TSPU: Russia’s Decentralized Censorship System

Diwen Xue, Benjamin Mixon-Baca*, ValdikSS*, Anna Ablove, Beau Kujath†, Jedidiah R. Crandall†, Roya Ensafi

University of Michigan, †ASU/Breakpointing Bad, *Independent
**The day the news died** Here are all Russia’s independent media outlets banned, blocked, or shuttered in just the past few days

12:49 am, March 5, 2022 · Source: Meduza

---

**Russia blocks access to Facebook and Twitter**

---

**Russian Internet Takes a Hit as Cogent Cuts Off Its Backbone Network**

A major internet service provider’s disconnection is a new step toward the “splinternet” that adds fragmentation to the global communication network.

---

**Russia’s Internet Censorship Machine Is Going After Tor**

The attempt to block the site, which helps users mask their online activity, is the latest in the country’s efforts to control the internet.

---

**Russia is blocking more and more VPNs**

By Anthony Spadafora published 23 days ago

---

**Over 600 Companies Have Withdrawn from Russia — But Some Remain**

April 14, 2022

---

**BBC, CNN and other global news outlets suspend reporting in Russia**

---

**TikTok created an alternate universe just for Russia**

The Chinese-owned social media giant weathered Putin’s information crackdown by muzzling its users there and cutting them off from the outside world, while allowing state propaganda
Internet Censorship

How Great is the Great Firewall? Measuring China's DNS Censorship

Internet shutdowns in 2021: the return of digital authoritarianism

A WEB OF IMPUNITY

The killings Iran’s internet shutdown hid
Censorship in Russia: 139-FZ

- 139-FZ “Blocklist Law” was signed in 2012.
- Roskomnadzor, federal agency on media and communication, maintains “the Registry of Blocking Sites”.
  - IP, subnets, domain names.
  - ISPs are required to block websites from the list.

July, 2012
Law 139-FZ signed, implemented as “Blocking Registry”

April, 2019
Decentralized Control: A case study of Russia

November, 2019
“RuNet” law came into force, requiring installation of “special equipment”.

2019 – 2020
ISPs received letters from RKN. DPI testing began in rural area.

2021-2022
Uniform censorship across ISPs, “out-of-registry” blocking.

March, 2021
The Twitter Throttling incident.
Censorship in Russia: “Decentralized Control”

- Blocking Registry grows to 132K domains and 324K IP addresses (2019).
- Significant differences in both types and amount of blocking between ISPs.

---

July, 2012
Law 139-FZ signed, implemented as “Blocking Registry”

April, 2019
Decentralized Control: A case study of Russia

November, 2019
“RuNet” law came into force, requiring installation of “special equipment”.

2019 – 2020
ISPs received letters from RKN. DPI testing began in rural area.

2021-2022
Uniform censorship across ISPs, “out-registry” blocking.

March, 2021
The Twitter Throttling incident.
Censorship in Russia: RuNet

- Appoints Roskomnadzor to guard the “stability, security, and integrity” of Russia’s Internet.
- Provides legal grounds for the government to require ISPs to install “special equipment”.

The President signed the law on sustainable Runet

Vladimir Putin signed on Wednesday the federal law "On Amendments to the Federal Law "On Communications" and the federal law "On Information, Information Technologies and Information Protection," Kremlin.ru reports.

This is the so-called law on the sustainability of the Runet, according to which a national Internet traffic routing system will be created in the country in order to ensure the reliable operation of the Runet.

July, 2012
Law 139-FZ signed, implemented as “Blocking Registry”

April, 2019
Decentralized Control: A case study of Russia

Novemlber, 2019
“RuNet” law came into force, requiring installation of “special equipment”.

2019 – 2020
ISPs received letters from RKN. DPI testing began in rural area.

2021-2022
Uniform censorship across ISPs, “out-registry” blocking.

March, 2021
The Twitter Throttling incident.
Leaked Installation Guide on TSPU

https://habr.com/ru/post/459894/

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Law 139–FZ signed, implemented as “Blocking Registry”</td>
<td>Decentralized Control: A case study of Russia</td>
<td>“RuNet” law came into force, requiring installation of “special equipment”.</td>
<td>ISPs received letters from RKN. DPI testing began in rural area.</td>
<td>Uniform censorship across ISPs, “out-registry” blocking.</td>
<td>The Twitter Throttling incident.</td>
</tr>
</tbody>
</table>
Censorship in Russia: RuNet

- Users report on blocked resources that were *not* present in the blocking registry (out-registry blocking).

