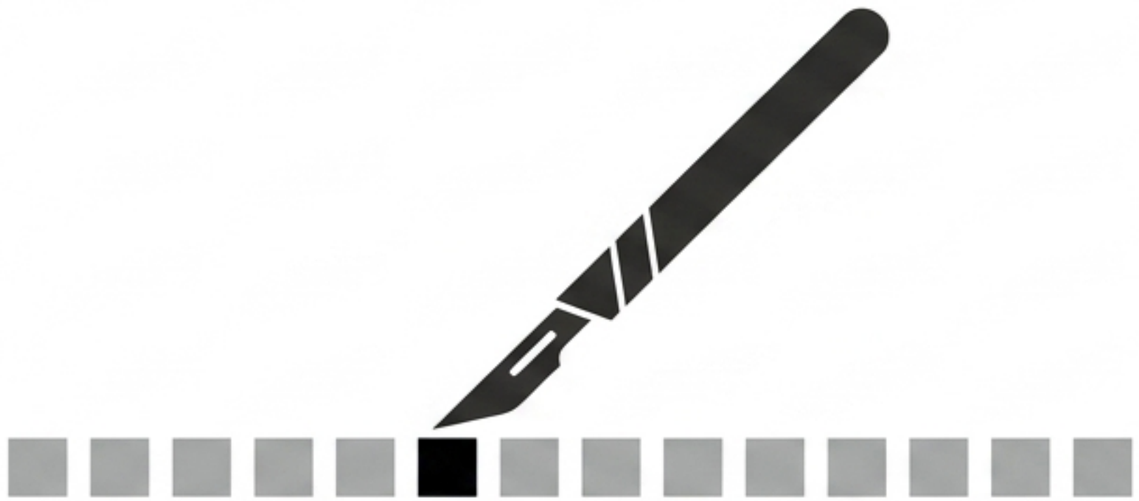
THE BLUNT INSTRUMENT

WHY THE DNS MUST ENABLE EXPRESSION, NOT SILENCE IT.

BASED ON THE 2026 REPORT BY ARTICLE 19.

