

IETF 115 - PEARG Meeting

# OOONI Measurements of Internet Censorship

Simone Basso (OOONI)



9th November 2022

# OOONI: Open Observatory of Network Interference

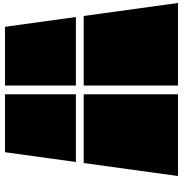
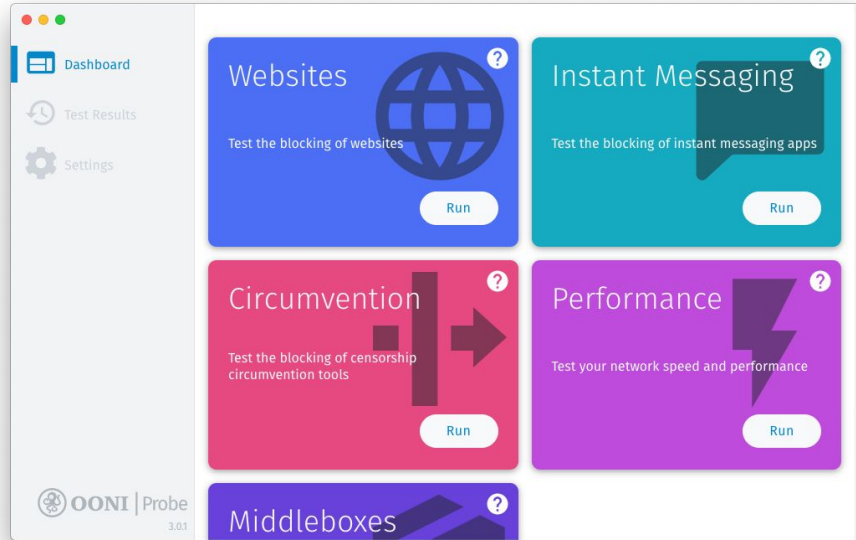
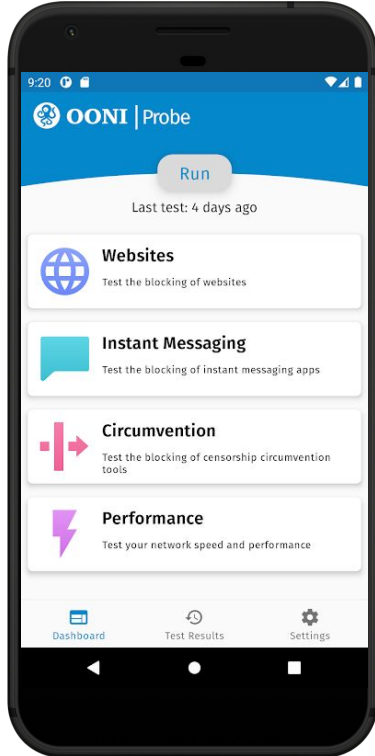
Free software project aimed at empowering decentralized efforts in increasing transparency of **internet censorship** around the world.

Since 2012, the OONI community has collected more than a billion of network measurements from *more than 200 countries*, shedding light on many cases of internet censorship around the world.



<https://ooni.org/>

# OOONI Probe (<https://ooni.org/install>)



# Measurement principles

https://example.com  
[1.2.3.4, 5.6.7.8]

1) DNS Lookup  
example.com

with getaddrinfo

[5.4.3.2] ?

with  
udp://1.1.1.1:53

NXDOMAIN ?