- Plus, measurement studies suggest *temporal and geographic uniformity.*
Censorship in Russia: Twitter Throttling

- Identical throttling behaviors were observed from vantage points across ISPs.
- Parliament member acknowledged that new DPI devices had been installed in major ISPs, which were used for throttling.

A new system was put into use!

- July, 2012: Law 139-FZ signed, implemented as “Blocking Registry”
- April, 2019: Decentralized Control: A case study of Russia
- November, 2019: “RuNet” law came into force, requiring installation of “special equipment”.
- 2019 - 2020: ISPs received letters from RKN. DPI testing began in rural area.
- 2021-2022: Uniform censorship across ISPs, “out-registry” blocking.
- March, 2021: The Twitter Throttling incident.

[1] Throttling Twitter: An Emerging Censorship Technique in Russia. IMC '21
Censorship in Russia: Twitter Throttling

July, 2012
Law 139-FZ signed, implemented as “Blocking Registry”

April, 2019
Decentralized Control: A case study of Russia

November, 2019
“RuNet” law came into force, requiring installation of “special equipment”.

2019 - 2020
ISPs received letters from RKN. DPI testing began in rural area.

2021-2022
Uniform censorship across ISPs, “out-registry” blocking.

March, 2021
The Twitter Throttling incident.

These events...

➔ marked a departure from Russia’s previous censorship model.

➔ suggest the deployment of an emerging system that enforces censorship uniformly across Russia in real-time, without relying on ISP’s technical capabilities or blocking registry.
But very little is known about its **design**, **capability**, or **the extent of its deployment**.

A better understanding of the TSPU is needed, as the model can be adopted by other countries with similar networks.
TSPU
технические средства противодействия угрозам
(Technical Measures to Combat Threats)

Centrally controlled by RKN, Decentrally deployed in ISP networks.
Measurement Setup & Challenges

A. Acquiring Vantage Points.

B. Distinguishing TSPU and ISP Censorship.

C. Adopting remote measurements due to the asymmetricity of TSPU censorship.
Understanding TSPU

1. **How:** Discover how TSPU tracks and blocks a connection.

2. **What:** Identify what resources are targeted by TSPU.

3. **Where:** Detect and Position TSPU devices w.r.t Russian users.
Identify TSPU Blocking: QUIC, IP, SNI-based

- Uniformity in blocking behaviors across ISPs.
- Consistency in blocking targets across ISPs.
- Co-location of different TSPU blocking mechanisms.

Example: SNI-based Blocking
TSPU Blocking: In-path

- In-path devices as TSPU modifies or drops packets to block connections.
Each blocking mechanism requires either dropping or modifying packets, suggesting in-path positions. Being in-path, TSPU has more means to interfere with users’ traffic, compared to on-path systems (e.g., GFW)
TSPU Blocking: Stateful

- Censorship Triggers.
- Degree of Statefulness
- State Timeouts
- Triggering Reliability

⇒ Refer to the paper
Understanding TSPU

1. **How:** Discover how TSPU tracks and blocks a connection.

2. **What:** Identify what resources are targeted by TSPU.

3. **Where:** Detect and Position TSPU devices w.r.t Russian users.
What Does TSPU Block?

Domain lists for testing

- **Tranco List:**
  - 10,000 Top domains.
  - Augmented with *Citizen Lab Global Blocklist*

- **Registry List:**
  - 10,000 domains from *Blocking Registry*.
  - Sampled from domains added after Jan 1, 2022
What Does TSPU Block?

Classifying Blocked Domains (n=9866)

- Topic modeling by clustering received HTMLs from control.
- “Informative media” are heavily targeted.
  - Blogs, news, social media
Understanding TSPU

1. **How:** Discover how TSPU tracks and blocks a connection.

2. **What:** Identify what resources are targeted by TSPU.