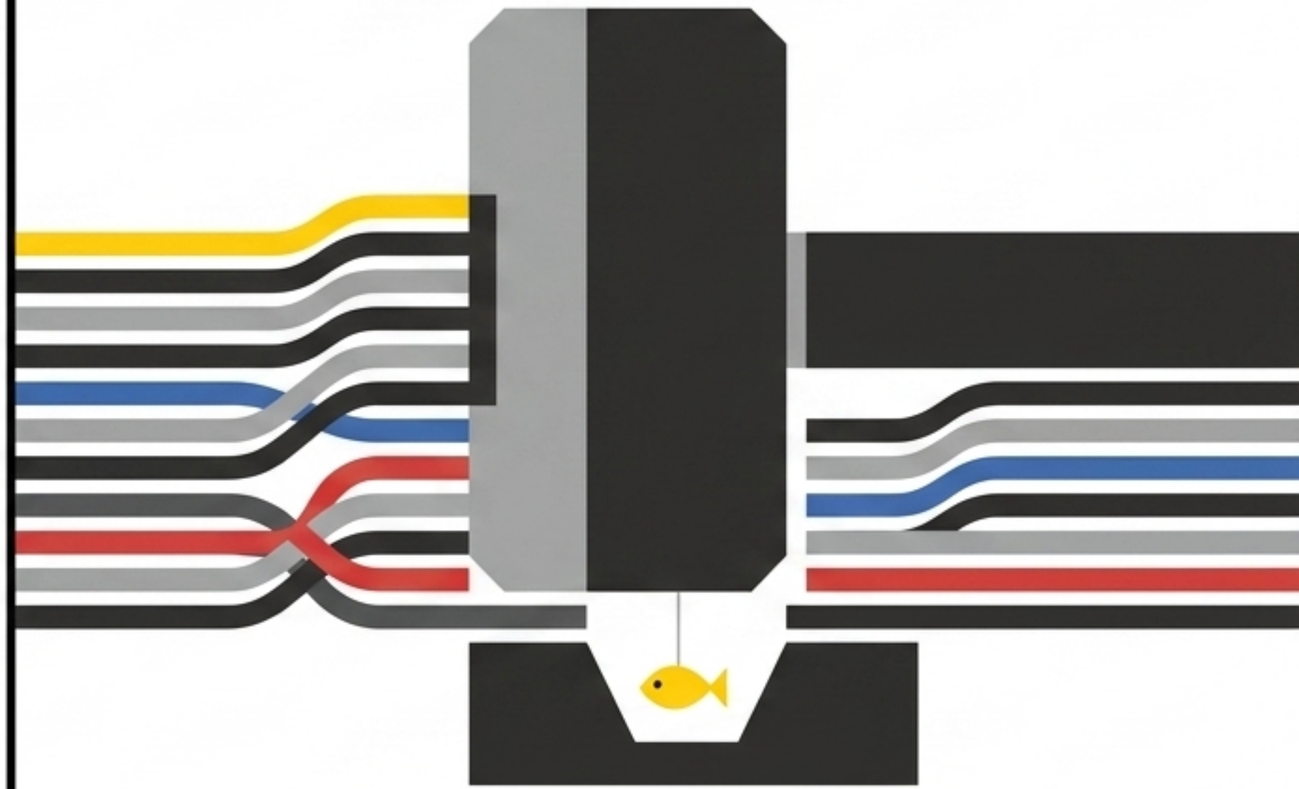
The Scalpel



Targeted Moderation

Content publishers and hosts can remove a single piece of illegal content without affecting the rest of the site.

The Sledgehammer



DNS Suspension

A suspension wipes out the entire domain. If a domain is suspended, the website, subdomains, data storage, and associated email servers vanish completely.

