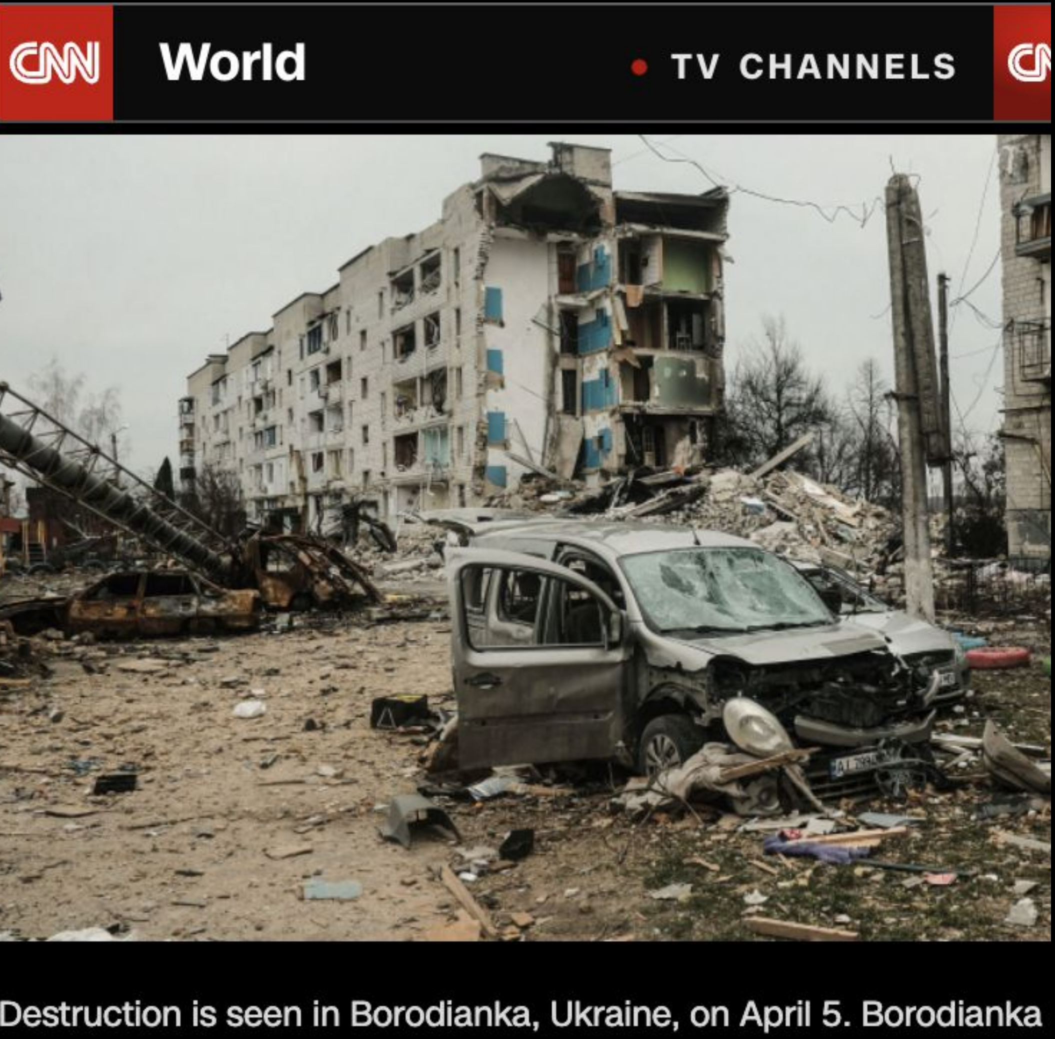
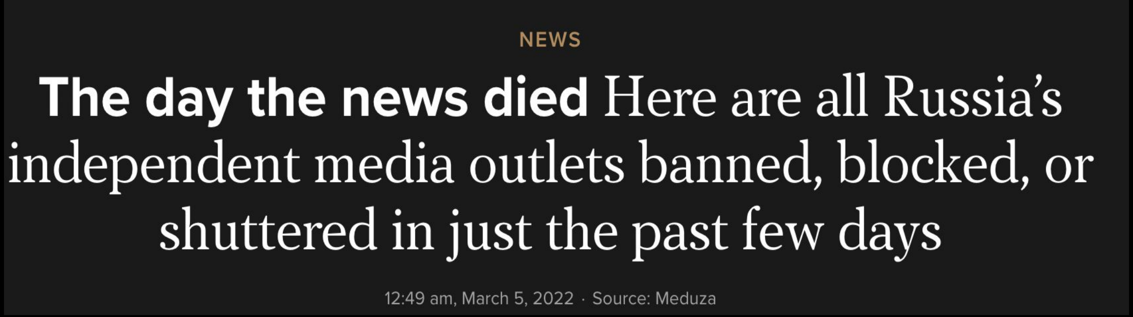
Protecting Users from Adversarial Networks

