UPDATED EDITION — HUMANITARIAN RELEASE

by Tsvi Arieli

December 2025 — Verified Against Current Ground Truth

This booklet is written for people living under oppression — those who face surveillance, punishment, imprisonment, or violence simply for speaking, thinking, learning, or communicating with the outside world.

It exists for one reason: to reduce harm and help you stay alive and free for as long as possible.

Legal / ethical disclaimer

All techniques described here are strictly for defensive, humanitarian, and educational purposes. They are intended to protect individuals from unjust persecution, not to undermine democratic societies or lawful institutions.

Laws differ by country; nothing here is legal advice. You are responsible for deciding what you do.

Reality disclaimer

No configuration, no tool, no manual can guarantee your safety against a determined state-level adversary.

Technology can close some doors; your behavior and OPSEC (operational security — the discipline of keeping sensitive activities hidden) are more important than any setting.

Treat everything here as risk reduction, never as "100% safe".

CHAPTER 17

HOW OPPRESSIVE SYSTEMS TRACK YOU THROUGH DNS — AND HOW TO STOP THEM

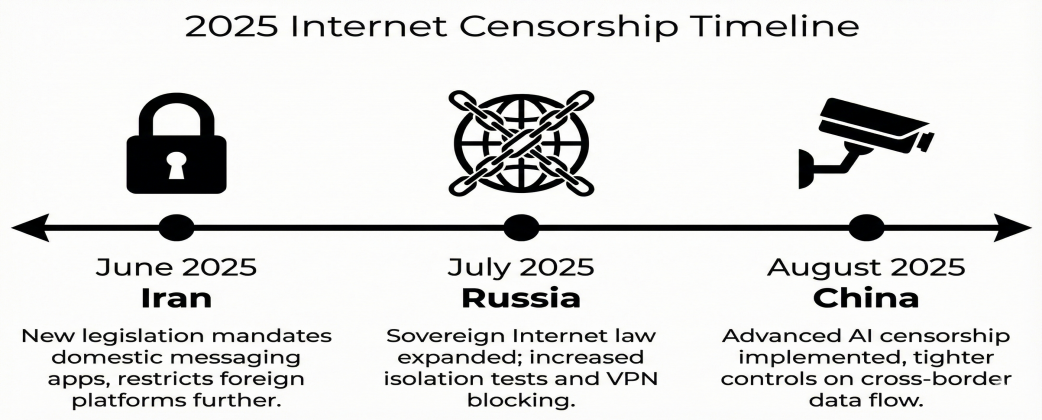
This chapter is written for one purpose:

> *> To stop them from seeing what you do online through DNS, metadata, and protocol leaks — as much as physics and politics allow.*

"They" here means anyone on your network path:

- Your ISP (Internet Service Provider — the company that connects you to the internet) or mobile provider
- WiFi owners (hotel, café, airport, workplace)
- National filtering systems and "lawful intercept" boxes
- Corporate admins and university IT
- Intelligence services and local security police
- Browser vendors doing "helpful" upgrades
- VPNs that silently misconfigure or misuse DNS

You do not choose whether these actors exist. You only choose how much they can see.



What is DNS?

Think of DNS as a phone book for the internet.

When you type "bbc.com", your device asks: "What number (IP address) is this name?" That question travels over the network — usually **in plain text**, visible to anyone watching.

This chapter shows:

- How DNS leaks happen
- How to test them (for real, not fake tests)
- How to close them on each major OS
- How to deal with captive portals (hotel WiFi login pages)
- How Tor, bridges, and VPNs interact with DNS
- Where the limits are

I. DNS Is Not Your Only Leak

Even if you perfectly hide DNS:

- **SNI** (Server Name Indication) usually shows the domain
- **IP addresses** show which network you contact
- **Traffic fingerprints** (size, timing, patterns) identify popular sites
- **Timing correlation** can link your traffic to known destinations
- **Your own mistakes** (logging into real-name accounts) destroy anonymity

What is SNI? When your browser connects to a website, it announces the name of that website during the handshake. This announcement is visible even before encryption starts.

So:

- DNS protection = privacy improvement, not magic invisibility
- For serious anonymity you always need Tor + OPSEC + device separation

Still, fixing DNS is one of the easiest and most impactful moves you can make.