Content moderation is moving deeper into the internet stack.

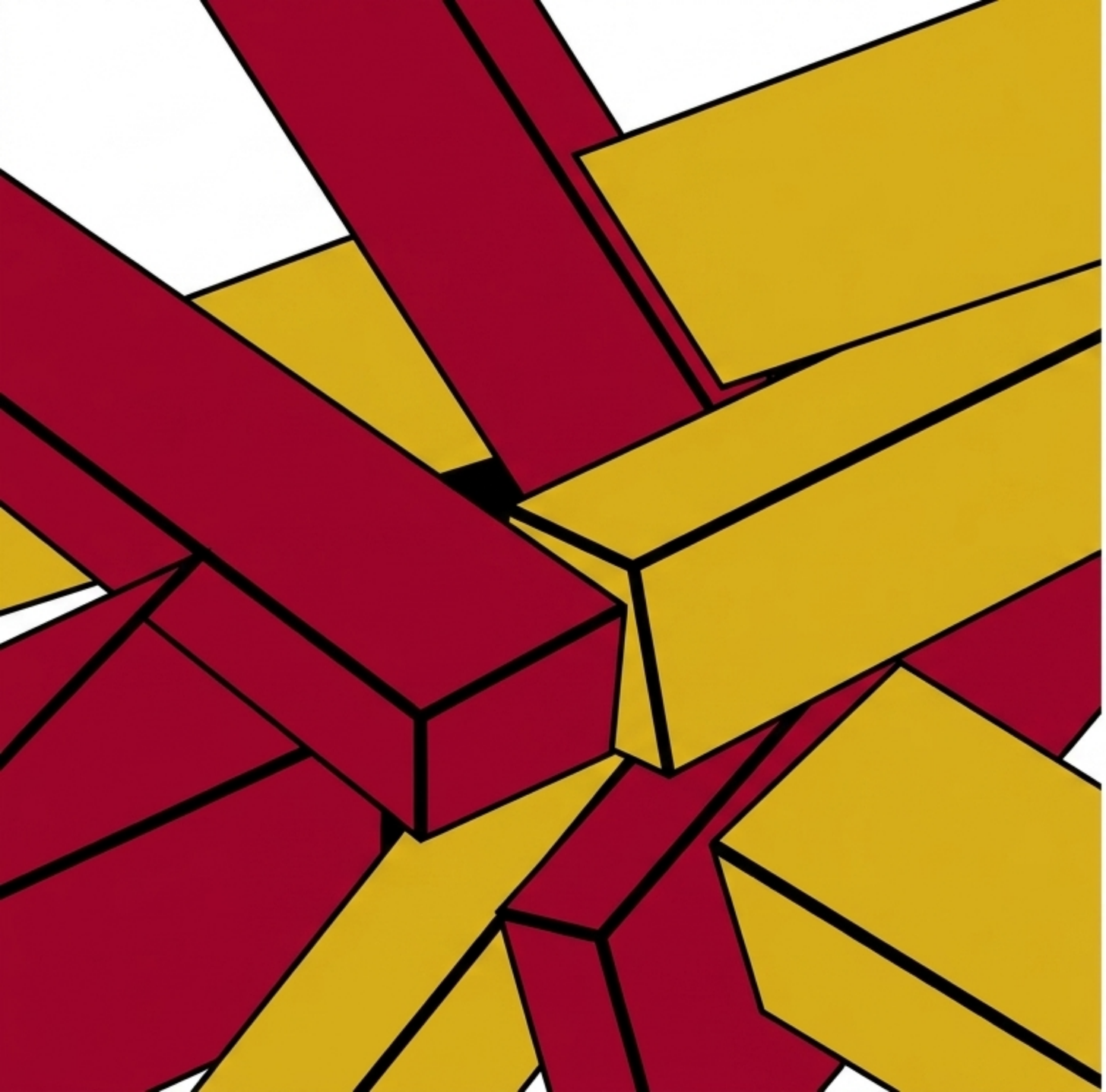
When governments and regulators weaponise the Domain Name System (DNS) to control content, they bypass standard legal frameworks. The impact on global freedom of expression is devastating, unaccountable, and disproportionate.