2) Measuring  
endpoints

TCP connect  
1.2.3.4:443

TLS handshake  
example.com

GET /

200 OK  
{{ body }}

TCP connect  
5.6.7.8:443

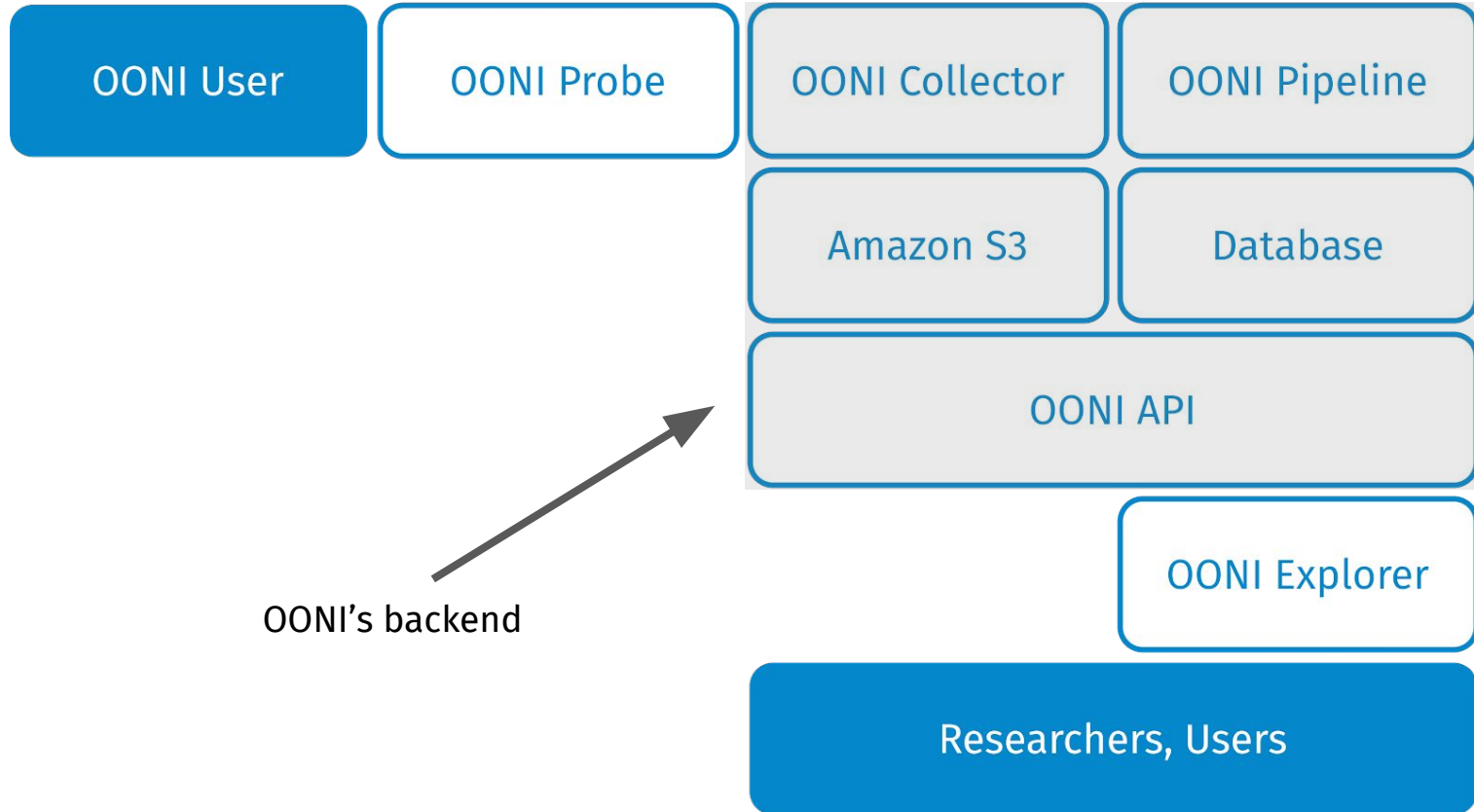
Timeout !

TCP connect  
5.4.3.2:443

TLS handshake  
example.com

ECONNRESET !

# Value Chain of a OONI Measurement



<https://explorer.ooni.org/chart/mat>

# OONI Measurement Aggregation Toolkit (MAT)

Create charts based on aggregate views of real-time OONI data from around the world

Country	ASN	From	Until	X Axis	Y Axis
All Countries ▼	AS1234	2022-10-08	2022-11-08	Measurement Day ▼	▼
Test Name	Domain	Input	Website Categories		
Web Connectivity ▼	twitter.com	https://fbcdn.net/robots.txt	ALL ▼		

Show Chart

<https://ooni.org/reports>

# Iran blocks social media, app stores and encrypted DNS amid Mahsa Amini protests

Simone Basso (OONI), Maria Xynou (OONI), Arturo Filastò (OONI), Amanda Meng (IODA - Georgia Tech), 2022-09-25

Protests **erupted** in Iran over the last week following the death of Mahsa Amini, a 22-year-old Kurdish woman who was reportedly beaten to death by Iran's morality police for allegedly violating strict hijab rules. Amid the **ongoing protests**, which have **reportedly** resulted in at least 31 civilian deaths, Iranian authorities **cracked down on the internet** in an attempt to curb dissent.