Roya Ensafi
University of Michigan



Destruction is seen in Borodianka, Ukraine, on April 5. Borodianka

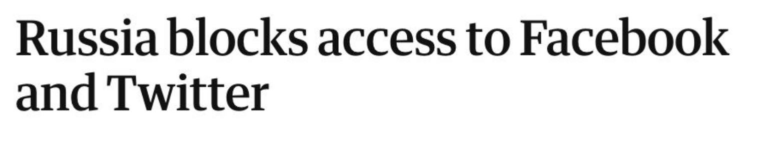
an President Volodymyr Zelensky speaks to the media a



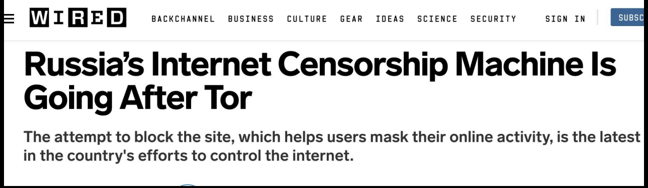
NEWS

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



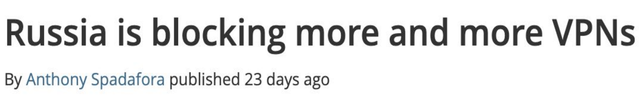
Russia blocks access to Facebook and Twitter



≡ WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY SIGN IN SUBSC

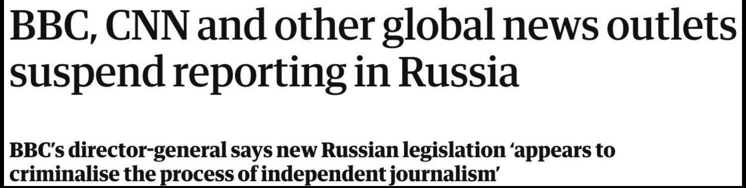
Russia's Internet Censorship Machine Is Going After Tor

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.



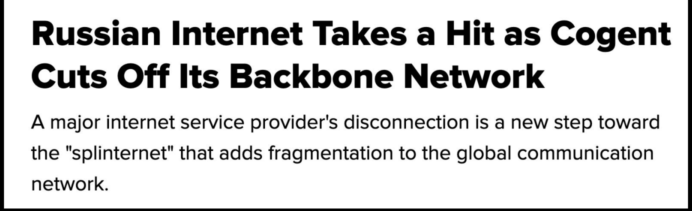
Russia is blocking more and more VPNs

By Anthony Spadafora published 23 days ago



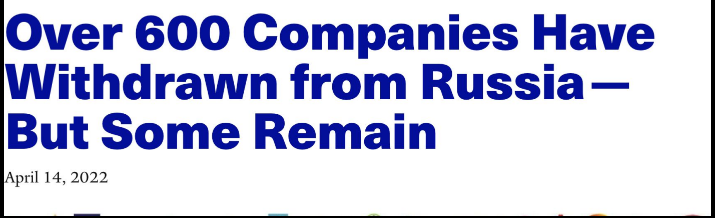
BBC, CNN and other global news outlets suspend reporting in Russia

BBC's director-general says new Russian legislation 'appears to criminalise the process of independent journalism'



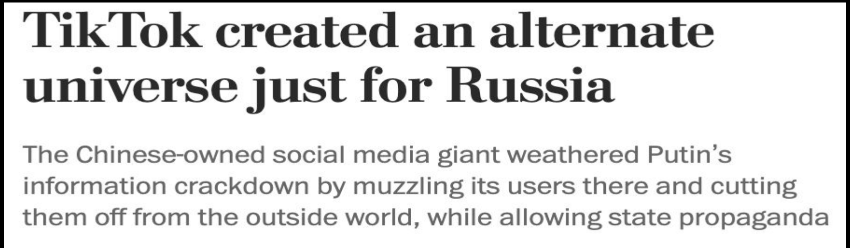
Russian Internet Takes a Hit as Cogent Cuts Off Its Backbone Network

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



Over 600 Companies Have Withdrawn from Russia — But Some Remain

April 14, 2022



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

© SalamPix/ABACA/pictur

Technical questions:

- What **sites** are being blocked? What is still accessible?
- How, technically, has Russia implemented its **information controls**?
- What will Russia likely do next ?
- What does this mean for **Internet freedom** ?