The Impact Zone

Infrastructure censorship in action across four continents.

India: The Silent Erasure

- **The Context**: In July 2020, three youth organisations launched a massive multilingual email campaign opposing updates to India’s Environment Impact Assessment (EIA) legislation.
- **The Mechanism:** The ccTLD registry operator for ‘.in’ disabled their domain names without warning, legal justification, or notification.
- **The Impact:** The websites and all associated email accounts vanished instantaneously. Organisers spent days troubleshooting phantom server issues, completely unaware they had been erased at the infrastructure level.

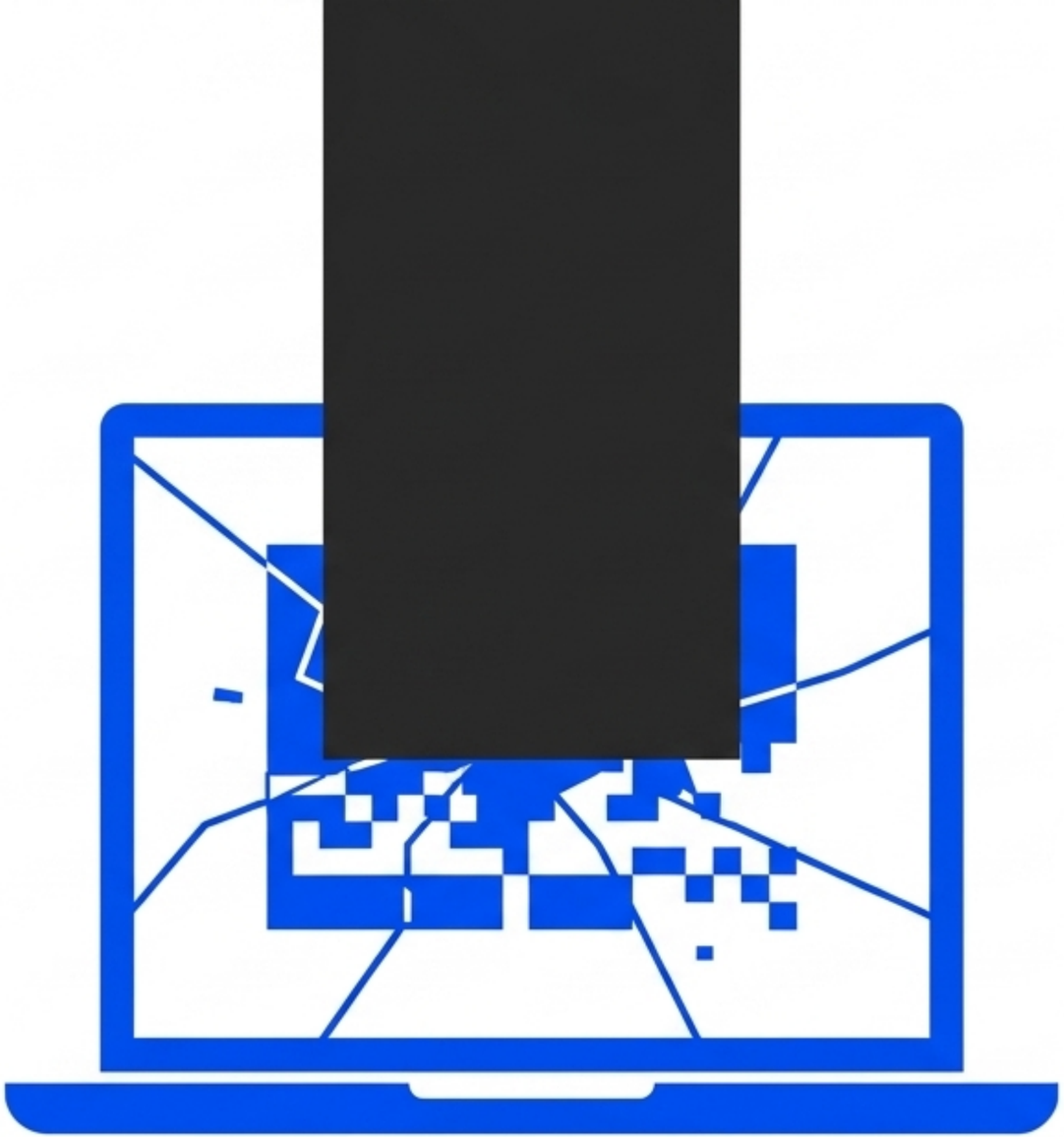


Spain: The Geopolitical Takedown

The Context: During the highly contentious 2017 Catalonian independence referendum, the Spanish government moved to suppress digital support.

The Mechanism: Police physically raided the ‘Fundació puntCAT’ registry, confiscated computers, and accused a senior executive of sedition to force the blocking of ‘.cat’ domains.

The Impact: Domains like ‘referendum.cat’ were blocked instantaneously. The registry warned ICANN that they were being forced to act as censors, suppressing freedom of speech for the entire Catalan-speaking internet community.