II. SNI, ECH, and What Your ISP Sees Even With "Good DNS"

1. SNI: the domain in clear text

Classic TLS (the encryption protocol that creates the "padlock" in your browser) handshake contains SNI — the domain name you want:

```
You → 104.26.10.10 (Cloudflare IP)
SNI: example.com
```

Your ISP, hotel, or national filter sees:

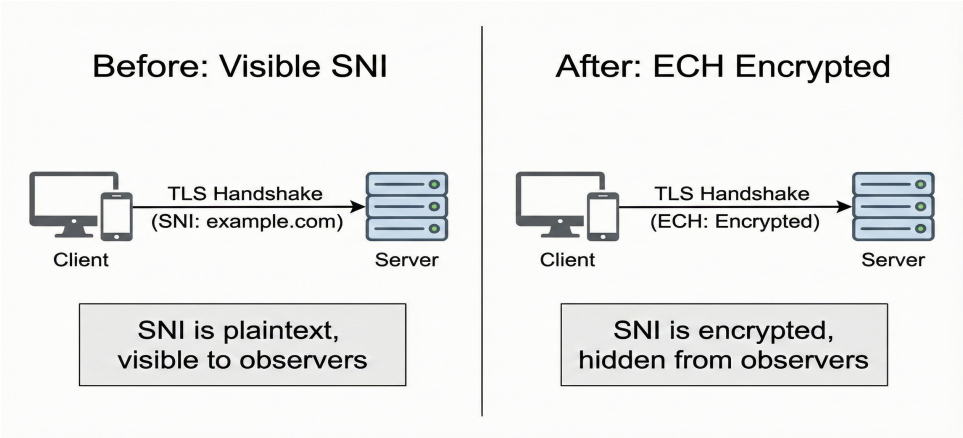
- The IP address
- The exact domain in SNI
- The timing and volume

This happens even if:

- You use DoH / DoT (encrypted DNS — explained below)
- Your VPN is configured "correctly"
- OS DNS is protected
- You disabled all "leak tests"

2. ECH: encrypting the ClientHello

What is ECH? ECH (Encrypted Client Hello) hides the SNI inside an encrypted envelope. Instead of announcing "I want bbc.com" in clear text, your browser encrypts this announcement.



Current reality (December 2025):

- Firefox + Cloudflare: often uses ECH by default in some regions
- Chrome / Edge: slowly rolling out support
- Apple ecosystem: uses it when both server and resolver support it

Then your ISP sees:

```
You → some IP in 104.16.0.0/13
No visible SNI
```

Much better.

3. When ECH silently fails

ECH can fail or be blocked when:

- Captive portals interfere
- Corporate / university firewalls strip or block it
- Your VPN or browser falls back silently

🔴 **CRITICAL: ECH IS BLOCKED IN RUSSIA AND CHINA**

In Russia and China, using ECH is now a trigger for blocking. The Great Firewall (China) and Roskomnadzor's TSPU systems (Russia) inspect the handshake. If ECH is detected, the packet is often DROPPED.

Updated ECH rules by country:

- Western countries: Enable ECH where supported
- **Russia: DISABLE ECH** — detection triggers blocking
- **China: DISABLE ECH** — strictly blocked
- Iran: Test carefully — sometimes works, sometimes blocked

If ECH breaks your connectivity, you are being filtered. Fall back to VPN or Tor immediately.

⚠️ ECH is a privacy tool, not an evasion tool. In hostile regimes, ECH makes you MORE visible, not less.

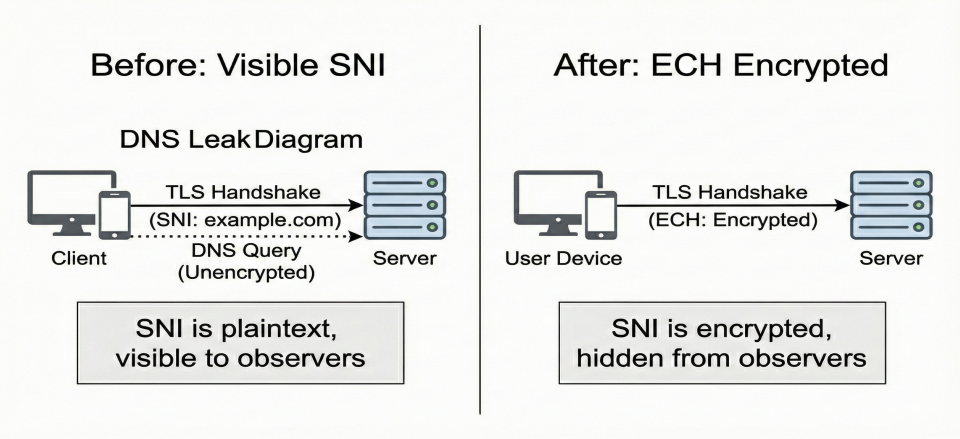
III. The Three DNS Problems You MUST Solve

You have three separate DNS enemies:

1. Plain DNS

- Default UDP/53 lookups through ISP or WiFi owner
- Completely visible, easily logged and filtered

What does this mean? Every time you visit a website, your device asks "where is this site?" using port 53. By default, this question is not encrypted. Anyone on the network can read it.



