DNS and Censorship

Farzaneh Badii, NCSG member
Digital Medusa
NCSG.is

Findings from the Digital Medusa DNS Resolvers 2025 report

- DNS resolver–level blocking is growing, often without transparency or due process.
- If public resolvers become more concentrated — it raises risks of coercion, policy capture, and fragmentation.
- Blocking at the resolver or naming layer can unintentionally restrict access to legitimate content or services.
- There is a clear need to keep DNS governance technical, interoperable, and open to preserve Internet freedom.
- Work was done in collaboration with .IE

When DNS Resolvers Empower Freedom

- In countries where ISPs block websites at the DNS level, users often switch to public resolvers such as Quad9, Cloudflare (1.1.1.1), or Google DNS (8.8.8.8).
- These resolvers typically **do not implement local blocking lists**, allowing users to reach sites otherwise filtered domestically.
- The Digital Medusa *DNS Resolvers 2025* report shows a strong link between **public resolver use and Internet Freedom scores**:

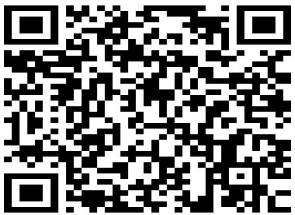
> "Countries with lower Internet freedom scores showed disproportionately high use of public resolvers, suggesting users rely on them to access uncensored information."
> *(Digital Medusa, 2025, p. 13)*

Italy’s Piracy Shield and Access to Google Drive

- **Initial blocking:** In October 2024, Italy's Piracy Shield law caused a temporary block of Google Drive, affecting users across the country.
- These were not malware or phishing domains — they were shared research or workspace links blocked by automated systems and untransparent blocklist.

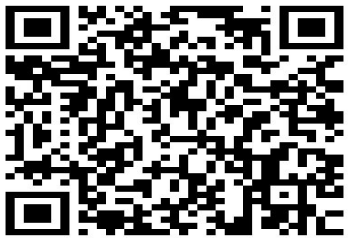
- The result: legitimate content disappeared from public access, with no due process or user notice.

“Bulk DNS blocking of Google Docs URLs illustrates how opaque blocklists, originally intended for IP enforcement,can suppress lawful communication and access to services.”
(Digital Medusa, 2025, p. 27)



Lessons learned for ICANN

- ICANN’s mission is to coordinate the policies for allocation of domain names — not to regulate content. It’s in the Bylaws and we will keep it like that.
- DNS abuse policy should stay narrowly focused on security and stability, not be repurposed for content moderation.
- When ICANN’s contracts (with registries/registrars) or its compliance mechanisms start incorporating measures that lead to content-related measures, mission creep occurs — turning technical governance into content control.



Key risks

- **Mission expansion**: framing “DNS abuse” broadly (e.g., including disinformation, illegal content) risks turning ICANN into a censorship intermediary.
- **Voluntary Public Interest Commitments (PICs)** in the new gTLD program can become de facto regulatory tools if not clearly limited or if “voluntary” commitments become expected norms.

Recommendations

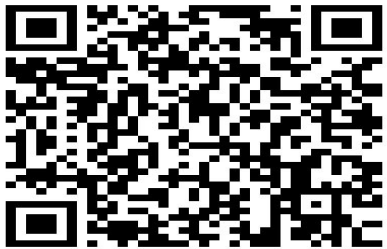
Keep ICANN’s role strictly technical and rooted in DNS security and stability.

Separate technical abuse (malware, phishing, botnets) from content regulation (speech or legality of information).

Promote transparency and due process in any blocking or suspension decisions.

Encourage diversity and decentralization of resolvers to reduce the risk of single points of control.

Maintain clear limits on PICs and new gTLD obligations to prevent content-based enforcement through contracts.



Keep in touch

To know more about Civil Society's work at ICANN go to our website: NCSG.is

Want to know more about Digital Medusa? Send me an email: farzaneh@digitalmedusa.org