Over the past week, Iran experienced **severe mobile network outages**, in addition to increased levels of internet censorship. In this report, we share **OONI network measurement findings from Iran** on the blocking of WhatsApp, Instagram, LinkedIn, Skype, Google Play Store, Apple App Store, and encrypted DNS (DNS over HTTPS). We also share **IODA** and **Cloudflare Radar** data on mobile network outages over the last few days.

<https://ooni.org/post/2022-iran-blocks-social-media-mahsa-amini-protests/>

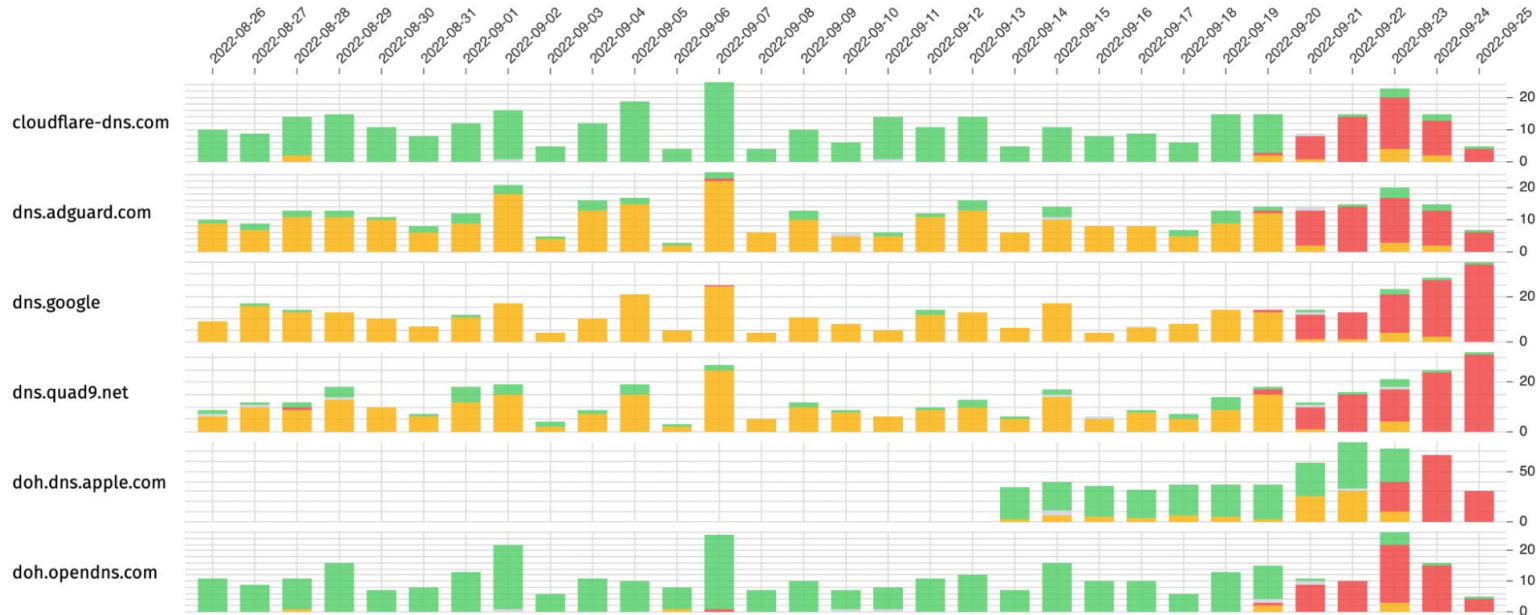
# DNS over HTTPS



## Iran

### Web Connectivity Test

ok\_count confirmed\_count anomaly\_count failure\_count



# Explaining color shift using doh.dns.apple.com

confirmed (= red) because the DNS lookup returns the 10.10.34.3{4,5,6} bogon

anomaly (= yellow) because we have timeouts connecting or during the TLS handshake

AS	#dns	#tcp	#tls	#success	count
Zi-Tel (206065)	yes		yes		18
TCI (58224)	yes	yes	yes		21
TCI (58224)	yes	yes	yes	yes ( !!! )	5

Subset of the data collected on 24 September 2022 for doh.dns.apple.com.

