

Great Firewall of China: Technical History, Censorship Mechanisms, Cases, Data and Circumvention

Research framework on network censorship, measurement, cases, countermeasures and reproducibility

Research status	Living Research / Frozen PDF Snapshot
Version	v2026.09.18.1
Publication date	September 18, 2026
Canonical web edition	https://freechina.live/english/great-firewall-china-technical-history-censorship-mechanisms-cases-data-circumvention/
Publisher	Free China Movement
Citation	Free China Movement, Great Firewall of China: Technical History, Censorship Mechanisms, Cases, Data and Circumvention, v2026.09.18.1, September 18, 2026.

Version-control note: this PDF is an immutable snapshot of the living web research page. Later substantive revisions receive a new version identifier; prior PDFs remain available in the web page's version history.

Executive Summary

The Great Firewall of China (GFW) is best understood as a family of network-level filtering and interference capabilities rather than a single appliance. This report separates network censorship from platform censorship, search suppression, account/identity rules, provider-held data, app-distribution controls, criminal enforcement and AI-service restrictions.

The research framework connects historical policy and infrastructure changes with named cases, measured mechanisms, countermeasure families, datasets and a reproducible test protocol. A technical observation should not by itself be converted into a claim about institutional motive, nationwide scope or a hidden implementation layer.

1. Scope: what counts as GFW evidence

- Network-layer evidence: DNS injection/poisoning, IP blocking, forged TCP resets, HTTP filtering, TLS/SNI interference, traffic fingerprinting, active probing and traffic injection.
- Platform-layer evidence: WeChat keyword filtering, search-result suppression, account deletion or geo-restriction. These are related to information control but are not, by themselves, GFW packet filtering.
- Identity/data evidence: real-name systems, subscriber records, IP/account metadata and provider data disclosure.
- AI/service evidence: model refusals, retrieval behavior, moderation or routing. A model refusal can occur over a fully functioning network connection.

2. Historical Development

1990s-2000: network expansion and national regulation

As commercial and academic internet access expanded, internet regulation became more formalized. The 2000 Internet Information Services Measures created a nationwide regulatory framework for internet information services. The policy layer should be studied alongside, but not confused with, the technical filtering layer.

Early 2000s: measurable DNS and connection interference

Technical studies documented forged DNS responses, keyword-triggered interference and injected TCP reset packets. A destination server can be healthy while a user's connection fails because interference occurs along the network path.

2004-2005: Shi Tao / 师涛 and the firewall-only fallacy

The Shi Tao case illustrates another layer: provider-held account and IP-related information was cited in prosecution evidence, according to CPJ. Network filtering, metadata, provider records and criminal enforcement must therefore be tracked separately.

2010: Google.cn

Google announced that it stopped censoring Google Search, Google News and Google Images on Google.cn and shifted users toward its Hong Kong service. The episode demonstrates the distinction between provider self-censorship, licensing pressure and network-level access restrictions.

2013: GitHub

GreatFire documented a period in which GitHub access was disrupted through multiple mechanisms, including connection resets and DNS poisoning. This case underlines the project's core rule: 'blocked' is not a sufficient technical description.

2014: LINE and KakaoTalk

Citizen Lab documented DNS tampering and HTTP request filtering affecting messaging services, with additional DNS interference affecting other services.

2015: Great Cannon

Citizen Lab described the Great Cannon as separate from but co-located with the Great Firewall. Its analysis showed traffic injection used in large-scale attacks against GreatFire-related infrastructure, extending the research model from traffic denial to traffic manipulation.

2016-2017: WeChat as a platform-layer contrast

Citizen Lab documented server-side, account-scoped and sometimes silent WeChat keyword censorship. The case is analytically useful because it is a platform control rather than direct GFW packet filtering.

2017: cross-border connectivity and VPN-market regulation

MIIT's 2017 internet-access market campaign restricted unauthorized provision of cross-border dedicated-line and VPN-related telecom services. This is a regulatory response affecting the circumvention ecosystem rather than a packet-filtering technique.

2020-2021: GFWatch

Citizen Lab's GFWatch used large-scale longitudinal DNS testing and reported more than 300,000 censored domains in its 2020 measurement period, with substantial pattern-driven overblocking and forged DNS responses that could leak into public resolver and archival datasets.

2022-2023: search censorship and measurement-tool blocking

Citizen Lab identified more than 60,000 unique search-censorship rules across eight China-accessible platforms. Separately, OONI reported that from July 7, 2023 its infrastructure was blocked through DNS injection and TLS interference, with backend services additionally affected by DNS tampering, TLS interference and IP blocking.

2023: F-Droid

OONI measurements attributed the blocking of the F-Droid open-source Android repository to DNS injection returning unrelated addresses.

