conditions must be treated as provisional, reviewable, and incapable of becoming ordinary governance without appropriate validation by the relevant institutional process and affected community.

This doctrine is not self-executing. It does not invalidate institutional acts by declaration. It becomes operational only when incorporated into bylaws, election rules, recognition criteria, court pleadings, donor conditions, public consultation standards, or community accountability practice. Its primary character is governance and public-interest analysis, not automatic legal invalidation.

4. Core Definitions

Internet institution: any organization, coordination body, registry, policy forum, operational community, standards-adjacent process, national council, IXP, or multistakeholder structure whose decisions affect the stability, interoperability, allocation, registration, coordination, or public-interest governance of the Internet.

Governance stress: a condition in which the institution’s ordinary authority, decision-making capacity, accountability mechanism, representational structure, technical function, or community trust is materially disrupted or placed under abnormal pressure.

Legality: conformity with applicable law, bylaws, court orders, contractual obligations, corporate instruments, and formal institutional rules. Legality is necessary but not identical to legitimacy.

Legitimacy: the justified authority of an Internet institution, demonstrated through traceable authority, bounded mandate, procedural fairness, meaningful participation, transparency, conflict disclosure, technical

competence, remedial capacity, and sustained acceptance by the affected community. In Internet governance, legitimacy has legal, procedural, substantive, operational, and social dimensions. Community acceptance is evidence of legitimacy, but the structural conditions that warrant acceptance must be examined separately.

Authority: the recognized power to act, decide, convene, administer, allocate, supervise, or bind a process. Under stress it must be traceable to source, scope, duration, and reviewability.

Mandate: the defined scope of purpose and power under which an actor is authorized to act. Mandate controls role, limits, duration, reporting, and correction.

Representation: meaningful inclusion of affected stakeholders before outcomes harden. It is not satisfied by symbolic attendance, late validation, or consultation without influence.

Affected community: the persons and institutions materially affected by the Internet institution's function, decisions, policies, or failures. In the RIR context, the affected community includes formal members and resource holders, but is not limited to them. It also includes network operators, policy participants, researchers, anti-abuse and cybersecurity communities, law-enforcement interfaces, civil society actors, governments, businesses, technical communities, and users affected by registry policies and number-resource administration. Formal membership may function as a practical proxy for the affected community only where the policy process remains open, transparent, and meaningfully accessible to non-member affected voices.

Capture: the condition in which an institution, election, registry function, reform agenda, or accountability mechanism is materially controlled, distorted, or redirected by an actor or coalition whose interests are not aligned with the institution's public-interest mandate.

Conflict disclosure: the publication of interests, relationships, funding sources, litigation positions, affiliations, advisory roles, or incentives that may influence judgment.

Technical continuity: the preservation of essential technical functions, service availability, registry integrity, data accuracy, security, and interoperability during stress.

External influence: material involvement by actors outside the ordinary governance structure, including courts, governments, donors, consultants, vendors, international organizations, regional bodies, and diplomatic coalitions.

Mandate substitution: the condition in which an external actor begins as supporter or facilitator but becomes the practical source of institutional direction.

Remedial capacity: the institution's ability to receive objections, correct defects, reverse improper decisions, discipline misconduct, and restore ordinary governance.

Procedural traceability: the ability to reconstruct how a decision was made, by whom, under what authority, using what evidence, after what consultation, with what conflicts, and subject to what review.

Community consent: informed acceptance, validation, or non-coerced acquiescence by the affected community. It does not require unanimity, but it does require a credible path to acceptance.

Affected-community support: meaningful participation, informed engagement, or non-coerced support from the affected community during the process being tested. It does not require unanimity and does not convert every objection into a legitimacy failure. It asks whether the affected community had a credible opportunity to understand, influence, challenge, and, where appropriate, support the process before outcomes hardened. Sustained community acceptance may then serve as evidence that legitimacy has been achieved or restored.

These definitions are intended to make the doctrine evaluative rather than rhetorical. They allow a reviewer to say that an institution may be lawful but weak in mandate, technically continuous but deficient in representation, externally supported but vulnerable to substitution, or electorally active but deficient in consent. [28], [29], [30]

5. The Governance Stress-Test

The Governance Stress-Test asks whether an Internet institution under abnormal pressure can still demonstrate legitimate authority. It is not designed to reward every complaint or paralyze ordinary operations. It is a diagnostic instrument for material stress conditions: litigation affecting governance, emergency administration, loss of board quorum, disputed election authority, serious membership-register controversy, credible capture allegations, external reform intervention, government pressure affecting independence, donor-shaped governance design, prolonged policy paralysis, technical-continuity risk, or community challenge supported by evidence.