2. OS-level leaks (even with VPN/DoH/DoT)

- Windows Smart Multi-Homed Name Resolution (Windows asks multiple DNS servers at once — including your ISP)
- IPv6 bypassing VPN (your device uses a different path that VPN doesn't cover)
- systemd-resolved mis-integration (Linux DNS manager not properly connected to VPN)
- Android Private DNS interfering with VPN/Tor
- Apple Private Relay interacting with VPNs

3. App-level leaks

- Apps that use their own DoH servers
- Hardcoded resolvers in SDKs / analytics
- Browsers doing "Secure DNS" outside your VPN
- Corporate clients using custom resolvers

⚠️ Fixing only one of these three = you still leak.

III-A. Android Private DNS Boot Leak

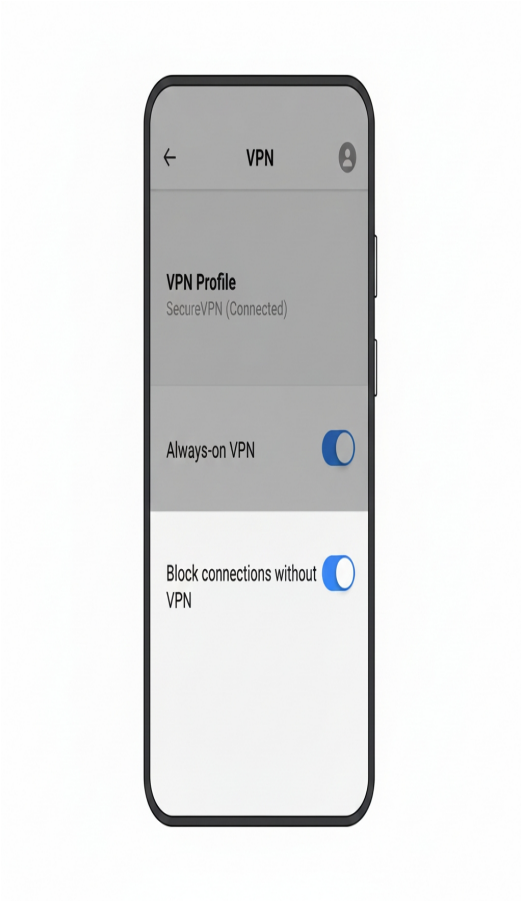
🔴 **CRITICAL: Android sends PLAINTEXT DNS before protection activates**

Android devices send a plaintext DNS query to connectivitycheck.gstatic.com BEFORE the Private DNS tunnel is established.

This happens:

- On every device boot
- On every network switch (WiFi to mobile, etc.)
- Before your VPN connects

Your ISP sees this query EVERY TIME you change networks, even with Private DNS enabled.



Mitigation: Go to:

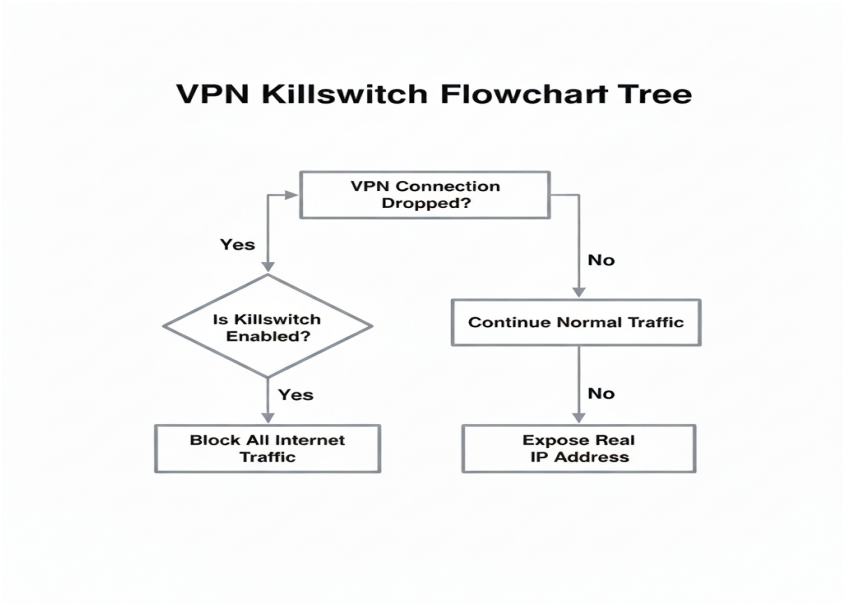
```
Settings → Network → VPN → [Your VPN]
✓ Always-on VPN
✓ Block connections without VPN
```

Do NOT rely on Private DNS alone. The "Block connections without VPN" option prevents any traffic (including boot DNS) from leaving without VPN protection.

IV. DoH vs VPN: When to Disable Browser DoH

What is DoH? DoH (DNS over HTTPS) encrypts your DNS questions inside a regular HTTPS connection. Your ISP cannot easily see which sites you're asking about.

What is DoT? DoT (DNS over TLS) does the same thing, but uses a dedicated encrypted connection instead of HTTPS.