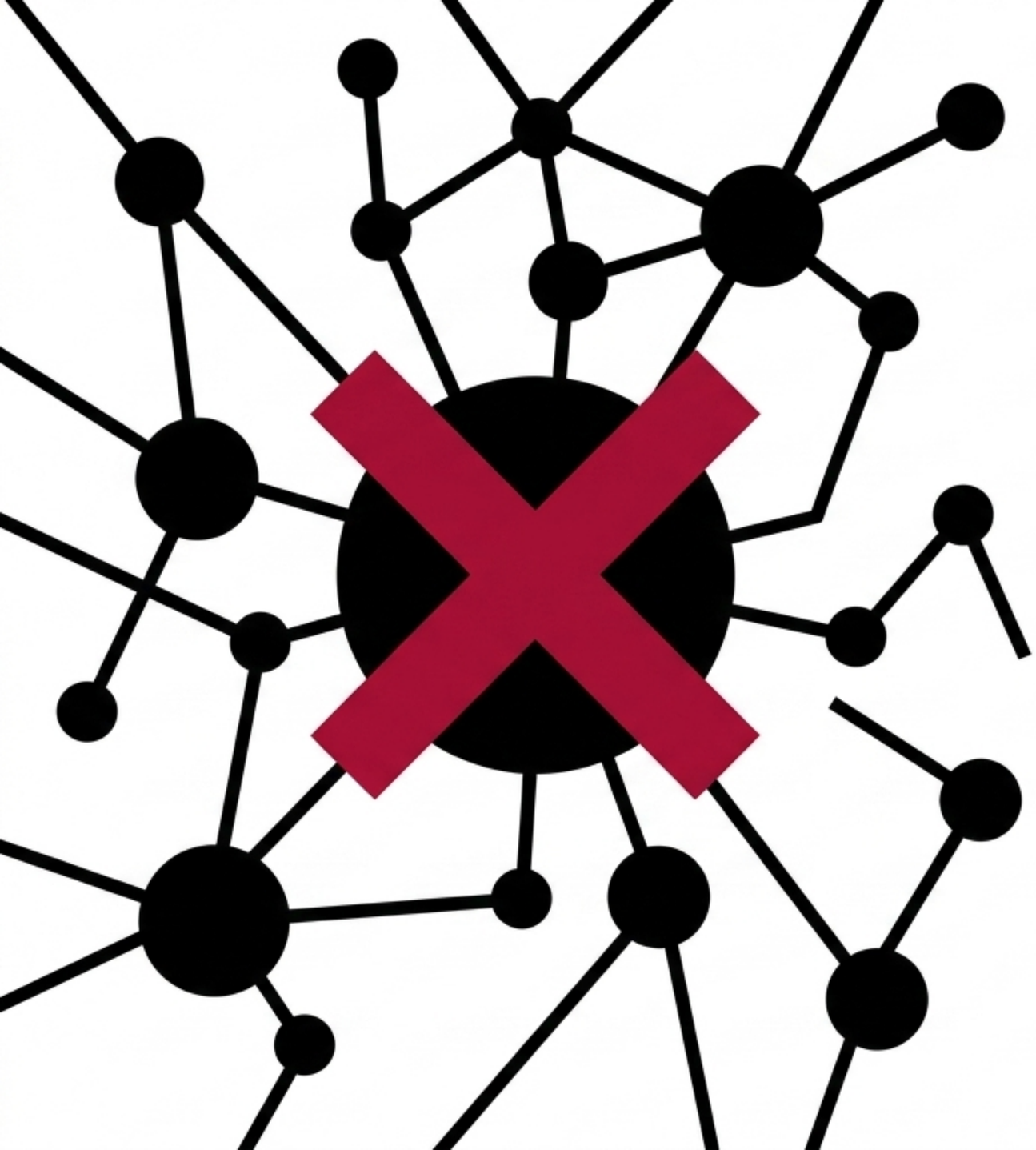


Nicaragua: The Exiled Press

The Context: In March 2025, the Ortega–Murillo regime escalated its systematic persecution of independent journalists, forcing hundreds into exile.

The Mechanism: The state-controlled ccTLD registry operator for '.ni' (the National University of Engineering) systematically blocked the domains of major independent news outlets like Confidencial and 100% Noticias.

The Impact: The news outlets were effectively "disappeared" from the national internet structure. They had to rely on pre-emptively registered alternative generic top-level domains (gTLDs) and social media to inform the public of the censorship.



Belarus: Transnational Repression

The Context: The Belarusian Association of Journalists (BAJ) has operated in exile since 2021 after being targeted under ‘anti-extremism’ legislation.

The Mechanism: The ccTLD operator for ‘.by’ suddenly mandated an ‘in-person identity verification procedure’ for the BAJ domain—a bureaucratic requirement added after the request was issued.

The Impact: Unable to return to Belarus without risking severe physical danger, BAJ could not comply. The domain was suspended, severing vital communication channels and putting confidential sources at immediate risk.