Detecting and defending against adversarial networks is challenging, due to the **Internet’s vast size and heterogeneity**, **the powerful capabilities of in-network threat actors**, and **the lack of ground-truth**.

Experiments must be conducted ethically and safely.

I build scalable techniques and systems to protect users from adversarial networks that violate the **confidentiality, integrity,** or **availability** of users' legitimate traffic.

WHO

Governments
Consumer ISPs
VPNs
Transit ISPs
Cellular providers
Content providers
Content delivery networks
Device manufacturers
Hackers for hire

WHAT

Blocking
Tampering
Net neutrality violation
Mass surveillance
Targeted surveillance
Content removal
Throttling
Denial of Service (DoS)

In this talk, I cover...

Leveraging side channel measurement to **detect and understand censorship**

Applying a multi-perspective approach to **safeguard the consumer VPN ecosystem**

The Ensafi Lab

https://ensa.fi

Ram Sundara Raman
PhD Candidate

Reethika Ramesh
PhD Candidate

Renuka Kumar
PhD Candidate

Diwen Xue
PhD Student

Anna Ablove
Master Student

Roya Ensafi
Professor

Armin Huremagic
RA

Maryam
RA

Gavin Li
Undergraduate

Alumni include:

M. Ikram
→ Lecturer, Macquarie University

A. Vyas
→ Masters Student, Cornell Tech

N. Ceccio
→ PhD Student, Wisconsin Madison

Victor Ongkowijaya
→ PhD Student, Princeton

Apurva Virkud
→ PhD student, UIUC

A. Stoll
→ Software Engineer, Google

Prerana Shenoy
→ Security Engineer, Atlassian

Elio Qoshi
→ Ura Design

Arham Jain
→ Software Engineer, Google

Detecting Censorship with Side Channels

The Art of Censorship Data Analysis
FOCI 2023

Measurement Methods for Locating & Examining Censorship Devices
CoNEXT 2023 🏆 IRTF Applied Networking Research Prize winner

Censored Planet: An Internet-wide, Longitudinal Censorship Observatory
ACM CCS 2020

Measuring the Deployment of Network Censorship Filters at Global Scale
NDSS 2020

Quack: Scalable Remote Measurement of Application-Layer Censorship
USENIX Security 2018

Internet-Wide Detection of Connectivity Disruptions
IEEE S&P (“Oakland”) 2017 , Invited to appear in the IEEE S&PMagazine

Global Measurement of DNS Manipulation
USENIX Security 2017 Invited to appear in USENIX ;login:, Winter 2017 Issue

Analyzing the Great Firewall of China Over Space and Time
PETs 2015

Detecting Intentional Packet Drops on the Internet via TCP/IP Side Channels
Passive and Active Measurement (PAM), 2014

Idle Scanning and Non-interference Analysis of Network Protocol Stacks Using Model Checking
USENIX Security 2010

How Have We Collected Data on Censorship?

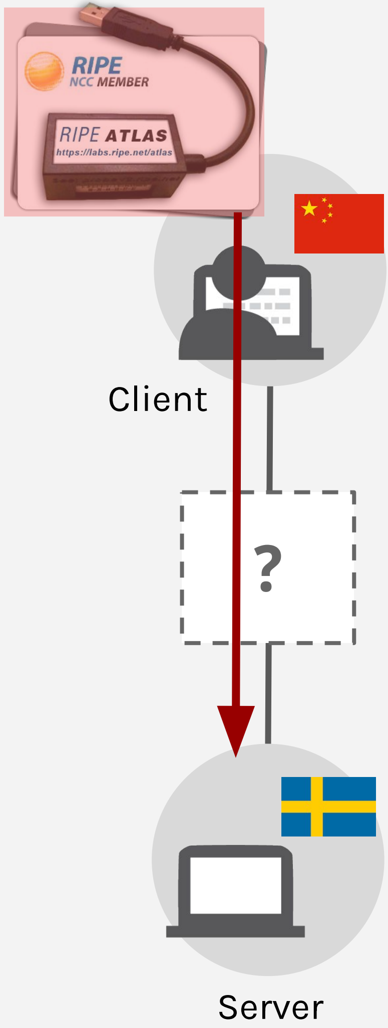
Old state of the art:

- Deploy hardware or software in censored region (e.g. RIPE Atlas, OONI probe)
- Ask people on the ground, or use VPNs, or research networks (e.g., PlanetLab)

THREE KEY CHALLENGES:

Coverage, continuity, and ethics

Collecting consistent, continuous, and global data requires a different approach.

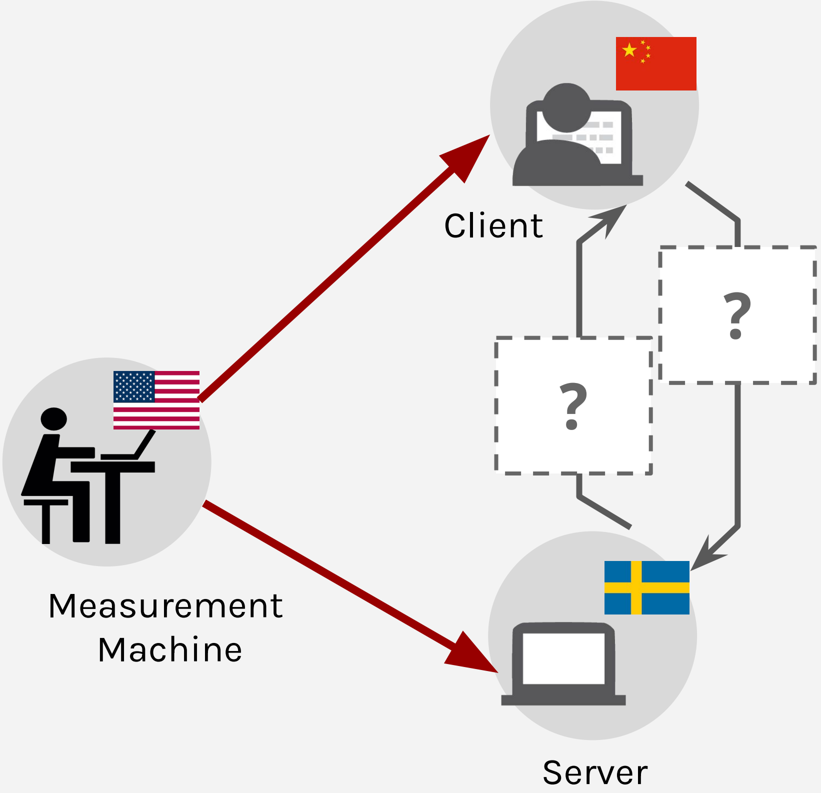


Measuring Internet Censorship Globally... Remotely!