The test has twelve components in this version: authority, mandate, representation, affected-community support, capture risk, conflict disclosure, emergency limits, technical continuity, external influence, remedial capacity, procedural traceability, and reviewer legitimacy. The first ten are the core institutional tests; reviewer legitimacy and candidate-support conflict are added safeguards because a stress-test process itself can become a site of influence.

Authority asks whether the actor controlling the process can show the source, scope, duration, and reviewability of its power. Mandate asks whether that actor remains within the role for which it was appointed or accepted. Representation asks whether affected stakeholders participated early enough and meaningfully enough to influence outcomes. Capture risk asks whether legal pressure, corporate-group influence, concentrated voting power, donor dependency, political leverage, or technical platform control gives one actor or coalition disproportionate power.

Conflict disclosure asks whether material interests are visible before trust is damaged. Emergency limits ask whether extraordinary measures are necessary, proportionate, time-bound, and restorative. Technical continuity asks whether essential functions are preserved without turning operational custody into governance control. External influence asks whether support remains assistance or becomes mandate substitution. Remedial capacity asks whether defects can be corrected before outcomes become irreversible. Procedural traceability asks whether the decision path can be reconstructed. Reviewer legitimacy asks whether the auditors, observers, emergency operators, or reviewers themselves are transparent and conflict-tested. Affected-community support asks whether the relevant community had a meaningful opportunity to understand, participate in, influence, challenge, and support the process before outcomes became difficult to reverse. Sustained community acceptance may then be treated as evidence that legitimacy has been achieved, preserved, or restored.

The stress-test should not be reduced to arithmetic. A single authority or mandate failure may be more serious than several minor procedural weaknesses. The doctrine should classify defects by severity: minor defects require disclosure and correction; moderate defects require formal remediation; serious defects require pause of irreversible action; structural defects require independent review, community revalidation, or escalation through the institution’s own legal and governance framework.

6. RIR Diversity and Model-Neutrality

Each RIR has its own legal personality, bylaws, membership structure, election model, regional culture, policy development process, and applicable jurisdiction. AFRINIC is not APNIC. APNIC is not ARIN. ARIN is not RIPE NCC. RIPE NCC is not LACNIC. A doctrine that attempted to impose one uniform governance constitution across all RIRs would be wrong and politically indefensible.

This doctrine is therefore model-neutral. It does not harmonize RIR bylaws or replace regional governance models. It tests whether each model remains legitimate under stress. The relevant question is not whether all RIRs look alike, but whether each RIR can show, under abnormal pressure, that its own authority is traceable, its own mandate bounded, its own community represented, its own conflicts disclosed, its own emergency measures limited, its own technical continuity protected, and its own remedies available.

The doctrine should be applied through the internal law and governance model of each institution. In an AFRINIC context, the test must begin with AFRINIC's bylaws, Mauritius law, AFRINIC's policy process, and the African Internet community. In an APNIC context, it must begin with APNIC's bylaws, Australian law, APNIC election procedures, and the Asia-Pacific community. The same logic applies in ARIN, RIPE NCC, and LACNIC contexts. Different bylaws, same burden: prove legitimacy under stress.

An RIR also acts in multiple capacities. When it facilitates number-resource policy, its authority is primarily community-derived and must remain open to the wider affected community. When it sets fees, approves budgets, appoints directors, or manages corporate affairs, it may act through its member-governance or corporate structure. When it preserves registry operations, it acts as a technical operator with continuity obligations. When it represents regional coordination interests, it acts in a public-interest and ecosystem role. Legitimacy under stress requires that the institution not use authority from one capacity to justify action in another. Community policy authority should not be converted into unchecked corporate discretion; corporate survival should not override community mandate; technical continuity should not become governance substitution.