VPN WITH killswitch:

- If VPN drops, all traffic stops
- You want VPN to control DNS, not browser
- → Disable browser DoH (Chrome/Firefox/etc.)
- Prefer OS-level DoH/DoT behind VPN or VPN's own DNS

VPN WITHOUT killswitch:

- If VPN drops, traffic continues → goes to ISP
- DoH in browser can be a fallback shield
- → Keep browser DoH on to avoid plaintext DNS when VPN fails

If you don't know:

1. Check VPN settings for "Kill switch" / "Block internet without VPN"
2. If exists → enable it → then disable browser DoH
3. If doesn't exist → keep DoH as fallback

Always test afterward (section VII).

V. Operating System DNS Behavior Matrix

What the OS tends to do, before you fix anything.

Windows 10/11:

- IPv6 leaks: Yes
- Smart multi-homed resolver: Yes (sends DNS to multiple servers at once — including your ISP)
- Browser DoH overrides system DNS: Yes
- VPN DNS override reliability: Unreliable
- Captive portal breakage risk: High

macOS:

- IPv6 leaks: Sometimes
- Private Relay conflicts with VPNs: Yes
- VPN DNS override reliability: Usually reliable
- Captive portal breakage risk: High

Linux (systemd):

- IPv6 leaks: Common
- systemd-resolved can leak: Yes (see section VII)
- VPN DNS override: Requires integration
- Captive portal breakage risk: Medium

Android:

- IPv6 leaks: Very common
- Private DNS boot leak: Yes (see section III-A)
- VPN DNS override: OEM-dependent
- Captive portal breakage risk: High

iOS:

- IPv6 leaks: Sometimes
- Private Relay conflicts with VPNs: Yes
- Cannot disable IPv6 at OS level
- Captive portal breakage risk: High

This is the baseline. Your job is to override and discipline this behavior.

VI. Captive Portals (Hotel/Airport WiFi) — Safe Workflow

What is a captive portal? The login page that appears when you connect to hotel or airport WiFi.

Captive portals break or interfere with:

- VPNs
- DoH / DoT
- ECH
- Tor connections
- RethinkDNS / firewalls
- Private Relay

If you just "turn things off" and forget to restore them, you stay exposed.

Safe captive portal sequence (minimal exposure):

1. Turn OFF VPN and killswitch temporarily

- Disable "Always-on VPN" / "Block connections without VPN"
- Purpose: allow the login page to appear

2. Temporarily disable encrypted DNS

- Firefox: Settings → Privacy & Security → DNS over HTTPS → Off
- Chrome/Edge: Settings → Privacy & Security → Security → Use secure DNS → Off
- Android: Settings → Network & Internet → Private DNS → Off
- iOS (if you installed a DoH/DoT profile): Settings → General → VPN & Device Management → remove DNS profile

3. Open the captive portal

- Try: http://neverssl.com in browser
- Log in, accept terms
- Do NOT open anything sensitive

4. Immediately re-enable protections

- Turn VPN back ON
- Enable killswitch / Always-on
- Re-enable DoH/DoT / RethinkDNS / ECH if you use them

5. Run DNS leak tests (see next section)

⚠️ Never keep "temporary" settings permanently. Portals are a trap for laziness.

VII. How to Test DNS Leaks (Properly)

1. Browser-level tests (good but incomplete)

Use multiple sites:

- https://browserleaks.com/dns
- https://dnsleaktest.com
- https://ipleak.net

These show which resolvers your browser uses. Limit: they do NOT show non-browser apps, OS-level leaks, or background services.

2. OS-level tests (reality check)

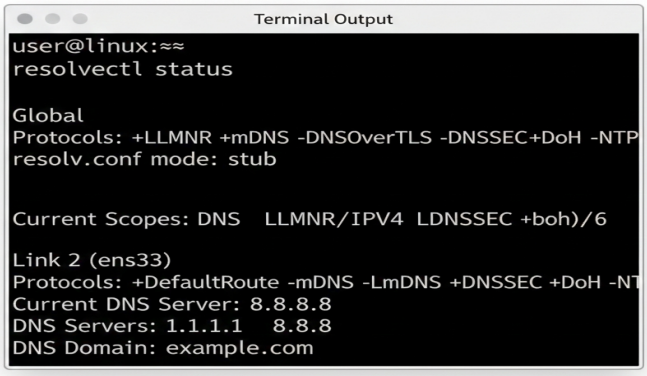
Windows:

```
ipconfig /all
Get-DnsClientServerAddress
nslookup example.com
```

⚠️ nslookup uses its own logic and may query different resolvers than the OS uses. Treat it as one data point, not absolute truth.

Linux (with systemd-resolved):

```
resolvectl status
```



Focus on the VPN interface (usually tun0, wg0):

- Does it show only VPN DNS servers?
- If you still see ISP DNS here → leak

🔴 **CRITICAL: systemd-resolved Split DNS Leak**

Even with a VPN active, systemd-resolved may send DNS queries to BOTH the VPN DNS AND the local router DNS in parallel.