We reduce multiple failures. Confirmed is stronger than anomaly. So we see the plot turning red.

# New blocks emerge in Russia amid war in Ukraine: An OONI network measurement analysis

Maria Xynou, Arturo Filastò, 2022-03-07

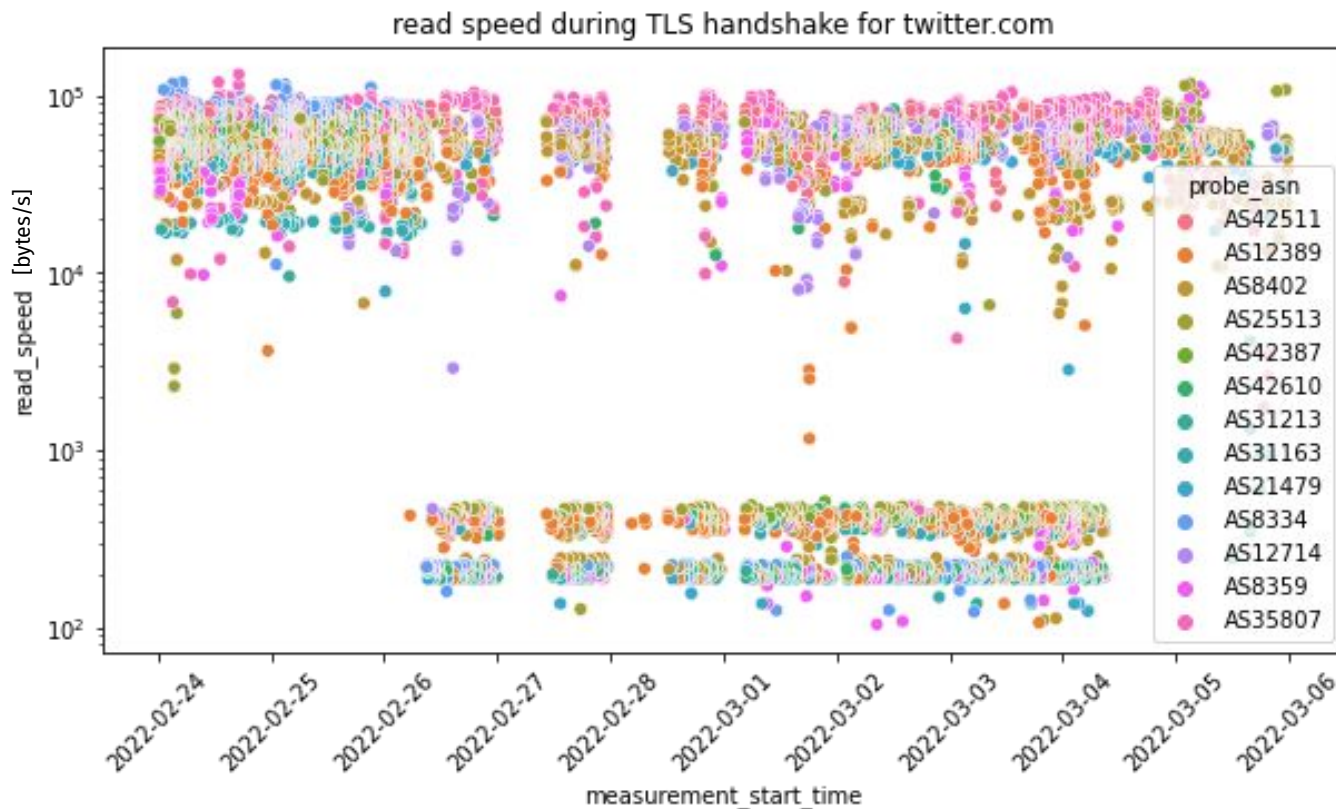
Information controls are known to occur during conflicts, and that's exactly what we're seeing in Russia following the recent invasion of Ukraine on 24th February 2022.

In recent days, [OOONI network measurement data](#) collected from Russia shows that many Internet Service Providers (ISPs) have started [blocking](#) access to several news media websites, as well as to a [website](#) (200rf.com) that shares information about captured and killed Russian soldiers in Ukraine. OONI data also shows that Russian ISPs started [throttling access to Twitter](#) on 26th February 2022, and switched to [blocking](#) it by 4th March 2022 – at which point, they also started [blocking access to Facebook](#). Censorship in Russia is generally implemented in a [decentralized](#) way, as blocks are not observed on all networks, while ISPs adopt a variety of different censorship techniques.