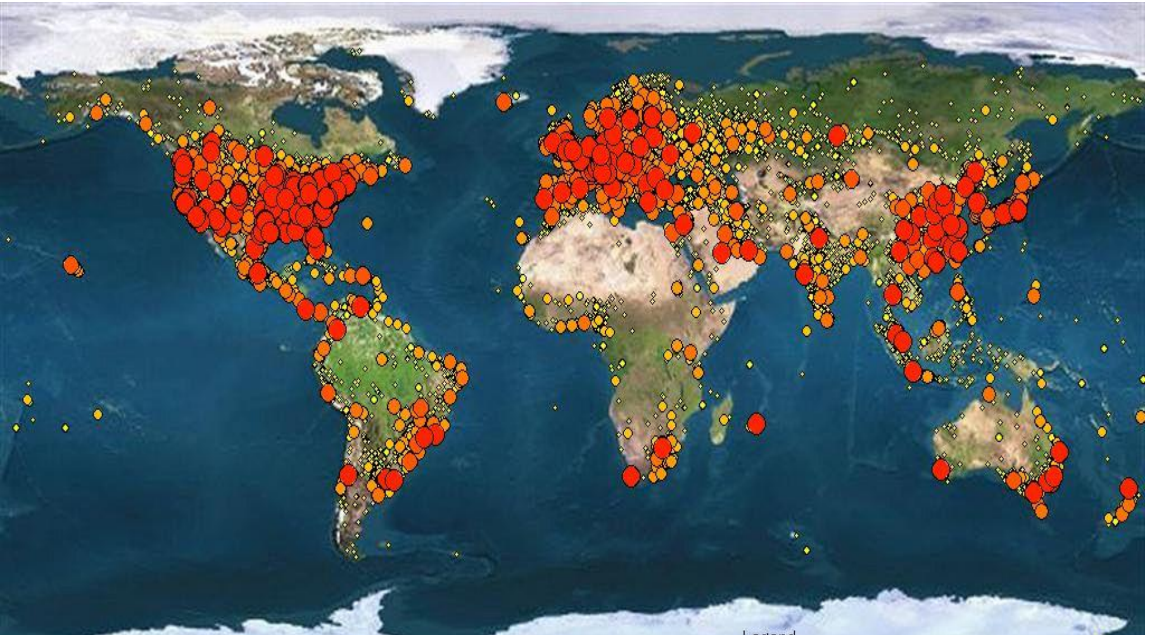
REFRAMING THE PROBLEM:

How can we detect whether pairs of hosts around the world can talk to each other?

... without volunteer participation?



Leveraging Existing Hosts as Vantage Points



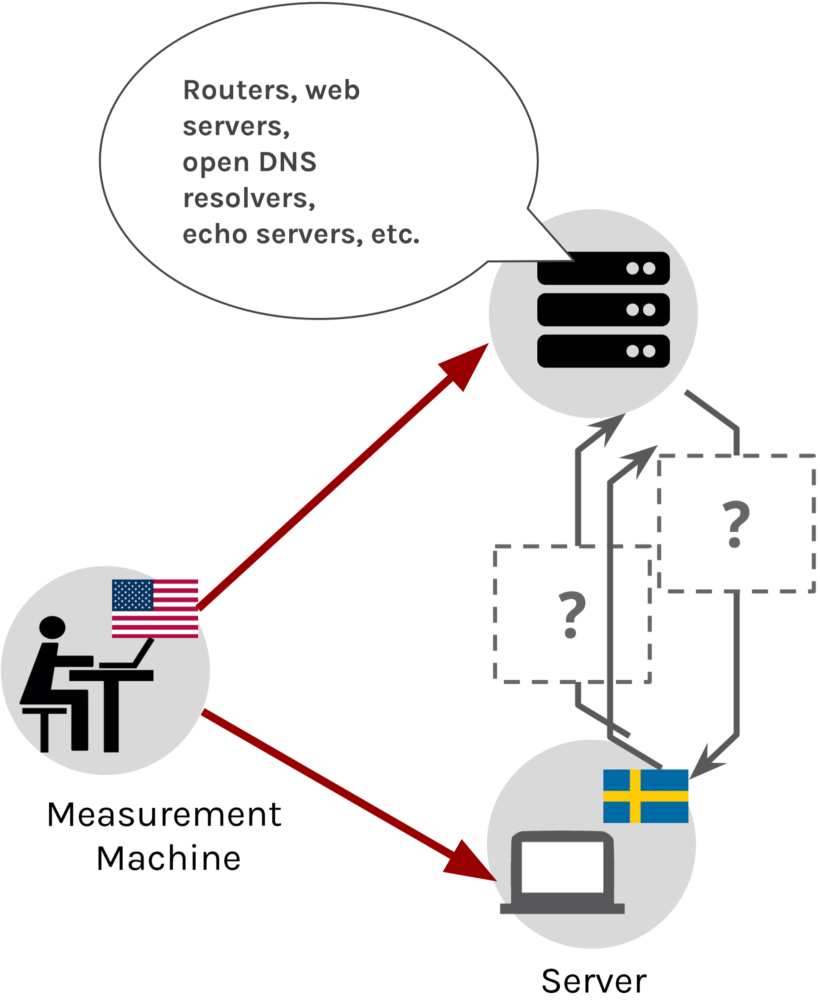
217 million IPv4 hosts w/ open ports
7 million open DNS resolvers
2 billion web servers
…

These machines speak to the world, and they follow **different Internet Protocols.**

My Approach:
Using Side Channels

REFRAMING THE PROBLEM:

How can we leverage subtle behavior of different Internet Protocols to detect whether two distant hosts can communicate on a given layer?