Verification:

```
resolvectl domain
```

Look for your VPN interface. It MUST show:

```
~.
```

(tilde dot)

If the tilde-dot is missing, you are leaking DNS outside the VPN.

Fix:

```
sudo resolvectl domain tun0 "~."
```

Replace tun0 with your VPN interface (wg0 for WireGuard).

macOS:

```
scutil --dns
dscacheutil -q host -a name example.com
```

Android (with Termux):

```
pkg install dnsutils
dig example.com
```

iOS: Use browser tests and VPN app diagnostics.

3. Packet capture (the truth)

Wireshark filter:

```
udp.port == 53 || tcp.port == 53
```

Linux/macOS:

```
sudo tcpdump -i any port 53
```

If you see ANY DNS packets outside the VPN tunnel, you have leaks.

VIII. IPv6 Leaks — Silent Killer

What is IPv6? IPv6 is the newer version of internet addresses. IPv4 looks like 192.168.1.1. IPv6 looks like 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

The problem: Most VPNs only tunnel IPv4. Many ISPs prefer IPv6. Result: your DNS and traffic escape outside the VPN through IPv6.

Fix by OS:

Windows:

Uncheck IPv6 on adapter:

```
Control Panel → Network and Sharing Center →
Change adapter settings → Properties →
Uncheck "Internet Protocol Version 6"
```

macOS:

```
networksetup -setv6off Wi-Fi
networksetup -setv6off Ethernet
```

Linux:

```
sudo sysctl -w net.ipv6.conf.all.disable_ipv6=1
sudo sysctl -w net.ipv6.conf.default.disable_ipv6=1
```

Android: Use VPN with IPv6 support or firewall to block IPv6. Behavior is OEM-dependent.

iOS: Cannot disable IPv6 at OS level. Must use VPN that explicitly supports IPv6.

IX. Tor Browser — Scope and Limits

What is Tor? Tor is a network that routes your traffic through multiple countries (usually 3), making it very difficult to trace back to you. Tor Browser is a modified Firefox that uses this network.

Current version: Tor Browser 15.0.1 (November 11, 2025)

Critical security fixes in this version:

- CVE-2025-13012: Race condition in graphics (High severity)
- CVE-2025-13016: WebAssembly boundary issues (High severity)

⚠️ UPDATE IMMEDIATELY if running an older version. Settings → Help → About Tor Browser → Check for Updates

Tor Browser protects only what goes through it. It does NOT protect:

- Operating system updates and telemetry
- Normal browsers running alongside it
- Messengers and email clients
- Background services and other apps

If something must be anonymous, do it ONLY in Tor Browser and avoid real-name accounts.

X. Tor Exit Nodes and DNS Spoofing

What is an exit node? The last computer in the Tor chain — the one that actually connects to the website you're visiting.

For HTTP (non-HTTPS) sites, exit nodes can:

- Forge DNS replies
- Redirect to phishing pages
- Inject malware

Mitigation:

- Avoid HTTP entirely
- Enable HTTPS-Only Mode in Tor Browser
- Prefer .onion services (websites that exist only inside Tor)
- Verify certificates

XI. SOCKS5 Remote DNS (Tor Outside the Browser)

What is SOCKS5? SOCKS5 is a protocol that lets you tunnel traffic through another computer. Tor uses SOCKS5.

If you tunnel other apps via Tor SOCKS5, enable remote DNS. Otherwise, your OS resolves DNS locally → DNS leak.

Correct pattern with curl:

```
curl --socks5-hostname 127.0.0.1:9050 https://example.com
```

⚠️ Using --socks5 (without -hostname) leaks DNS through your system resolver.

XII. Tor Bridges and Circumvention Under Dictatorships

What is a bridge? A Tor entry point that is not publicly listed. If your country blocks known Tor servers, you need a bridge to enter the Tor network.

General rules:

- Use bridges if default Tor fails or Tor use is incriminating
- Obtain bridges securely
- Never share your bridge list publicly

Bridge types (in order of typical effectiveness):

obfs4 (recommended primary):

- Obfuscates Tor traffic to look like random noise
- Works in most censorship regimes
- Get bridges: bridges.torproject.org or email bridges@torproject.org (from Gmail/Riseup)

WebTunnel (NEW 2025):

- 143+ active bridges globally as of September 2025
- Disguises Tor as regular HTTPS traffic
- Works in Russia but struggles with Iran's whitelist filtering
- Rapidly blocked after deployment; rotate bridges every 30 days

⚠️ Bridges are blocked within days of becoming known. Always have backups.

