Network Shutdowns and Internet Governance

By Ankita Rathi
NextGen@ICANN 83, Prague

Overview of Network Shutdowns

Intentional disruption of Internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information.

These actions cause major technical and socio-economic impacts: loss of trust, stalled services, GDP losses.

They can ranges from total blackouts to selective blocks or throttling of specific services (e.g. social media, websites).

DNS and its manipulation in Shutdowns

Authorities exploit DNS to block access in several ways:

- DNS Blocking: Instructing ISP resolvers to not resolve certain domain names.
- DNS Poisoning: Injecting false DNS answers so that a domain resolves to a wrong IP.
- DNS Hijacking: Redirecting queries for a target domain to a different DNS server or an alternate address.
- DNS injection: where some middlebox between the client and resolver intercepts the DNS query and deliberately responds with a forged response bearing an incorrect IP address.

DNS manipulation is popular because it’s easy for ISPs to implement via their existing resolvers.

India

India experiences frequent Internet shutdowns (often local/regional). While many shutdowns are complete network cuts. India alone has recorded 665+ shutdowns since 2012; the highest in the world.

Research shows some Indian ISPs notably the large state-run providers (BSNL and MTNL) have engage in DNS poisoning on the authorities' behest. One study found about 600 DNS resolvers in these networks giving out falsified DNS answers to censor sites.

Other ISPs use techniques like blocking at the HTTP level or deep packet inspection, but DNS tampering remains common.

Implications for ICANN and Internet Governance

DNS-based shutdowns directly impact the infrastructure that ICANN oversees, such as domain name resolution and the stability of the DNS root zone. These disruptions compromise the security, stability, and resilience of the Internet's core systems.

- Threat to DNS Stability: Widespread DNS manipulation by governments can undermine the stability and trust in the global DNS.

- One Internet vs. Fragmentation: If multiple governments alter DNS resolutions (each essentially running a splintered “version” of DNS for their citizens), we risk a fragmentation of the Internet.

- Threats to Human Rights and Democratic Freedom: DNS-based shutdowns can impede access to information, restrict freedom of expression, and hinder the right to peaceful assembly.

- Undermining Multistakeholder Governance Models: Unilateral actions by states to control or manipulate DNS infrastructure without broader consensus challenge this model.

Thank you

Happy to connect on LinkedIn: