Trust and E2EE: Why Weakening End-to-End Encryption Threatens the Global Internet Identifier System

Srijan Rai I NextGen@ICANN

Presented at ICANN 85 -Mumbai

The Invisible Shield

End-to-End Encryption (E2EE) is the bedrock of trust for the DNS. However it is threatened by :-

The Political Challenge

Legislative mandates demanding access to encrypted content

Emerging Technical Challenges

Current AI-driven riskS and upcoming Quantum risks

The Political Challenge #1: Client-Side Scanning

Governments are moving beyond backdoors to Client-Side Scanning (CSS)—scanning content on the device before it is encrypted (Source: arXiv:2110.07450, IETF).

ICANN Relevance – The Dual-DNS Reality

If content is blocked or filtered by local AI agents at the source, Universal Reachability—ICANN's core mission, is affected

- **Case Example:** Under 2026 enforcement of UK's Online Safety Act and EU's Chat Control, registrars in scanning-heavy jurisdictions become liabilities. Users may bypass official DNS for un-monitored "Alternative Roots," fragmenting the global internet.

The Political Challenge #2: Sovereignty & The Splinternet

1

Data Sovereignty

Nations mandate locally-approved cryptographic standards for business

2

Encryption Sovereignty

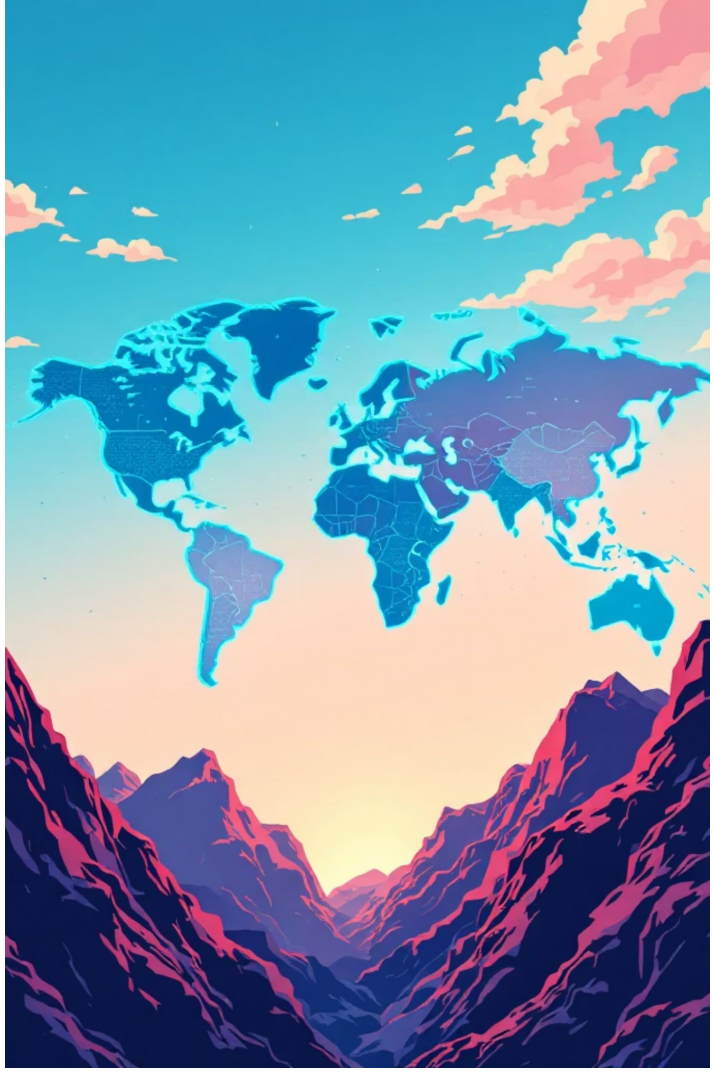
"Secure" in one country becomes "illegal" in another

3

DNSSEC Risk

Compromised Global Chain of Trust

We risk a **Splinternet** where global interoperability becomes a legal impossibility.



Technical Risks #1: The AI "Supercharger"

The Absence of "Human Cost"

Hacking has moved from "high-skill" to "low-cost/automated-infinite" (Radware 2025,Global Threat Analysis Report).

Autonomous Penetration Engines

Enthusiasts use AI to run 10,000 bots scanning for dangling DNS records (Subdomain Hijacking) 24/7

AI Malware in DNS Resolvers

Autonomous bots "live" in resolvers, learning traffic patterns via AI-analysis to redirect high-value queries

Technical Risks #2: AI-Enhanced Metadata Analysis

The Blind Spot

Even with E2EE, AI sees through the shield using Traffic Fingerprinting.

The Mechanism

Analyzing packet sizes and timing to predict activity (Source: Microsoft Research - Whisper Leak, 2025).