Snowflake:

- Uses WebRTC through volunteer browsers
- Good fallback when obfs4 fails
- China: Built-in bridges blocked as of August 2025
- Russia: Usable as secondary fallback
- Enable in Tor Browser: Settings → Connection → Snowflake

meek-azure (last resort):

- Routes through Microsoft Azure CDN
- Slowest option but hardest to block
- Use only when other bridges fail

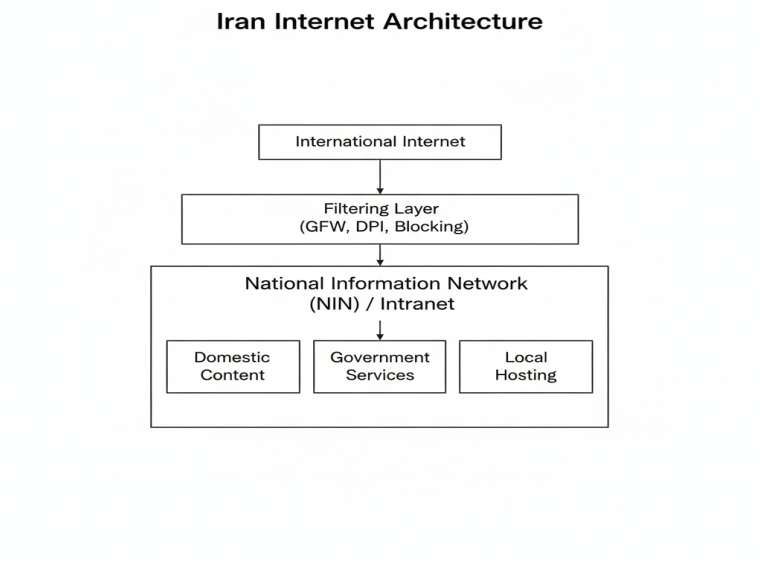
DEPRECATED — Do not use:

- ScrambleSuit: Abandoned since 2013
- Conjure Bridges: No longer active

XII-A. Iran — June 2025 "Stealth Blackout" Infrastructure

🔴 **CRITICAL: Iran has deployed new surveillance infrastructure**

During the June 2025 "Stealth Blackout", Iran revealed new systems:



1. National Information Network (NIN):

- Separate from global internet
- Government can isolate Iran completely
- Some services only available on NIN

2. Protocol Whitelisting:

- ONLY allowed: DNS, TLS, HTTP on specific ports
- SSH: Throttled to unusable speeds
- Unknown protocols: BLOCKED by default

3. Verified Identity System:

- All internet activity linked to national ID
- SIM cards require biometric verification
- Assume EVERYTHING is attributed to you personally

What works in Iran (December 2025):

- **Psiphon** — PROVEN: 1.5 million users during June 2025 shutdown
- obfs4 bridges — require frequent rotation
- "Fragmented" Client Hello tools

What does NOT work:

- Direct Tor connection
- Standard VPNs without obfuscation
- Snowflake (limited effectiveness)

Patterns indicating you are being monitored:

- Connection becomes very slow but doesn't fail completely
- Specific sites slow while others work normally
- Connection works, then fails at same time daily
- Your VPN works, your neighbor's same VPN doesn't (targeted)

⚠️ IF YOU NOTICE THESE PATTERNS → You are flagged. Switch methods immediately.

XII-B. Russia — July 2025 Legal Changes and Technical Blocking

🔴 CRITICAL: New VPN/Tor law signed July 31, 2025

Law provisions (effective September 1, 2025):

- Fines for searching "extremist" content via VPN: 3,000-5,000 rubles
- VPN advertising penalties: 50,000-500,000 rubles
- Repeat violations: up to 1,000,000 rubles
- VPN providers must connect to Russian registry and filter prohibited content

Important nuance: Using VPN itself is NOT yet criminal. However, VPN use serves as "aggravating circumstance" in other charges. Penalty only applies if proven accessing prohibited content.

Technical blocking:

- SORM systems log all traffic at ISP level
- Roskomnadzor blocks known Tor nodes and VPN servers
- DPI detects standard VPN protocols (WireGuard, OpenVPN)
- ECH is actively blocked

What works in Russia (December 2025):

- obfs4 bridges — primary method, but increasingly blocked by DPI
- WebTunnel — effective, requires private bridges on non-standard ports
- Shadowsocks-2022
- VLESS with Reality
- AmneziaWG (obfuscated WireGuard)

Operational security:

- Don't discuss VPN use on Russian platforms (VK, OK, Telegram)
- Don't access obviously "extremist" sites via Russian IP
- Assume all VPN usage is logged by ISP via SORM
- Use separate device for sensitive activity

XII-C. China — Great Firewall Updates

GFW operates differently from other censorship:

1. Active Probing: GFW connects TO your VPN/proxy to verify it's a circumvention tool. If confirmed → IP blocked within minutes.

2. Protocol Fingerprinting:

- OpenVPN: DETECTED and blocked
- WireGuard: DETECTED and blocked
- Standard HTTPS VPN: Often detected
- Tor (even with simple bridges): Frequently blocked

3. Machine Learning Detection: Traffic patterns analyzed in real-time. Even encrypted traffic can be classified by timing/size patterns.