In this report, we share an in-depth analysis of new censorship events that have recently emerged in Russia based on [OOONI network measurement data](#).

<https://ooni.org/post/2022-russia-blocks-amid-ru-ua-conflict/>

# twitter.com throttling



# A Quick Look at QUIC Censorship

Kathrin Elmenhorst, 2022-06-16

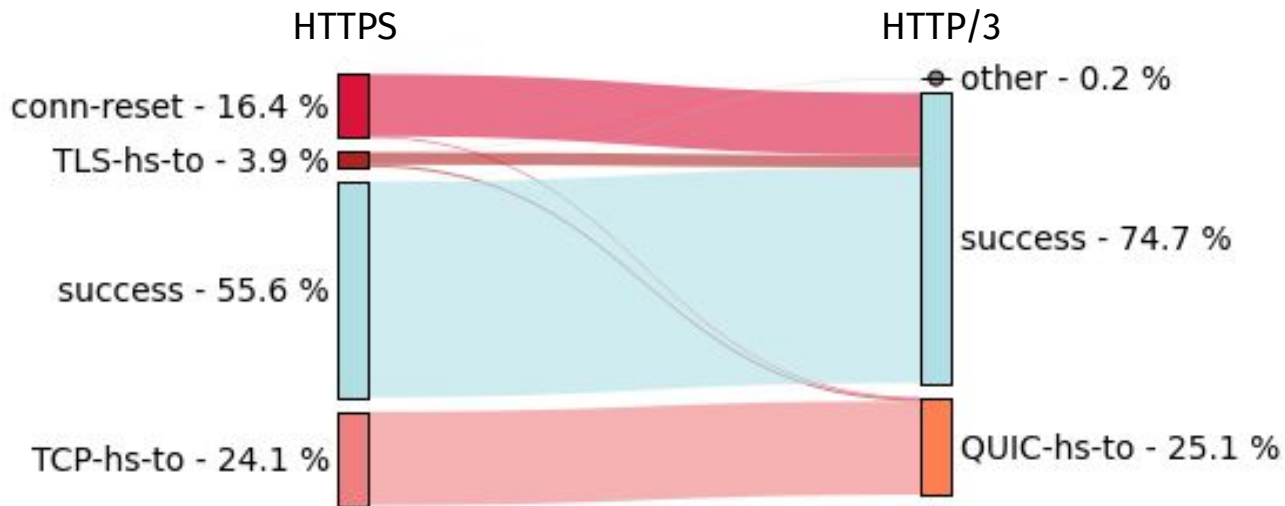
*This blog post was originally published by the Open Technology Fund to disseminate Kathrin Elmenhorst's QUIC-and-HTTP/3 censorship research as part of her ICFP fellowship with OONI.*

Last year, the new network protocol **QUIC** was introduced. QUIC is a general-purpose transport layer network with the goal of reducing latency compared to existing protocols. Since the introduction of QUIC, we have seen rising volumes of QUIC-based web traffic in the form of **HTTP/3**.

As QUIC usage increases, it has become the target of censorship efforts. From the perspective of censors, the emergence of QUIC and HTTP/3 means two things:

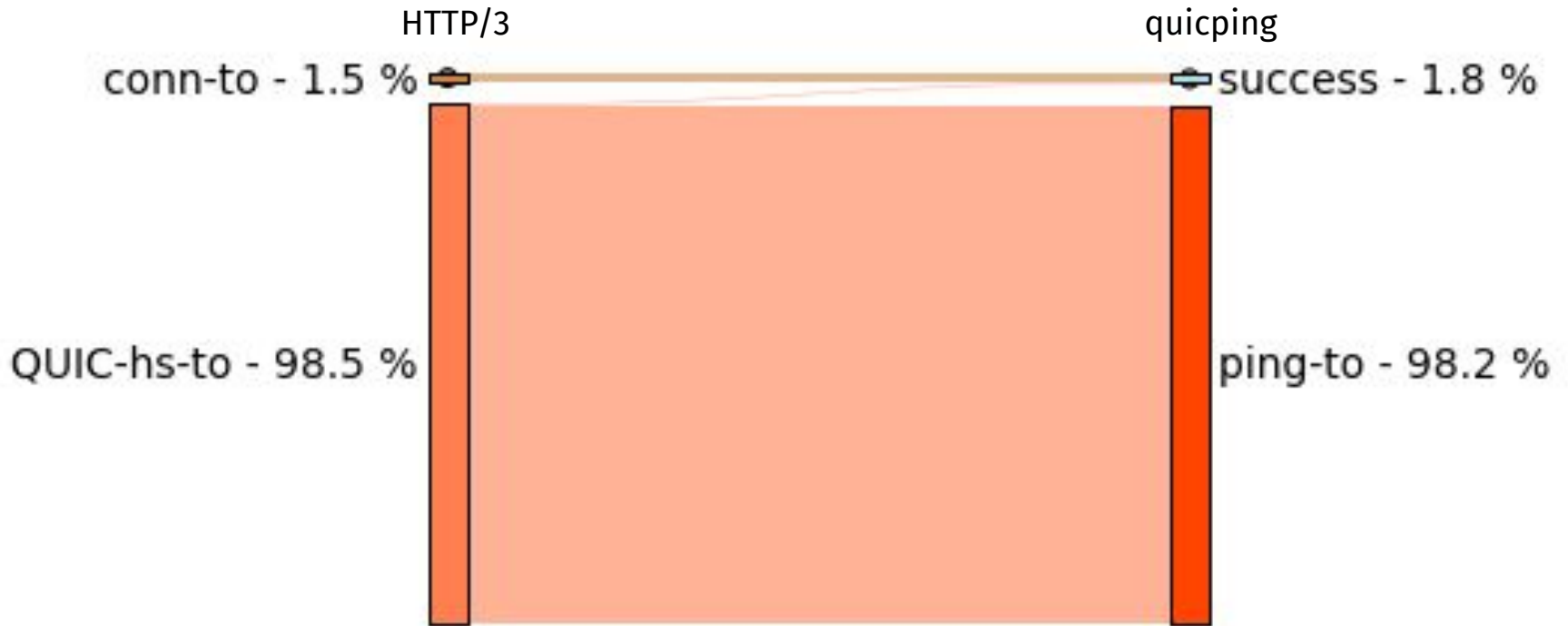
- HTTP/3 web traffic looks differently to firewalls, such that censors need to deploy new strategies to detect it.
- QUIC is better protected by encryption. QUIC encryption hides not only the details of the communication but also most of the connection metadata from observers.

<https://ooni.org/post/2022-quick-look-quic-censorship/>



Failure rates of HTTPS vs HTTP/3 (AS45090; China)