3. **Where:** Detect and Position TSPU devices w.r.t Russian users.
Local TTL Measurement

TSPUs are close to end-users.
Detect & Locate TSPU

Local Measurement
TTL-based measurements from in-country vantage points.
- Limited scale

Remote Measurement
Problem: TSPU censorship is not symmetric (RU→US only)
- ECHO + Asymmetric Routing
  - (refer to the paper)
- IP Fragmentation Characteristics
TSPU: IP Fragmentation Behaviors

- How TSPU handles fragmentation:
  - Buffers fragments
  - Forward Individually
  - Overwrite TTL (Time-To-Live)
  - Drop Duplicates (non-RFC)
  - Maximum 45 fragments.
TSPU: IP Fragmentation Behaviors

- How TSPU handles fragmentation
  - Buffers fragments
  - Forward Individually
  - Overwrite TTL (Time-To-Live)
  - Drop Duplicates (non-RFC)
  - Maximum 45 fragments.
Large-scale Scanning for TSPU
➔ 1.013M/4.005M (25.31%) traceroutes suggest TSPU.
  ◆ 6,871 unique TSPU devices

➔ TSPUs are within two hops away in over 70% cases.

➔ Location and the substantial number of deployments suggest a different approach from the GFW.
Large-scale Scanning for TSPU

- TSPUs installed in upstream ISPs.
  - The TSPU law explicitly allows downstream ISPs to rely on upstream providers for compliance.
Takeaway

● Our study found pervasive deployment of TSPU devices in Russia.

● TSPU empowers RU government to *unilaterally* control the Internet.
Takeaway

● Our study found pervasive deployment of TSPU devices in Russia.
● TSPU empowers RU government to unilaterally control the Internet.
● In-path and close to edges, TSPU can launch attacks beyond censorship. (e.g., MITM, targeted surveillance)
Takeaway

● Our study found pervasive deployment of TSPU devices in Russia.

● TSPU empowers RU government to unilaterally control the Internet.

● In-path and close to edges, TSPU can launch attacks beyond censorship. (e.g., MITM, targeted surveillance)

● Decentralized deployment, centralized control.
  ○ May become a blueprint for other countries with similar network topology.
TSPU: Russia’s Decentralized Censorship System

Diwen Xue, Benjamin Mixon-Baca*, ValdikSS*, Anna Ablow, Beau Kujath*, Jedidiah R. Crandall*, Roya Ensafi

University of Michigan, *ASU/Breakpointing Bad, *Independent
Circumvention

Client-side Strategies
- IP fragmentation/TCP segmentation.
- TLS padding, prepending another TLS record.
- Encrypted proxies, VPNs.
  - Face blocking themselves

Server-side Strategies
- Window-size Reduction
- Split Handshake
Backup
Backup
Backup
Asymmetricity of TSPU censorship

- US
  - SYN
  - SYN/ACK
  - Root Server
  - Root Server

- RU
  - SYN
  - Root Server
  - Resolver
  - Resolver

RU:IP=1
  - src.ip = IP2
  - SYN

RU:IP=2
  - src.ip = IP1
  - SYN/ACK

RU:IP=1
  - src.ip = IP2

DNS

US

RU

US

RU

US

RU

39
Triggers and Behaviors (SNI)

- SNI (Server Name Indication)
  - Transferred in plaintext in at the beginning of a TLS session
- Depending on the domain name, different blocking behaviors were observed.
Triggers and Behaviors (IP, QUIC)

- **IP-based blocking**
  - Connections blocked regardless of payloads or TCP port.

- **QUIC Blocking**
  - Protocol fingerprint based on plaintext “Version” field.

- **Require dropping or modifying packet (In-path Capability)**

---

![Diagram showing IP-based blocking and QUIC blocking](image-url)
● ClientHello Fuzzing
  ○ To understand which parts of the packet are inspected.
Asymmetric TSPUs

- TSPU Law allows ISPs to route upstream and downstream through different TSPUs.
- Discover upstream-only TSPUs
  - By exploiting the fact that only local connections are censored.
- Located three TSPUs with asymmetric visibility.
Remote Measurement: Echo

- Echo servers would echo back anything sent to them.
  - Ensures that triggers would be sent once from RU to remote.
- Client needs to set port to 443.
  - The roles of “client” and “server” are reversed.
TSPU State Management - IP Fragmentation

- How TSPU handles fragmentation
  - Buffers fragments
  - Forward Individually
  - Overwrite TTL (Time-To-Live)
  - Maximum 45 fragments.
TSPU State Management - TCP Flags

- Sequences of TCP flags
  - Create states at TSPU
  - Remote-originated sequences bypass inspection & blocking.

- Remote SYN(s) confuses TSPU
  - Simultaneous Open / Split Handshake
  - SNI-IV still blocks the connection.
TSPU State Management - States Timeouts

- Connection entries are removed after timeouts.
- TSPU timeout values do not conform to any major OSes.
  - Short timeout for SYN-SENT allows opportunity for circumvention

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Timeout</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote.SYN; SLEEP; Local.SYN; Remote.SA; Local.Trigger</td>
<td>60</td>
<td>SYN_SENT</td>
</tr>
<tr>
<td>Local.SYN; Remote.SYN; Local.A; SLEEP; Local.Trigger</td>
<td>105</td>
<td>SYN_RCVD</td>
</tr>
<tr>
<td>Local.SYN; Remote.SA; SLEEP; Remote.ACK; Local.Trigger</td>
<td>480</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>Local.Trigger(SNI-I); SLEEP</td>
<td>75</td>
<td>SNI-I</td>
</tr>
<tr>
<td>Local.Trigger(SNI-II); SLEEP</td>
<td>420</td>
<td>SNI-II</td>
</tr>
<tr>
<td>Local.Trigger(SNI-IV); SLEEP</td>
<td>40</td>
<td>SNI-IV</td>
</tr>
<tr>
<td>Local.Trigger(QUIC); SLEEP</td>
<td>420</td>
<td>QUIC</td>
</tr>
</tbody>
</table>
Censorship in Russia: Pre-TSPU

- “Decentralized Control”, termed by previous work*.
- Facilitated by the commoditization of filtering technologies
- ISPs *independently* implement censorship in their networks.
  - “Registry of Banned Sites”, maintained by Roskomnadzor.
  - Specific blocking techniques were not prescribed.

→ Model also adopted by other countries, e.g., UK.

*Decentralized Control: A Case Study of Russia NDSS'20*
Conventionally, Censorship = Centralized.

- Filters placed at choke points in the nation’s Internet topology.

[3] Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran
Thousands of privately-owned, distributed ISPs makes leveraging a centralized architecture challenging.
Censorship in Russia, pre-TSPU

- Significant differences in both types and amount of blocking between ISPs.
Changes in Russia’s Censorship Model

- "On Sustainable RuNet" law signed on May 1, 2019.
- Appoints Roskomnadzor to guard the “stability, security, and integrity” of Russia’s Internet.
- Provides legal grounds for the government to require ISPs to install “special equipment”.

The President signed the law on sustainable Runet

Vladimir Putin signed on Wednesday the federal law "On Amendments to the Federal Law "On Communications" and the federal law "On Information, Information Technologies and Information Protection," Kremlin.ru reports.

This is the so-called law on the sustainability of the Runet, according to which a national Internet traffic routing system will be created in the country in order to ensure the reliable operation.
Changes in Russia’s Censorship Model

- ISPs receive letters from Roskomnadzor, demanding information and installation of black-box DPIs, a.k.a TSPU.

- ISPs are concerned these devices may increase risks of failure and deprive citizens of their right to information.

https://habr.com/ru/post/459894/
Changes in Russia’s Censorship Model

- Users report on blocked resources that were not present in the blocking registry (out-registry blocking).
- Plus, measurement studies suggest temporal and geographic uniformity.

Identical throttling behaviors were observed from vantage points across ISPs.

Throttling was widespread, implemented in at least 401 ASes, even though the domains were not in the blocking registry.

A new system was put into use!
Measuring TSPU is Challenging

1. Acquiring vantage points
2. Distinguishing ISP and TSPU censorship
3. Adopting remote measurement due to asymmetricity of TSPU censorship
Run in-country measurement to characterize:
  - SNI-based Censorship
  - IP-based blocking
  - QUIC blocking

Remote measurements to scan the deployment of TSPUs.
TSPU
(Technical Measures to Combat Threats)

Centrally controlled by RKN, Decentreally deployed in networks.

- **How** TSPU blocks a connection?
- **What** resources it blocks?
- **Where** it is installed w.r.t. Russian users?
TSPU Blocking: In-path and Stateful

Connection tracking, degree of statefulness, reliability
→ Refer to Paper