The Global Typology of Abuse

State-Directed Force vs. Administrative Exploitation	Domestic Suppression	Transnational Repression
	Spain: Police raids and sedition charges forcing direct registry compliance.	No specific data provided for this quadrant, but the structure is present.
	India & Nicaragua: Silent infrastructural suspension via state-controlled or aligned ccTLDs.	Belarus: Weaponising terms of service to force impossible administrative compliance on exiled entities.

Key Takeaway: Governments are exploiting the unique operational structures of registries to execute censorship that bypasses judicial scrutiny.

The Operators

ICANN, registries, and the hidden rules of the internet stack.

The Tiers of Infrastructural Power

ICANN (The Standard Bearer)

The global multistakeholder body that manages the DNS and sets baseline contractual policies.

Registries (The Enforcers)

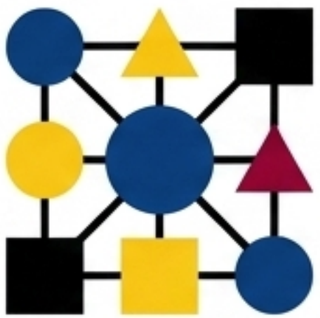
They manage the top-level domain databases (.com, .org, .br, .uk) and hold the ultimate technical power to suspend domains.

Registrars (The Intermediaries)

The retail layer that liaises directly with the domain owners (registrants).

ICANN’s Narrow Baseline

To prevent infrastructure from being used for content moderation, ICANN limits “DNS Abuse” to five strictly technical categories:



Botnets: Remotely controlled infected networks

Malware: Spreading malicious software

Pharming: Redirecting users to fake websites

Phishing: Tricking users for sensitive information

Spam: Used as a delivery mechanism for the above

This narrow definition sets a vital baseline to protect lawful speech.

The Threat of Definition Creep

ICANN (Strict)

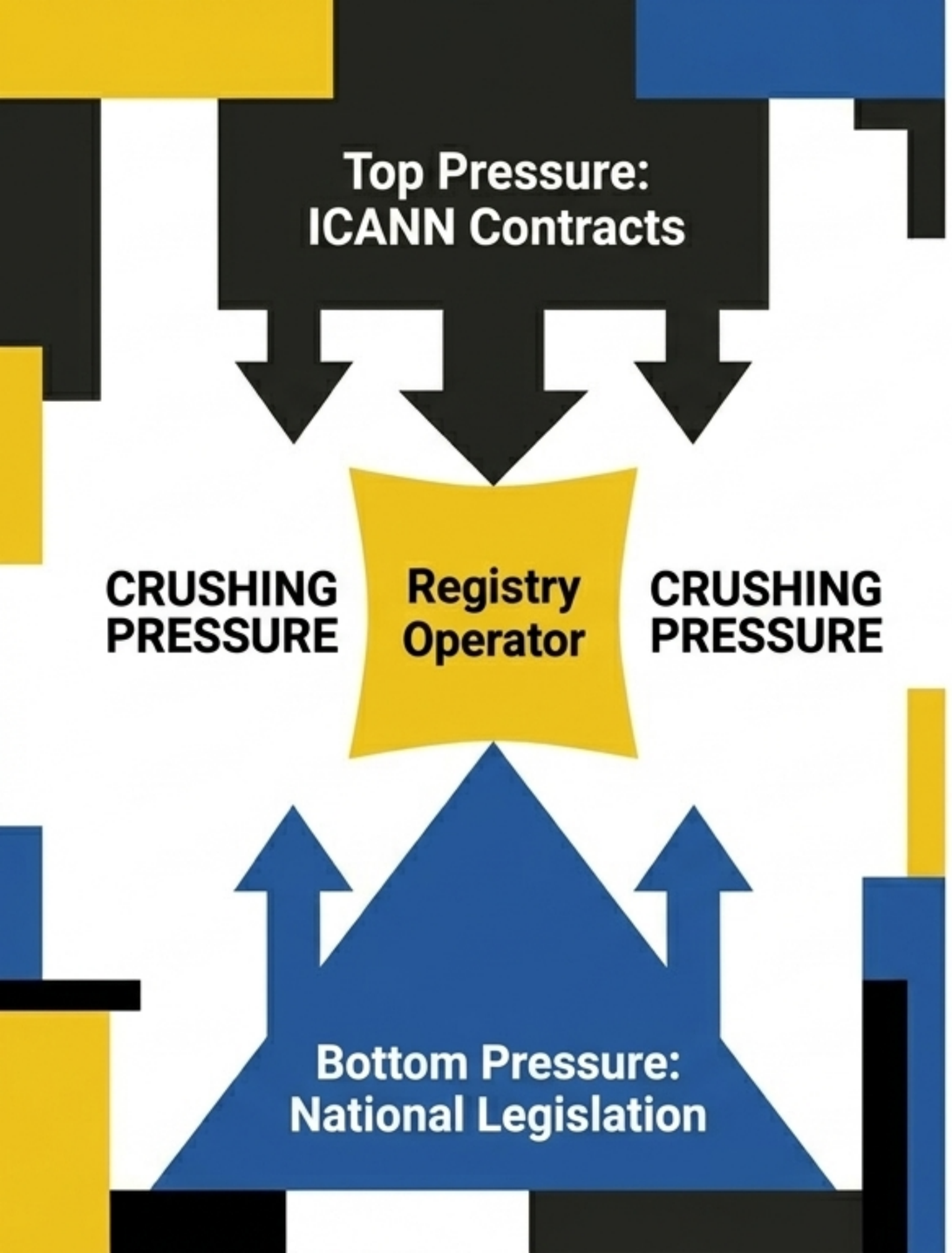
- Adheres strictly to the 5 technical categories.
- Content-neutral by design.