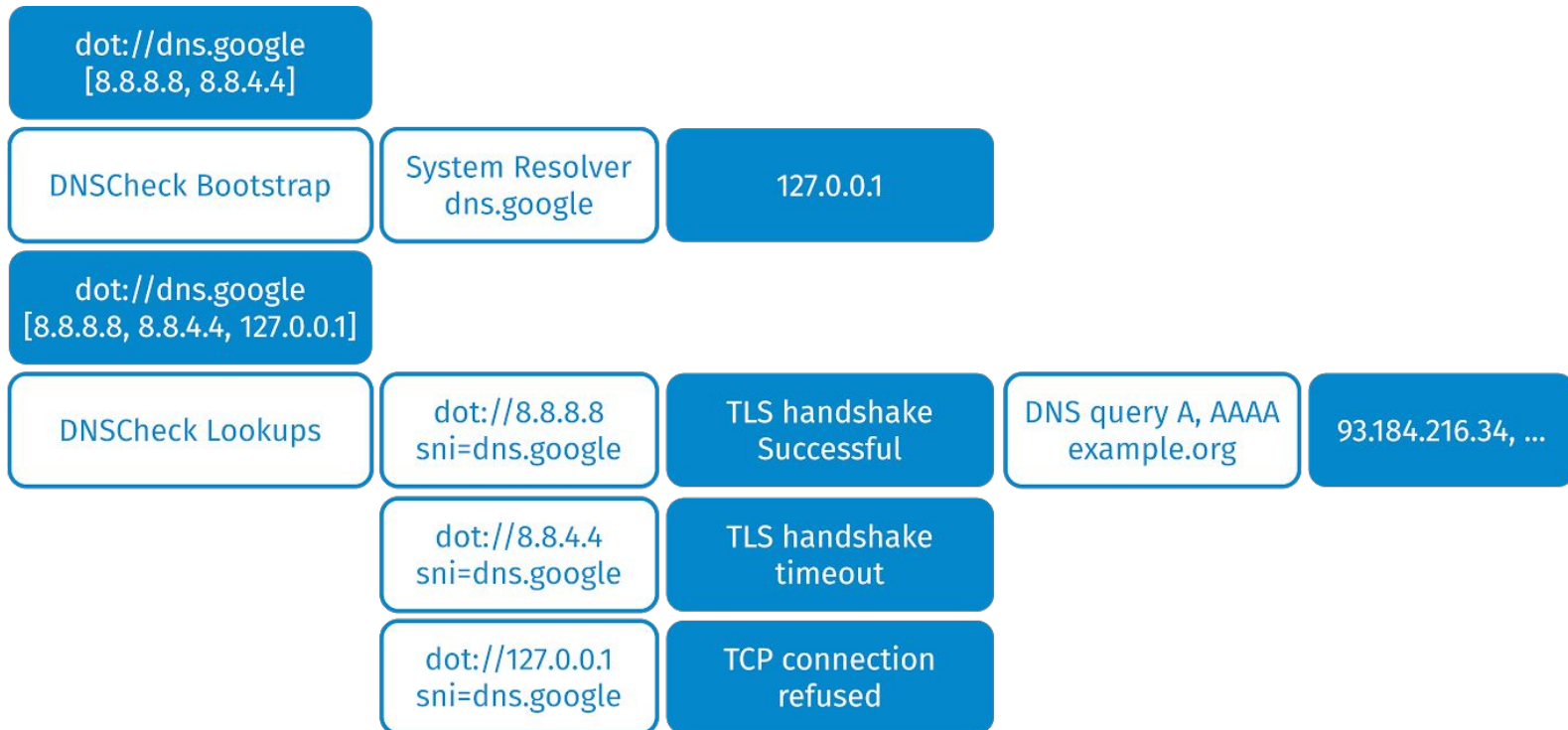
See <https://github.com/kelmenhorst/quic-censorship/issues/1>



Failure rates of HTTP/3 vs quicping (AS45090; China)