7. Continuity, Accountability, and the Missing Legitimacy Layer

The RIR system already has continuity and accountability language. ICP-2 required a candidate RIR to demonstrate organizational, operational, and community capacity. The current RIR Governance Document draft contains continuity and emergency-continuity concepts. The RIRs conducted accountability assessments during the IANA transition, and IANA numbering-service performance is subject to review under the post-transition SLA environment. These facts must be acknowledged because the doctrine is not an argument that continuity has been ignored. [7], [8], [11], [15]

The missing layer is not continuity. The missing layer is legitimacy under stress. A registry can keep functioning while its authority is disputed. A community can still receive services while elections are contested. A receiver or emergency administrator may preserve operations while changing the practical source of governance direction. A reform project may claim public value while its mandate, funding, drafting power, and validation pathway remain unclear. Continuity answers whether the registry can operate. Legitimacy-under-stress answers whether the institution remains accepted as the proper authority while it operates.

The doctrine should therefore be understood as a supplement to continuity and lifecycle governance. It is not a repetition of ICP-2. It is a test for the pre-derecognition and pre-emergency-transfer condition: the period when an RIR or other Internet institution is still alive and functioning, but when trust, authority, mandate, election integrity, external influence, or community consent have become materially contested.

8. AFRINIC and APNIC as Different Stress Types

This paper does not ask the reader to adopt any party's full narrative of the AFRINIC dispute. It uses official institutional records to identify a governance-stress condition and then applies the doctrine to that condition. AFRINIC is the late-stage stress case: litigation, emergency administration, impaired governance, technical-continuity claims, and the tension between local legal authority and regional/global Internet effect. AFRINIC's own litigation materials record extensive litigation and state that interim orders in some matters impeded the Board from operating. That official record is sufficient to establish a severe institutional stress condition, whatever one thinks of the merits of individual disputes. [19]

The AFRINIC case also shows why an RIR should not be treated as a merely local legal entity stripped of its regional and global character. An RIR may be incorporated under local law, but its function has regional and global technical consequences. It is part of the Internet Numbers Registry System. Its governance affects resource holders, operators, policy development, registry confidence, regional Internet stability, and global coordination. [5], [6], [20]

APNIC is a different case. It is not a collapse case; it is a preventive election-stress case. APNIC's 2023 by-law reform was framed as a response to community feedback after the March 2023 Executive Council election and as an effort to enhance nominee eligibility criteria and mitigate vulnerabilities in the EC election process. Its later reform process addressed term limits, term length, and geographic concentration safeguards. APNIC does not prove that election capture can be eliminated. It proves that a functioning institution can harden election architecture before breakdown. [21], [22]

Together, AFRINIC and APNIC show two uses of the doctrine. AFRINIC shows the cost of late stress testing. APNIC shows the value of preventive stress testing. One is rescue under pressure. The other is institutional hardening before breakdown. The lesson is that election architecture, eligibility rules, litigation-conflict provisions, affiliation disclosure, geographic-balance safeguards, and remedial mechanisms are not administrative decoration; they are legitimacy infrastructure.

9. External Influence and Mandate Substitution

External assistance is not the enemy of Internet governance. Courts may be necessary. Governments have legitimate roles. Donors can build capacity. Regional bodies can coordinate. ICANN and other technical institutions can support education and participation. The problem is not assistance; it is mandate substitution.

Mandate substitution occurs when an external actor begins as supporter, funder, facilitator, convener, adviser, or technical helper, but becomes the practical source of institutional direction. The community remains visible, but the agenda, drafting, funding, validation, or reform pathway is controlled elsewhere. In Internet governance, drafting power is governance power.

The ICANN-Smart Africa cooperation provides a useful boundary case. Official materials frame the relationship around capacity development, outreach, engagement, and African participation in Internet governance. Such cooperation may be legitimate and useful. But where capacity-building ecosystems move into reform proposals, transitional frameworks, or governance architecture for an institution under stress, the burden of disclosure and community validation increases. [23], [24], [25]

ICANN's November 2025 statement on AFRINIC governance is important because it drew the boundary clearly: changes or proposals concerning AFRINIC governance must be discussed and decided by AFRINIC members and the African Internet community, regardless of who proposes them. Later correspondence also clarified the distinction between funding, proposal development, and institutional endorsement. That distinction should become a general rule: assistance is legitimate only when disclosed, bounded, mission-consistent, non-substitutive, conflict-transparent, procedurally traceable, and capable of community correction. [26], [27]

10. Why Opacity Has Defenders

The doctrine will face resistance because it makes hidden power visible. Incumbents may resist it because it exposes weak accountability. Large members may resist it because it limits bloc influence. Governments may resist it because it places boundaries around sovereignty claims. Donors may resist it because it reveals funding architecture and drafting power. Consultants may resist it because it turns advisory influence into a matter of public record. Courts may ignore it unless it is translated into legal concepts such as bylaws, fiduciary duty, procedural fairness, natural justice, public-interest function, or evidence of reasonableness.