Routers, web servers, open DNS resolvers, echo servers, etc.
?
?
Measurement Machine
Server

Side Channels Techniques for Remotely Measuring Censorship

DNS Layer

Satellite (2017) →
Institutional open resolvers

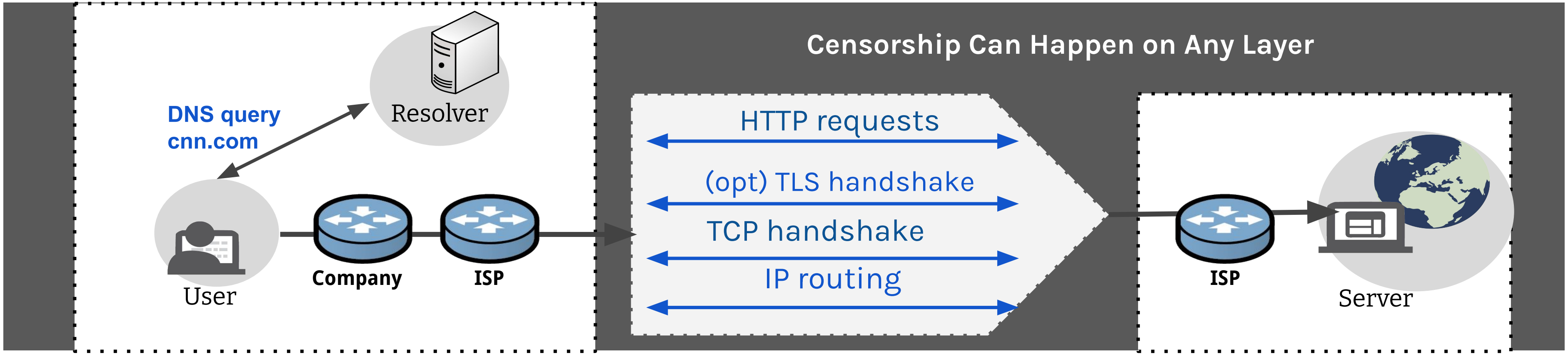
TCP/IP Layer

Spooky (2014)
Augur (2017)
→ Global IP_ID routers

Application Layer

Quack (2018)
HyperQuack (2020)
→ Services that reflect data
(e.g. Echo, HTTP, HTTPS)

Side Channels Techniques for Remotely Measuring Censorship



DNS Layer

Satellite (2017) →
Institutional open resolvers

TCP/IP Layer

Spooky (2014)
Augur (2017)
→ Global IP_ID routers

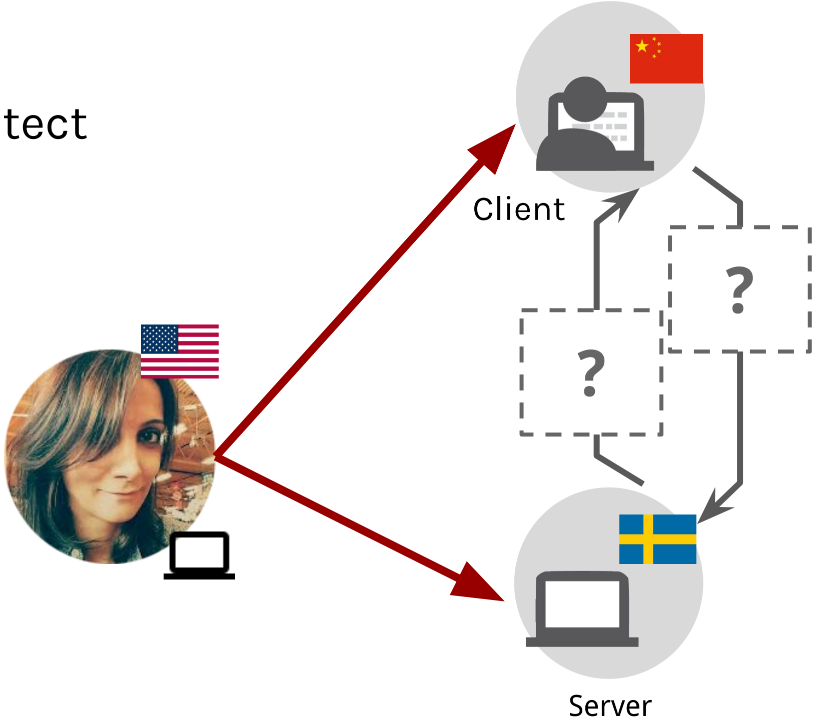
Application Layer

Quack (2018)
HyperQuack (2020)
→ Services that reflect data
(e.g. Echo, HTTP, HTTPS)