What works in China (December 2025):

- VLESS + Reality (self-hosted, mimics real websites)
- Hysteria2
- Tor with meek-azure (slow but works)
- Shadowsocks with AEAD obfuscation

What does NOT work:

- Most consumer VPN apps without obfuscation
- OpenVPN protocol
- WireGuard protocol
- Direct Tor connection
- Snowflake (built-in bridges blocked August 2025)

Preparation before entering China:

- Download all tools before arrival (GitHub blocked in China)
- Set up Shadowsocks/V2Ray/VLESS server or obtain from trusted provider
- Have multiple fallback methods configured
- Assume hotel WiFi is fully monitored

XII-D. Psiphon — Proven Tool for Iran

What is Psiphon? Psiphon is a multi-protocol circumvention tool. It automatically tries different methods (TCP, SSH, HTTP, DNS-prefix) to find one that works.

During Iran's June 2025 "Stealth Blackout":

- 1.5 MILLION Iranians used Psiphon at peak
- 330+ terabytes of data transferred
- Outperformed Tor, Snowflake, and most VPNs

Why Psiphon works:

- Multi-protocol design
- Exploits "holes" left open for government services
- Adapts to blocking in real-time

Download BEFORE you need it:

- Android: APK from psiphon.ca (not Play Store in Iran)
- Windows/macOS: psiphon.ca
- iOS: Limited availability — use VPN instead

⚠️ Psiphon provides ACCESS. Tor provides ANONYMITY. Use Psiphon as complement to Tor, not replacement.

XIII. RethinkDNS — Power, Bugs, and When to Trust It

What is RethinkDNS? An Android app that acts as a local firewall + DNS manager. It can block trackers, ads, and control which apps can access the internet.

Current version: v0.5.5 series (v0.55p/q as of September 2025)

🔴 **CRITICAL: Stability has DEGRADED in 2025**

Known issues on Android 13-15:

- Installation failures via direct APK; requires F-Droid Client
- Connectivity issues: apps show active sessions but no internet
- Background crashes when using heavy apps
- Service stops silently; accessibility permissions break
- VPN engine stalls
- IPv6 leaks confirmed
- Always-On VPN conflicts

Use RethinkDNS only when:

- You use stable F-Droid builds, not sideloaded APKs
- You test after EVERY reboot
- You combine with VPN killswitch as backup
- You do NOT rely on it for life-critical anonymity

⚠️ For high-risk scenarios: Do NOT use RethinkDNS as sole protection.

XIV. Verifying What DNS Your VPN Really Uses

Most VPNs say "we use our own secure DNS". Some lie, many oversimplify.

Step 1 — Look into the VPN config

Open your .ovpn or WireGuard config. Look for lines like:

```
dhcp-option DNS 10.8.0.1
```

This means VPN pushes internal DNS (good).

If you see:

```
dhcp-option DNS 8.8.8.8
dhcp-option DNS 1.1.1.1
```

Then your VPN forwards to Google/Cloudflare. That may still be better than ISP (especially in Iran/Russia) — but you should know.

Step 2 — Watch DNS packets from VPN interface

Linux example (OpenVPN on tun0):

```
sudo tcpdump -i tun0 port 53
```

- If you see DNS going inside tun0 → good
- If you see DNS from wlan0 / eth0 instead → leak

For WireGuard (often wg0):

```
sudo tcpdump -i wg0 port 53
```

Step 3 — Confirm who actually answers

```
dig txt o-o.myaddr.l.google.com @RESOLVER_IP
dig +short txt whoami.ds.akahelp.net
```

These reveal the IP your DNS query originates from.

XV. Machine Learning Traffic Detection (New Threat)

🔴 CRITICAL: DPI has evolved beyond signature matching

Traditional DPI looked for signatures in packets. ML-Based DPI (deployed 2024-2025) analyzes PATTERNS in encrypted traffic.

Even without seeing content, ML can detect:

- Tor usage (65%+ accuracy)
- VPN protocols by traffic patterns
- Circumvention tool signatures
- Anomalous encrypted traffic behavior

Detection methods deployed:

- Packet flow analysis (timing, size patterns)
- TLS handshake fingerprinting
- Active probing (sending probe traffic, analyzing responses)
- Behavioral heuristics

Implication: Encryption alone no longer protects you. You need OBFUSCATION that mimics normal traffic.

Recommended obfuscation tools:

- obfs4 — randomizes traffic patterns

- VLESS + Reality — mimics connections to real websites
- Psiphon — multi-protocol adaptation
- AmneziaWG — obfuscated WireGuard

XVI. Resolver Choice and Fingerprinting

Paradox: Using very rare resolvers makes you less predictable to ISP, but more unique to global observers.