This resistance is not accidental. Opacity has value. It allows influence without formal responsibility, sponsorship without disclosure, consultation without control, and legitimacy branding without accountability. The doctrine does not assume that institutions will adopt stress tests because they are elegant. They will adopt them only if communities, courts, consultations, donors, public scrutiny, or recognition frameworks make opacity more costly than disclosure.

African institutional reality also requires balance. African governments and regional bodies are not irrational in seeking greater influence. The continent faces infrastructure deficits, dependency on foreign platforms, uneven technical capacity, cybersecurity risk, and weak bargaining power in global digital markets. The doctrine does not deny those concerns. It argues that the cure must build African technical and institutional capacity without replacing community-based Internet governance with political centralization. [31]

11. Legal Caution: Local Law, Regional Mandate, Global Effect

A finding of legitimacy stress is not, by itself, a finding of legal invalidity. It means the process may be lawful but institutionally deficient. Legal invalidity depends on applicable law, bylaws, court orders, evidentiary standards, and the competent forum. The doctrine operates as a governance and public-interest test unless incorporated into binding instruments.

However, where the institution is an RIR or another Internet coordination body whose functions affect regional and global Internet stability, it should not be treated as a merely local legal entity stripped of its regional mandate, technical coordination role, and global systemic effect. A court, receiver, government, donor, or reform actor may be operating within a local legal frame, but the consequences of its action may extend beyond local corporate law into the integrity of the Internet Numbers Registry System, regional community trust, global interoperability, and the legitimacy of the multistakeholder model. [5], [8]

This does not place RIRs above law. It means that legal and governance analysis should be honest about the institution's function. The local legal shell is real. So is the regional and global effect. Both must be taken seriously.

12. Candidate Support, Litigation Conflict, and Election Legitimacy

Election legitimacy in Internet institutions depends not only on whether votes are counted. It also depends on the validity of the authority convening the election, stability of the rules, credibility of nominee eligibility, integrity of the voter base, conflict disclosure, corporate-affiliation transparency, campaign-support transparency, independent oversight, available remedies, and community acceptance.

An Internet governance institution should not accept, validate, or treat as conflict-free any candidate who is endorsed, sponsored, funded, promoted, vouched for, strategically supported, or materially backed by a person, company, foundation, association, coalition, or related entity engaged in legal conflict with the institution itself, unless an independent eligibility body determines that no material conflict exists. This rule should apply not only to direct litigants, but also to related corporate bodies, controlling shareholders, officers, employees, legal representatives, funders, campaign organizers, affiliated foundations, and coordinated support networks.

Geographic concentration should also be assessed with more realism than country-counting alone. In regional Internet institutions, capture may occur through concentration inside a particular sub-region, language bloc, market corridor, political alliance, or economically dominant cluster. A continent is not politically, economically, or infrastructurally uniform. A formally regional institution may lose representational legitimacy if governance power concentrates in a sub-region while other parts of the service area become peripheral.

The scarcity and value of number resources strengthen this concern. RIR governance is not only procedural; it is connected to scarce and valuable resources, especially IPv4 address space, transfer markets, leasing practices, resource-holder incentives, and enforcement posture. Where resource scarcity creates market power, election capture and policy capture can become economic strategies. The doctrine therefore treats capture risk as both procedural and economic.

13. Reviewer Legitimacy

Any stress-review mechanism must itself be stress-tested. A doctrine designed to detect capture must not create another capture pathway. If ICANN, the NRO, peer RIRs, auditors, emergency operators, consultants, governments, observers, or independent experts are involved in reviewing a stressed institution, their authority, conflicts, funding, methodology, evidence standard, scope, and limits must be disclosed. [8], [10]

This is especially important where audits, emergency continuity, recognition review, rehabilitation, or derecognition mechanisms are being discussed. Reviewers may have expertise, but they may also have institutional interests. Other RIRs may have peer knowledge, but they are not interest-free. ICANN may have a coordination role, but it should not become the routine governor of regional legitimacy. Governments may have public-interest concerns, but they must not become substitute sources of RIR community mandate.

