

DNS, Conflict & the Noncommercial Internet User

Middle East, War Zones & Digital Rights

Who We're Talking About: Noncommercial Users

*"A journalist in Gaza types a URL. A student in Tehran searches for a textbook.
An activist in Beirut tries to reach their lawyer. For them, DNS is not infrastructure — it is lifeline."*



Journalists & Activists

Rely on open DNS to reach audiences, coordinate, and document abuses



Students & Educators

Need unrestricted access to knowledge, research platforms & tools



Artists & Creators

Publish, collaborate, and reach global audiences via domain names



Civil Society & NGOs

Register domains, serve communities, and communicate with diaspora

These are not edge cases — they are the majority of internet users in conflict-affected societies.

When the Internet Goes Dark

Shutdowns, war & infrastructure collapse across the Middle East

100+

documented internet
shutdowns in Iran since 2019

~80%

drop in Gaza internet traffic
during Israeli ground operations (Cloudflare)

34+

countries globally used
DNS-based censorship in 2024

- ▶ Iran: ongoing shutdown since 2022 — infrastructure weaponized against its own citizens
- ▶ Gaza: physical destruction of telecom infrastructure + deliberate connectivity suppression
- ▶ Sudan, Yemen, Libya: recurring blackouts during military offensives
- ▶ Cloudflare Radar shows real-time BGP route withdrawals & traffic collapse during attacks

DNS as a Tool of Censorship & Control

HOW DNS BLOCKING WORKS IN THE REGION



Methods Used	Targeted Content	Regional Examples
- DNS spoofing / poisoning - NXDOMAIN injection - Resolver hijacking by ISP BGP route manipulation Deep packet inspection + DNS block	- VPN & circumvention tools - Journalism & news sites - Human rights organizations Social media platforms LGBTQ+ community sites	- blocks 50%+ of top sites - religious & political content - news sites during protests VoIP blocking X/YouTube episodic blocks

DNS Under Attack During Conflict

Phishing, spoofing & weaponized DNS targeting civil society

⚠ Threats to Noncommercial Users

Spear-phishing journalists

Fake login pages mimicking secure comms tools, NGO portals

Lookalike domains

Adversaries register similar domains to intercept activists

DNS hijacking

Redirect users to surveillance/malware pages during elections

Election interference

Fake voting info sites hosted on plausible-looking domains

✓ Protective Measures We Can Champion

- DNSSEC deployment & awareness for registrants in conflict zones
- Promote free domain privacy/proxy services for at-risk users
- Partner with EFF, Access Now, Cloudflare Project Galileo for rapid response

Training materials: how to detect spoofed domains & phishing attempts

Push registrars to offer emergency domain locking for at-risk registrants

Privacy, WHOIS & Law Enforcement Access



The Privacy Gap

Many Middle East domain registrants are unaware of proxy/privacy registration services. Their personal data — home addresses, phone numbers, email addresses can appear in public WHOIS.

In authoritarian states, this data can be harvested to identify, locate, and target dissidents, journalists, and civil society organizations.



Law Enforcement Data Access

Law enforcement agencies can formally request registrant data from accredited registrars. ICANN's RDRS (Registration Data Request Service) raises questions:

Are civil society registrants protected? Will requests from authoritarian agencies be fulfilled without due process safeguards?

NCSG Position: Proxy/privacy services must be accessible, affordable, and actively promoted to registrants in high-risk regions.

What can we do?

01

DNS Market Study — Middle East

NCSG requested ICANN commission a DNS market study for the region. Push for inclusion of civil society access, language diversity, and affordability metrics.

02

Human Rights Impact Assessments (HRIA)

Integrate HRIA methodology into DNS Abuse PDP ensuring policy doesn't harm at-risk users especially in conflict zones.

03

Emergency Domain Protections

Develop domain locking / fast-track transfers for civil society registrants under state threat — use support systems like Cloudflare's Project Galileo.

04

Awareness & Capacity Building

Outreach to Middle East registrant communities on WHOIS privacy, human rights issues, phishing defense — in Arabic, Persian, Turkish. Partner with regional digital rights orgs.