2026: AI controls are a different layer

Free China Movement's DeepSeek black-box audit documented content-sensitive response differences. Those observations concern AI-service behavior, not the GFW itself, and remain a separate field in the research model.

3. Technical Mechanism Matrix

Mechanism	Observed behavior	Typical symptom	Evidence family
DNS injection / poisoning	Forged DNS replies return incorrect or unrelated addresses	Domain resolves to false IPs or inconsistent answers	GFWatch, OONI, GitHub/F-Droid
IP blocking	Packets to selected destinations are dropped or rejected	Correct DNS but destination remains unreachable	OONI network tests
Forged TCP reset	Injected RST packets terminate sessions	Connection closes immediately after trigger	Citizen Lab GFW/Great Cannon work
HTTP request filtering	Plaintext requests inspected for host/path/keywords	Some URLs fail while same service remains reachable	Messaging/GitHub historical tests
TLS/SNI interference	TLS handshake or exposed hostname is disrupted	HTTPS fails before content loads	OONI China measurements
Active probing	Suspected circumvention endpoints are contacted to classify them	Bridges/proxies become blocked after discovery	Tor anti-censorship research
Traffic fingerprinting	Encrypted patterns are classified without reading plaintext	Specific protocols fail despite encryption	Tor and censorship research
Traffic injection	Network system injects or redirects traffic	Browsers can be induced to send attack/redirect traffic	Great Cannon 2015

4. Historical Countermeasure Matrix

Method	Purpose	Main limitation / response
HTTPS	Protects page content and URL paths in transit	Does not necessarily hide destination IP or hostname; TLS can be interfered with

Method	Purpose	Main limitation / response
VPN / encrypted proxy	Tunnels traffic to an external server	Endpoints/protocols can be blocked or fingerprinted; provision is regulated
Tor bridges	Uses non-public relays when public Tor is blocked	Bridges can be enumerated or discovered
obfs4	Obfuscates Tor traffic and resists active scanning	Bridge distribution remains an arms race
Snowflake	Uses short-lived volunteer proxies	Connectivity and performance vary
WebTunnel	Makes traffic resemble ordinary HTTPS	Effectiveness changes as detection changes
Mirror / overseas hosting	Replicates content outside domestic hosting controls	Mirrors can be enumerated and blocked
Email / newsletters	Distributes content outside one web endpoint	Filtering and metadata exposure remain possible
Distributed archives	Preserves deleted material	Repositories can themselves be blocked
Censorship measurement	Documents mechanism and scope empirically	Measurement infrastructure may itself be targeted

5. Research Data Sources

Dataset / project	Primary use	Strength	Limitation
OONI Explorer	Network measurements from real probes	Open, protocol-specific observations	Coverage varies by network, time and participation
GFWatch	Large-scale DNS monitoring	Longitudinal, high-volume testing	Focused primarily on DNS
GreatFire Analyzer	Historical China accessibility testing	Long-running China-specific archive	Individual URLs can have sparse coverage
Citizen Lab	Technical/platform censorship research	Controlled experiments and methodological detail	Studies are time/service specific
Tor Project / Metrics	Tor reachability and anti-censorship work	Protocol-specific operational expertise	Does not measure all censorship

6. Reproducible GFW Measurement Schema

Required row fields: Date/time | test location/network/ASN | domain/IP | protocol | DNS result | TCP result | TLS result | HTTP/application result | control destination | suspected mechanism | packet capture or screenshot | measurement URL | repeat count | independent corroboration | policy/case relation | countermeasure tested | outcome | confidence.

- Use a control destination on the same protocol whenever possible.
- Repeat tests across multiple networks and times before describing a service as blocked nationwide.
- Separate DNS failure, IP reachability, TLS failure and application-layer filtering.
- Do not infer institutional motive from a packet trace alone.
- Preserve primary evidence and exact timestamps.
- Record intermittent outcomes as intermittent instead of forcing a binary blocked/unblocked label.

7. Sensitive-Information Rule

Technical censorship research can create risk for probe operators and circumvention infrastructure. Public reporting should minimize unnecessary personal identifiers, live credentials, private bridge addresses, unpublished family data and other operational information that could expose individuals or infrastructure.

8. Selected References

- Citizen Lab. China's Great Cannon (2015).

- Citizen Lab. GFWatch: A Longitudinal Measurement Platform Built to Monitor China's DNS Censorship at Scale.
- Citizen Lab. Missing Links: A Comparison of Search Censorship in China (2023).
- OONI. China started blocking OONI (2023).
- Tor Project. Censorship circumvention documentation and bridge/pluggable-transport guidance.
- Free China Movement. Shi Tao / 师涛 profile.
- Free China Movement. DeepSeek Black-Box Audit (2026).