Reviewer legitimacy is therefore not a secondary issue. It is a condition of trust in the review itself. The stress-test must face in both directions: toward the stressed institution and toward those claiming authority to diagnose it.

14. Beyond RIRs: IXPs, National Councils, and Digital Governance Processes

The doctrine is not confined to RIRs. Internet Exchange Points can pass traffic while governance becomes captured by a dominant member, state agency, donor project, or commercial sponsor. A community IXP should have visible membership criteria, governance rules, route-server policy processes, conflict rules, and dominant-member safeguards. A commercial IXP may operate commercially, but it should not borrow community legitimacy without community governance.

National Internet councils, IPv6 councils, cybersecurity coordination bodies, and digital transformation committees present another stress pattern. They may claim multistakeholder legitimacy while being state-heavy, consultant-shaped, donor-funded, or disconnected from operators. Such bodies should disclose appointing authority, terms of reference, membership categories, funding sources, meeting records, conflict rules, implementation pathways, and correction mechanisms. A council that speaks for the Internet community must show how that community participates in, influences, and can challenge its work.

Externally funded reform processes require a public legitimacy file: initiating authority, funding source, terms of reference, consultant selection, stakeholder map, drafting history, comments received, comments rejected, conflict disclosures, final recommendations, and implementation status. This is not excessive bureaucracy. Where external actors shape governance, the community has a right to see the architecture of influence.

15. Limits and Safeguards

The doctrine is not a veto power. Losing an argument does not make a process illegitimate. A stakeholder may dislike an outcome while the process remains valid. The stress-test applies where there is a material defect in authority, mandate, representation, capture resistance, conflict disclosure, emergency limits, technical continuity, external influence, remedy, reviewer legitimacy, or community consent.

The doctrine is not anti-court, anti-government, anti-donor, anti-ICANN, anti-RIR, or anti-reform. Courts may be necessary. Governments have legitimate roles. Donors can build capacity. Regional bodies can coordinate. Reform may be essential. The doctrine asks only that power be disclosed, mandate be bounded, representation be meaningful, and remedies remain available.

The doctrine must also be protected from misuse. Bad actors can weaponize legitimacy language to delay elections, block reform, challenge lawful decisions endlessly, or discredit outcomes they dislike. Any legitimacy challenge should identify the specific defect, the evidence supporting it, the material impact, and the remedy sought. The remedy should be proportionate: disclosure for minor defects, remediation for moderate defects, pause of irreversible action for serious defects, and independent review or revalidation for structural defects.

16. Conclusion

The Internet's coordination institutions were not built as empires. They were built as trust machines. Their authority depends on the willingness of operators, members, governments, businesses, civil society, technical communities, and users to accept that their processes are sufficiently lawful, competent, fair, open, accountable, and correctable. That acceptance is not merely reputational; it reflects the deeper premise that these institutions exercise authority on behalf of communities whose cooperation, reliance, and participation make coordination possible. When that acceptance weakens, the institution may continue to exist, but its coordination power begins to decay.

The Governance Stress-Test Doctrine does not replace ICP-2, the RIR Governance Document, RIR bylaws, ICANN accountability mechanisms, local law, or existing continuity mechanisms. It defines a missing legitimacy layer for moments when institutions remain alive and operational while authority, mandate, elections, external influence, reviewer integrity, and community consent are under abnormal pressure.

The doctrine's final proposition is simple: legitimacy is infrastructure. It must be designed, tested, maintained, and repaired. Continuity keeps the institution functioning. Legitimacy keeps it accepted. Internet governance now needs institutions that can prove, under stress, that their authority is traceable, their mandate bounded, their representation meaningful, their conflicts disclosed, their capture risks controlled, their emergency powers temporary, their technical continuity preserved without governance substitution, their external influence transparent, their reviewers accountable, their remedies practical, and their outcomes capable of community consent.

Annex A - Ten-Part Stress-Test Instrument

This annex is an operational tool. It should be adapted to the institution's own bylaws, law, governance model, and community structure. It is not a uniform constitution and not legal advice.