See <https://github.com/kelmenhorst/quic-censorship/issues/1>

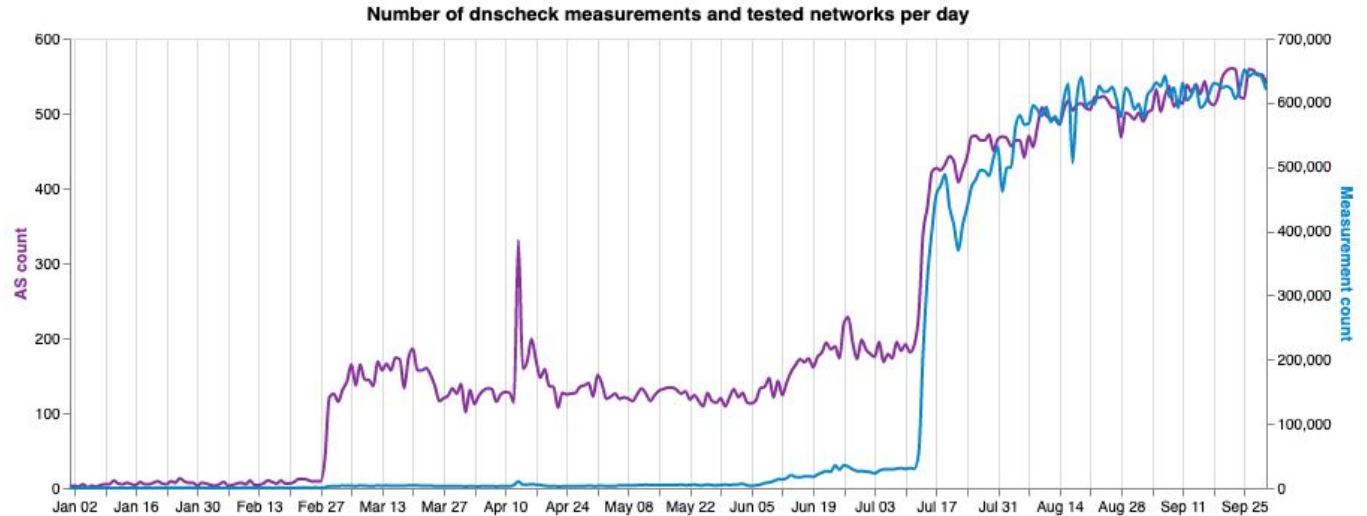
# The DNSCheck Experiment



# DNS Check is now in OONI Probe!

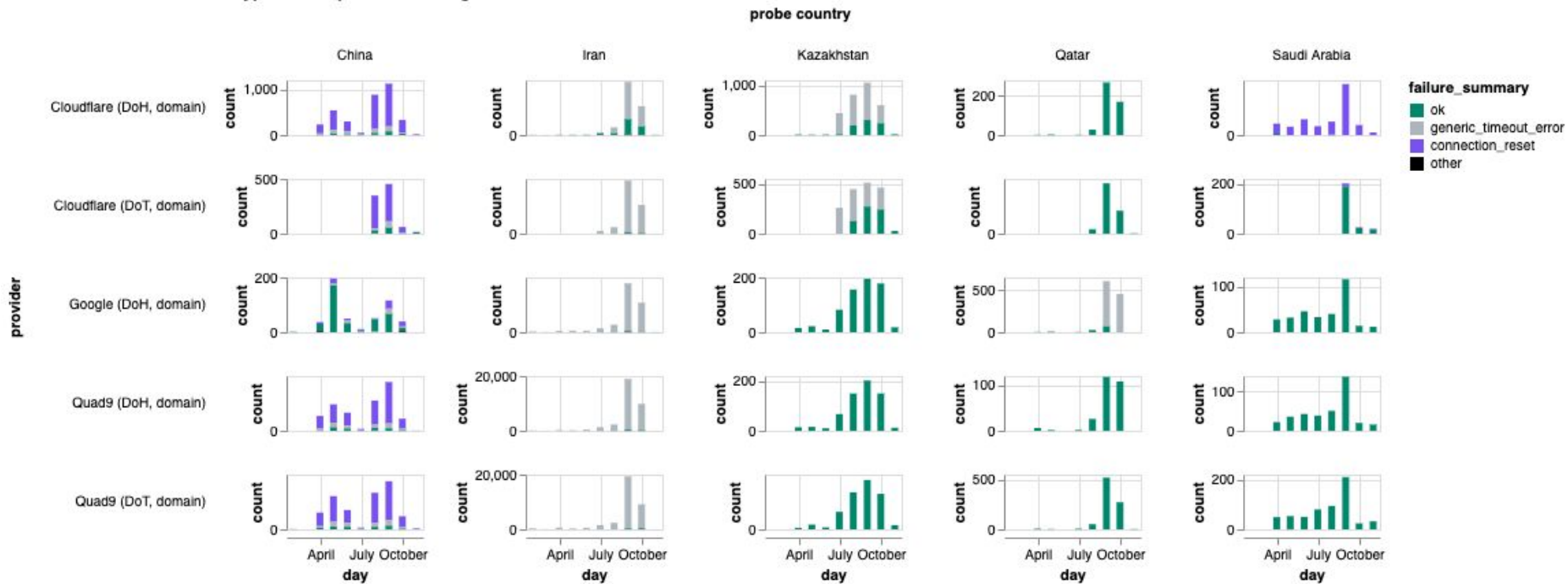
As of October 2022

- 189 countries
- 4593 ASs
- 45M measurements



# TLS measurements

TLS measurements for encrypted DNS providers using their domain



# Conclusion / future work

- “Parrot” the fingerprint of popular TLS implementations
- Integrate QUIC measurements into mainline web measurements
- Add follow-up checks (e.g., SNI blocking) to mainline web measurements
- Support DoH3 and DoQ in dnscheck
- Automatically explode measurements in DNS, TCP, TLS, ...
- Classify by anomaly reason (e.g., TLS timeout or TCP connect timeout) instead of just saying anomaly inside MAT charts
- Experiment with [cloudflare/go](https://cloudflare.com/go) to use ECH

# Thank you!



[contact@openobservatory.org](mailto:contact@openobservatory.org)



<https://slack.ooni.org/>



[@OpenObservatory](https://twitter.com/OpenObservatory)



<https://github.com/ooni>