The Implication

AI allows governments and larger entities to process intercepted data at a a scale. If the **shape o**f your traffic betrays your content, the End-to-End encryption promise is effectively broken.

Technical Risks #3: Mapping Future Risks: Quantum & HNDL

Today
Adversaries storing up encrypted DNS traffic

1

Future
Quantum "Shor's Algorithm" moment unlocks data

2

Crisis
Historical integrity of DNS chain collapses

3

Harvest Now, Decrypt Later (HNDL)
Adversaries are storing encrypted traffic today for future decryption

Quantum-Vulnerability
Our foundations (RSA/ECC) may turn obsolete against future Quantum computers

DNSSEC & Quantum
If root zone isn't Quantum-Resistant (PQC) soon, it leaves a massive vulnerability for later

Relevance to ICANN

Mission Creep

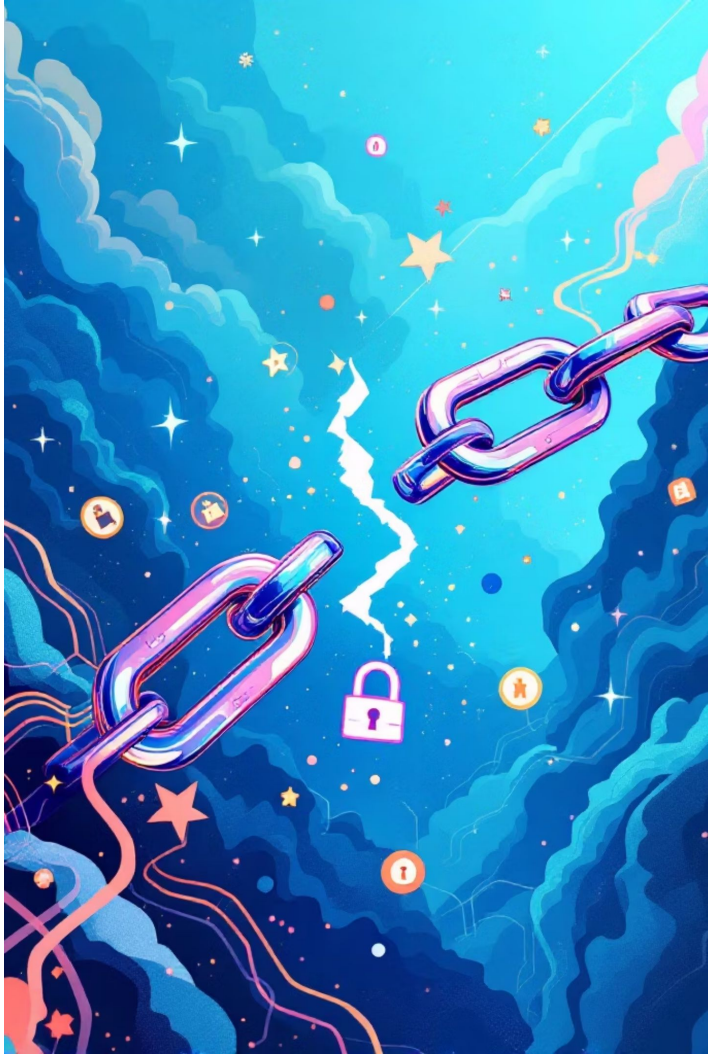
Forcing ICANN-contracted parties to facilitate intercepts politicizes our technical mandate

SSR (Security, Stability, Resiliency)

A backdoor for a good guy is a front door for an adversarial actor or AI bot

The Trust Deficit

If users don't trust the global root, they move to fragmented private networks, diluting ICANN's mission and role



Socio-Technical Solutions: Security Without Exclusion

The 'Security vs. Surveillance' Paradox: When we prioritize security-first without a social lens, we risk creating infrastructure for surveillance.

Example: Client-Side Scanning & Encrypted Client Hello (ECH)

Socio-Technical Solution: Strengthen international legal cooperation for targeted investigations. This allows for law enforcement needs without weakening the encryption shield for the global population.

The Shift: We must move toward Socio-Technical solutions, where the technical implementation is governed by human-centric processes.

Call to Action: Steps to Manage Emerging E2EE Risks

1. Multistakeholder Policy Integration

- Governmental Advisory (GAC) Alignment:
- At-Large Community Mobilization:
- Technical-Political Synergy

2. Technical Resilience & Capacity Building

- Emerging Risk Mapping Unit
- Quantum-Resistant Roadmap
- Hardening Protocols

3. Ecosystem Advocacy & External Engagement

- External Multistakeholderism:
- Youth & Talent Pipelines
- Supporting country level and regional initiatives

Political pressure and emerging technical vulnerabilities threaten E2EE. Vigilance and proactive defense can help preserve digital security.

Q&A

Srijan Rai
Email- srijanrai3@gmail.com