Test	Core question	Green	Amber / Red	Black
Authority	Can the actor show source, scope, duration, and reviewability?	Clear and public.	Incomplete or materially disputed.	No valid authority for function.
Mandate	Is the actor within its proper role?	Limited and restorative.	Broad, unclear, or creeping.	Temporary actor becomes constitutional authority.
Representation	Are affected stakeholders meaningfully included?	Early and influential.	Late, uneven, symbolic, or selective.	Community bypassed while legitimacy is claimed.
Capture risk	Can one actor or bloc control the process?	Risks mapped and mitigated.	Concentration or influence weakly addressed.	Process substantially controlled by conflicted actor.
Conflict disclosure	Are interests visible?	Proactive disclosure.	Incomplete or private handling.	Hidden conflicts materially affect legitimacy.
Emergency limits	Is emergency power temporary?	Necessary, proportionate, time-bound.	Poorly bounded or reviewable.	Emergency becomes ordinary governance.
Technical continuity	Are services preserved without governance substitution?	Auditable and role-separated.	Continuity implications unclear.	Continuity used for permanent substitution.
External influence	Is assistance non-substitutive?	Roles, funding, mandate disclosed.	External influence under-disclosed.	External actor becomes practical authority.
Remedial capacity	Can defects be corrected?	Practical remedies exist.	Remedies slow, costly, or unclear.	No meaningful remedy before irreversible outcome.
Affected-community support	Did the affected community have meaningful opportunity to understand,	Meaningful participation and broad procedural support.	Limited participation, pragmatic support, or unresolved legitimacy doubts.	Outcome treated as imposed, captured, or procedurally unacceptable by

	participate, influence, challenge, or support the process?			materially affected stakeholders.
Reviewer legitimacy	Are reviewers themselves accountable?	Authority, conflicts, method disclosed.	Disclosure incomplete.	Reviewer process becomes capture path.

Annex B - Legal Translation Table

This table translates governance concepts into legal and institutional hooks that may be useful in bylaws, pleadings, court-facing argument, public consultations, or accountability processes. Exact legal effect depends on jurisdiction and instrument.

Doctrine concept	Possible legal/institutional hook	Practical use
Authority traceability	Ultra vires, statutory authority, bylaws, court mandate, board authority	Shows whether actor had power to act.
Mandate limitation	Fiduciary duty, scope of appointment, terms of reference	Shows whether power was exceeded.
Conflict disclosure	Fiduciary duty, natural justice, conflict-of-interest rules	Shows whether decision-makers or candidates were conflicted.
Election legitimacy	Bylaw compliance, member rights, procedural fairness	Tests validity and credibility of election process.
Remedial capacity	Due process, right to be heard, appeal/review rights	Shows whether affected parties could correct defects.
External influence	Public-interest governance, funding disclosure, consultation integrity	Shows whether support became control.
Community consent	Legitimate expectation, member mandate, public-interest legitimacy	Shows whether authority remains accepted.
Reviewer legitimacy	Independence, conflict disclosure, audit integrity	Shows whether review process is itself trustworthy.

References

By “neither purely sovereign nor purely private,” this doctrine refers to the hybrid authority of Internet coordination institutions. Their legitimacy does not arise solely from state sovereignty, nor solely from private corporate autonomy. It arises from a combination of technical coordination, contractual or institutional recognition, multistakeholder participation, public-interest reliance, and community acceptance. This is consistent with the Tunis Agenda’s multistakeholder definition of Internet governance, NETmundial’s emphasis on inclusive and legitimate multistakeholder processes, and RFC 7020’s description of the globally coordinated Internet Numbers Registry System.

[1] World Summit on the Information Society, Tunis Agenda for the Information Society, 2005. https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.pdf

[2] NETmundial, NETmundial Multistakeholder Statement, 2014. https://netmundial.br/2014/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf

[3] NETmundial+10, Multistakeholder Statement, 2024. https://netmundial.br/pdf/NETmundial10-MultistakeholderStatement-2024.pdf

[4] Internet Society, Policy Brief: Internet Governance, 2025. https://www.internetsociety.org/resources/policybriefs/2025/internet-governance/

[5] IETF/RFC Editor, RFC 7020: The Internet Numbers Registry System, 2013. https://www.rfc-editor.org/rfc/rfc7020