gTLDs (Expanded)

- Contractually bound to ICANN, but frequently add ‘online content abuse’ (like CSAM, impersonation, or trademark disputes) to their specific Terms & Conditions.

ccTLDs (The Wildcard)

- Not bound by ICANN.
- Highly susceptible to state alignment.
- Terms often expand to include inherently political and ambiguous concepts like ‘defamatory speech’, ‘public policy’, or ‘national security’.



The Jurisdictional Squeeze

Top Pressure: ICANN Contracts

Strict compliance required to maintain registry operator status.

Bottom Pressure: National Legislation

New regulatory burdens. The EU's Consumer Protection Cooperation (CPC) and Markets in Crypto-Assets (MiCA) empower authorities to order **domain deletions** without conducting prior human rights impact assessments.

The Result:

Registries are forced to preemptively over-moderate and comply with legally dubious suspension requests simply to avoid institutional liability.

The Void

Disappearing due process and the black box of suspension.

The Black Box of Suspension

Step 1: The Complaint

A government agency, law firm, or third party flags a domain for alleged abuse.

Step 2: The Decision

The registry assesses the claim internally based on its unique Terms & Conditions. The registrant is rarely contacted.

Step 3: The 404 Error

The domain is suspended. Services go dark. The registrant discovers the suspension solely because their website and email suddenly stop working.

The Human Rights Deficit

No Transparency

Decisions are made behind closed doors.

Registries are not required to disclose how definitions are interpreted or applied.

No Notification

Targeted organisations are routinely denied prior warning, robbing them of the chance to migrate data or warn vulnerable sources.

No Appeals Mechanism

Currently, ICANN contracts do not require registries to provide any due process or mechanism for a registrant to contest a wrongful suspension.

A Blueprint for Resilience

Systemic recommendations to protect the infrastructure of expression.

Fixing the Infrastructure Layer

For Registries & Registrars (The Gatekeepers)

1. Implement escalating responses: Use temporary holds and registrant outreach before permanent deletion.
2. Enshrine transparency: Publish detailed reports on takedown requests and establish landing pages for suspended sites.
3. Establish clear, accessible appeals processes for registrants.