Guideline:

- For privacy from local ISP / regime: popular public resolvers (Google 8.8.8.8 / Cloudflare 1.1.1.1 / Quad9 9.9.9.9) can be safer than exotic ones
- For high-end anonymity: you should be on Tor anyway

⚠️ Quad9's "Swiss jurisdiction" protection is weakened by German, French, and Italian legal orders (2024-2025).

XVII. When They Block Your DNS

Typical blocks:

- Port 853 (DoT) blocked
- Known DoH IPs (Cloudflare 1.1.1.1, Google, Quad9) blocked
- VPN protocols blocked or throttled
- Sometimes ECH fingerprints blocked

Fallback strategy:

4. Try DoH on different providers (some networks only block the usual ones)
5. Try VPNs with obfuscation / stealth modes ("Stunnel", "obfsproxy", "Stealth VPN")
6. Try Tor with Snowflake or meek bridges
7. Last resort: plaintext DNS — only for short time, to bootstrap VPN/Tor, then re-enable protections

XVIII. System Time Skew — Why Everything Suddenly Breaks

What happens with wrong clock:

- HTTPS certificates fail
- DoH/DoT connections fail
- VPN connections may fail
- Only plain DNS "magically works" → dangerous temptation

Fix time before you assume censorship.

Linux (systemd):

```
sudo timedatectl set-ntp true
timedatectl status
```

Check that NTP service: active

On systems using chrony:

```
sudo chronyc makestep
chronyc tracking
```

⚠️ ntpdate is DEPRECATED and not installed on modern distributions (Ubuntu 24.04+, Fedora 41+, Debian 12+).

Windows:

```
w32tm /resync
```

Or: Settings → Time & Language → Date & Time → Set time automatically

macOS:

```
sudo sntp -sS time.apple.com
```

Android / iOS: Enable "Set time automatically" / "Use network-provided time"

XIX. Threat Models: Who Are "They" in Practice?

You are usually dealing with some combination of:

1. Local adversary

Café WiFi owner, hotel, shared apartment. Goal: sniff, steal accounts, petty control.

2. ISP + infrastructure

Logs sites visited, sells data, obeys local orders. In authoritarian states: first layer of surveillance.

3. National filtering / censorship

Country-wide DNS poisoning, blocking Tor/VPN endpoints, traffic shaping and throttling.

4. Targeted surveillance

You personally are of interest (activist, journalist, dissident). They correlate timing, purchase logs, phone records, real-world informants.

This chapter reduces visibility for 1–3.

Against 4, it is necessary but not sufficient; you also need: behavior discipline, minimal exposure online, physical safety planning.

XX. Privacy vs Anonymity — What DNS Can and Cannot Do

Privacy:

- Hiding what you read from your ISP or WiFi owner
- Avoiding injection/spoofing of fake pages
- Making surveillance more expensive

Anonymity:

- Hiding who you are
- Preventing your actions from being linked to your real identity
- Surviving targeted investigations

DNS defenses mostly give privacy.

They do NOT:

- Hide SNI (unless ECH works)
- Stop global timing analysis
- Protect you if you log into real-name accounts

For anonymity you need: Tor (properly used), device separation, long-term OPSEC (not mixing identities).

XXI. Minimum Safe Configuration Checklist

If your risk is non-trivial, at minimum:

8. **Fix IPv6 leaks** — Disable IPv6 where possible, or use VPN with proper IPv6 support
9. **Use a VPN with killswitch** — "Block internet without VPN" enabled
10. **Disable browser DoH if VPN has killswitch** — Let VPN control DNS
11. **If VPN has no killswitch, keep browser DoH as fallback**
12. **Android: Enable "Block connections without VPN"**
13. **Linux: Verify systemd-resolved has ~. on VPN interface**
14. **Prefer mainstream public resolvers over ISP DNS** — Especially in hostile regimes
15. **Test DNS leaks after every major change** — New WiFi, new SIM, new VPN, new OS version
16. **Handle captive portals carefully** — Short exposure, then restore protections and test
17. **Use Tor Browser isolated from identity** — No real-name accounts through Tor
18. **Use bridges in Iran/Russia/China** — Prefer obfs4
19. **Russia/China: DISABLE ECH** — It triggers blocking
20. **Iran: Consider Psiphon as primary access tool**
21. **Assume tools fail silently** — Verify, verify, verify

XXII. Summary

They see you through:

- DNS
- SNI
- Traffic patterns
- Your own mistakes

This chapter gives you:

- Concrete commands
- Detection methods (not just pretty tests)
- Fallback strategies
- OS-specific fixes
- Tor and bridge guidance for the hardest environments
- Current tool status (December 2025)
- Legal updates

You cannot make yourself impossible to track.

You can make yourself much harder and more expensive to track — and sometimes that is the difference between being an easy target and being left alone a little longer.

That extra time and safety is the entire point.

— END OF CHAPTER 17 —

Verified and updated: December 1, 2025

This guide is free. Share it. Translate it. Save lives.