[6] IANA, Number Resources. https://www.iana.org/numbers

[7] ICANN, Criteria for Establishment of New Regional Internet Registries (ICP-2), 2001/2012 page. https://www.icann.org/resources/pages/new-rirs-criteria-2012-02-25-en

[8] NRO, RIR Governance Document Version 2, 28 August 2025. https://www.nro.net/policy/internet-coordination-policy-2/rir-governance-document-version-2/

[9] NRO, RIR Governance Document Version 2 Consultation Community Input Report, 2 February 2026. https://www.nro.net/policy/internet-coordination-policy-2/rir-governance-document-version-2-consultation-community-input-report/

[10] ARIN, RIR Governance Document Version 2 Status Report May 2026 Now Available, 8 May 2026. https://www.arin.net/announcements/20260508/

[11] NRO, RIR Accountability Assessment Reports. https://www.nro.net/accountability/rir-accountability/regional-internet-registry-accountability-assessment-reports/

[12] NRO, AFRINIC Accountability Assessment. https://www.nro.net/afrinic-accountability-assessment/

[13] AFRINIC, Minutes of the Board Meeting Held on 11 May 2016. https://afrinic.net/board/meeting/2016/min-0511

[14] AFRINIC, Annual Report 2016. https://afrinic.net/ast/pdf/annual-reports/afrinic-annual-report-2016.pdf

[15] NRO, ICANN-RIR Service Level Agreement for IANA Numbering Services. https://www.nro.net/wp-content/uploads/ICANN-RIR-SLA-signature.pdf

[16] NRO, Joint RIR Stability Fund. https://www.nro.net/accountability/rir-accountability/joint-rir-stability-fund/

[17] ICANN, CCWG-Accountability Supplemental Final Proposal on Work Stream 1 Recommendations, 2016. https://www.icann.org/en/system/files/files/ccwg-accountability-supp-proposal-work-stream-1-recs-23feb16-en.pdf

[18] ICANN, Bylaws: Mission, Commitments and Core Values. https://www.icann.org/resources/pages/bylaws-2018-06-22-en

[19] AFRINIC, Litigation FAQs. https://www.afrinic.net/litigation-faq

[20] AFRINIC, Consolidated Policy Manual. https://www.afrinic.net/policy/manual

[21] APNIC, Proposed By-law Reform 2023. https://www.apnic.net/about-apnic/organization/structure/proposed-by-law-reform-2023/

[22] APNIC, Proposed APNIC By-law Reform 2026. https://www.apnic.net/about-apnic/organization/structure/proposed-by-law-reform-2026/

[23] ICANN and Smart Africa, Memorandum of Understanding, 12 November 2024. https://www.icann.org/en/system/files/files/mou-smart-africa-icann-12nov24-en.pdf

[24] ICANN, ICANN and Smart Africa Collaborate to Boost Internet Governance Across Africa, 13 November 2024. https://www.icann.org/resources/press-material/release-2024-11-13-en

[25] Smart Africa, Statement on the Coordinated Continental Response: Safeguarding Africa's Digital Sovereignty, 23 July 2025. https://smartafrica.org/smart-africa-statement-on-the-coordinated-continental-response-safeguarding-africas-digital-sovereignty/

[26] ICANN, ICANN's Commitment to the Africa Community, 18 November 2025. https://www.icann.org/en/blogs/details/icanns-commitment-to-the-africa-community-18-11-2025-en

[27] ICANN, Lindqvist to Dammak correspondence, 24 November 2025. https://itp.cdn.icann.org/en/files/correspondence/lindqvist-to-dammak-24-11-2025-en.pdf

[28] Mark C. Suchman, Managing Legitimacy: Strategic and Institutional Approaches, Academy of Management Review, 1995. https://doi.org/10.5465/amr.1995.9508080331

[29] Vivien A. Schmidt, Democracy and Legitimacy in the European Union Revisited: Input, Output and Throughput, 2010. https://doi.org/10.1111/j.1467-9248.2010.00856.x

[30] Elinor Ostrom, Governing the Commons: The Evolution of Institutions for Collective Action, 1990. https://doi.org/10.1017/CBO9780511807763

[31] United Nations, Global Digital Compact, 2024. https://www.un.org/global-digital-compact/sites/default/files/2024-09/Global%20Digital%20Compact%20-%20English_0.pdf