For ICANN (The Standard Bearer)

1. Embed human rights explicitly into Consensus Policies.
2. Contractually require all registries to offer transparent recourse mechanisms.
3. Maintain the strict technical definition of DNS abuse to prevent policy overreach.

Regulation and Survival

For Governments (The Regulators)

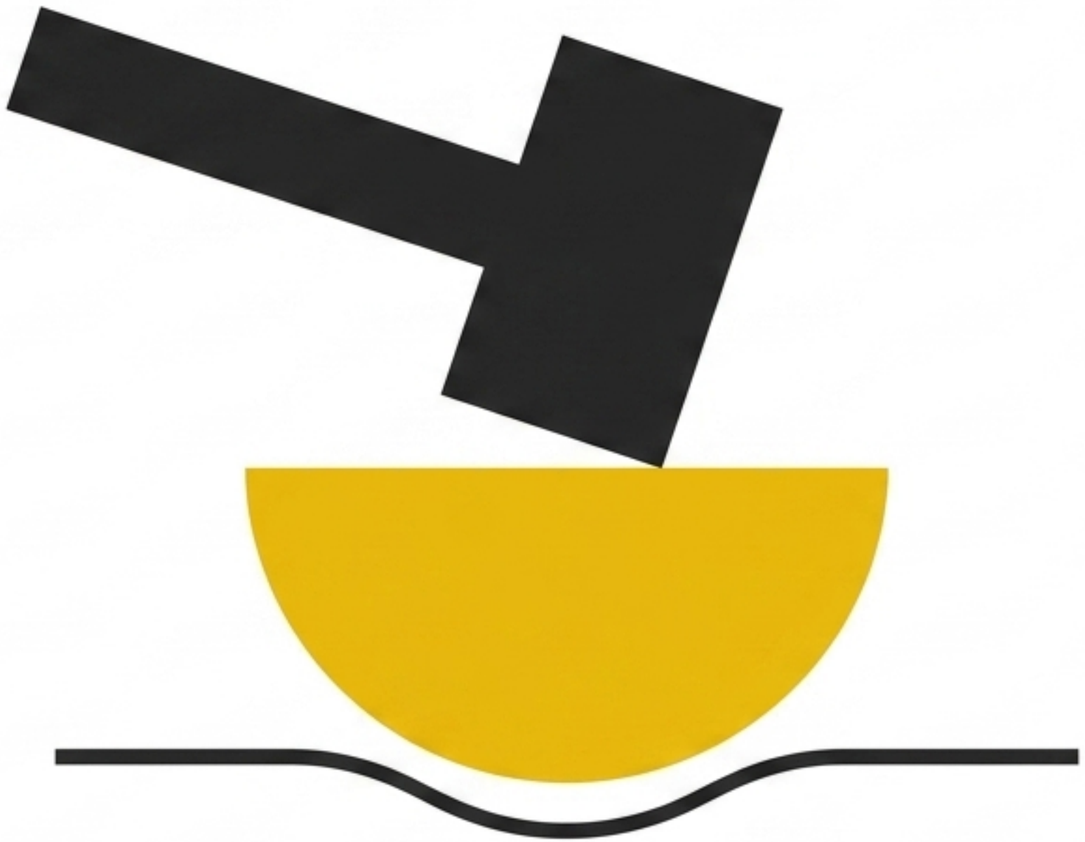
1. Conduct mandatory Human Rights Impact Assessments before legislating domain-level enforcement.
2. Reserve domain suspension strictly as a last resort.
3. Target the actor closest to the content first (e.g., hosting providers) before breaking the DNS level.

For Civil Society (The Targets)

1. Diversify infrastructure: Pre-emptively register backup domains on safer, independent gTLDs.
2. Monitor registry Terms and Conditions closely.
3. Develop rapid-response advocacy plans to alert networks the moment a suspension occurs.

Protect the Infrastructure. Enable Expression.

The Domain Name System must remain neutral, technical infrastructure—not a blunt instrument for state censorship.



Scan to read the full policy brief and research report by ARTICLE 19.