Spooky Scan

Spooky Scan uses TCP/IP side-channels to detect whether a client and server can communicate (and in which direction packets are blocked)

Goal: Detect blocking from off-path



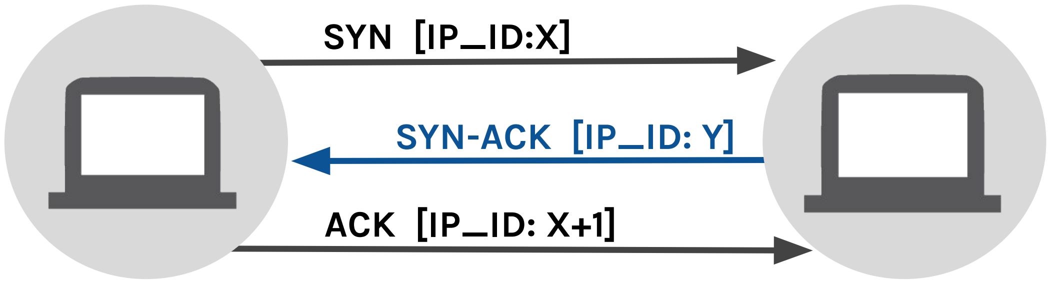
* **Detecting Intentional Packet Drops on the Internet via TCP/IP Side Channels** Roya Ensafi, Knockel, Alexander, and Crandall (PAM ’14)

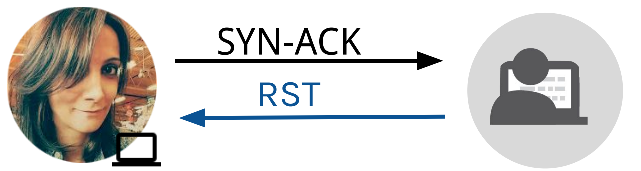
* **Idle Port Scanning and Non-interference Analysis of Network Protocol Stacks Using Model Checking** Roya Ensafi, Park, Kapur, and Crandall (Usenix Security 2010)

* **TCP Idle Scan** Antirez (Bugtraq 1998)

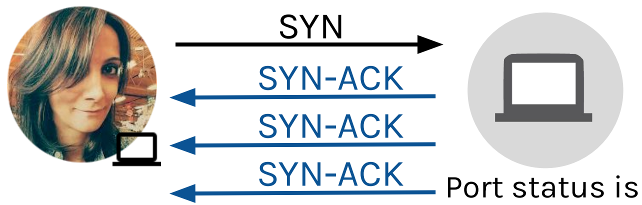
Background: TCP/IP Protocol

TCP Handshake:





Port status is **open/closed**



Port status is **open**

Spooky Scan Requirements

Client

Must maintain a global value for IP_ID

Server

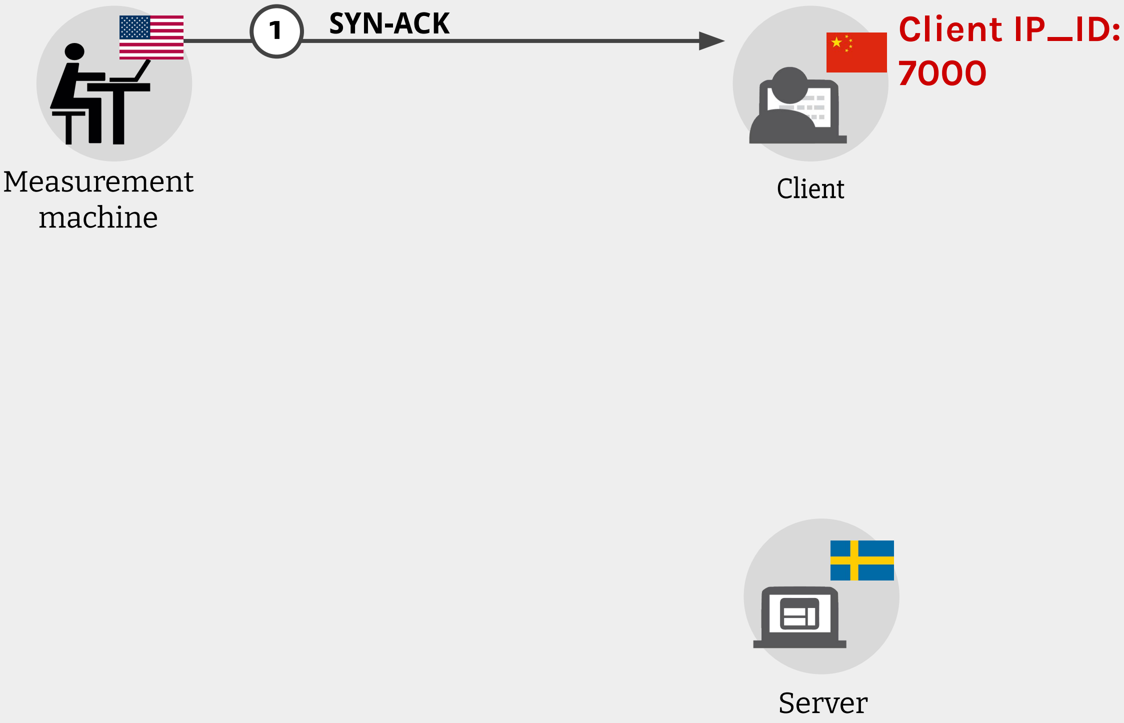
Open port and retransmitting SYN-ACKs

Measurement Machine

Must be able to spoof packets

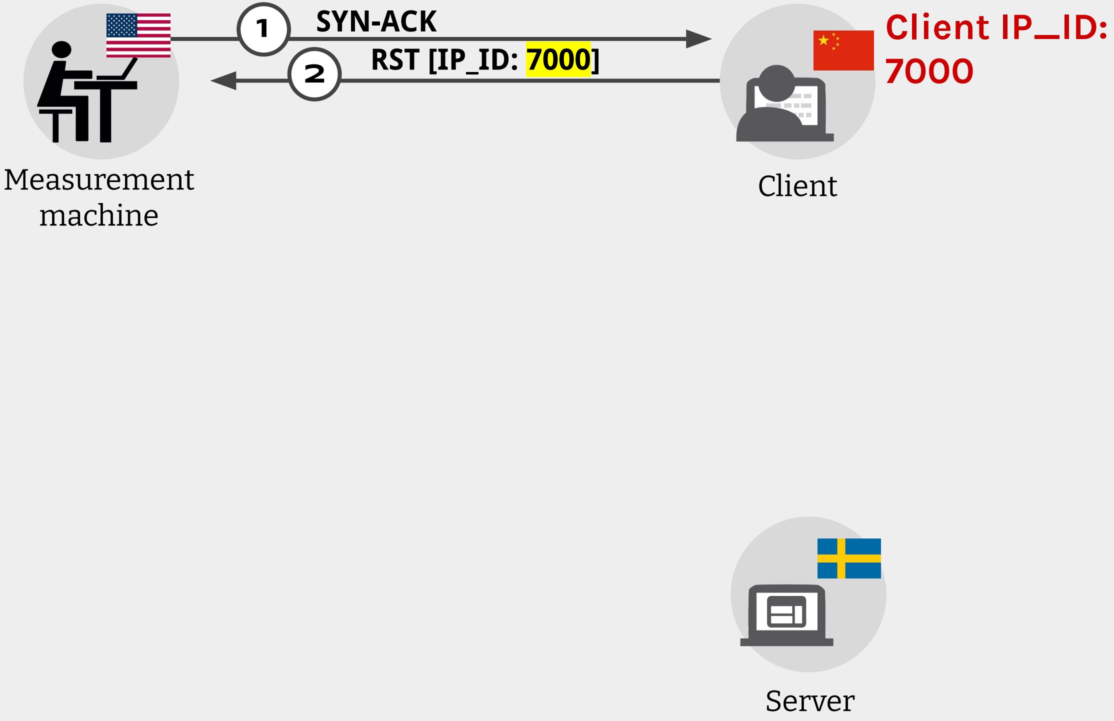
Spooky Scan

No direction blocked



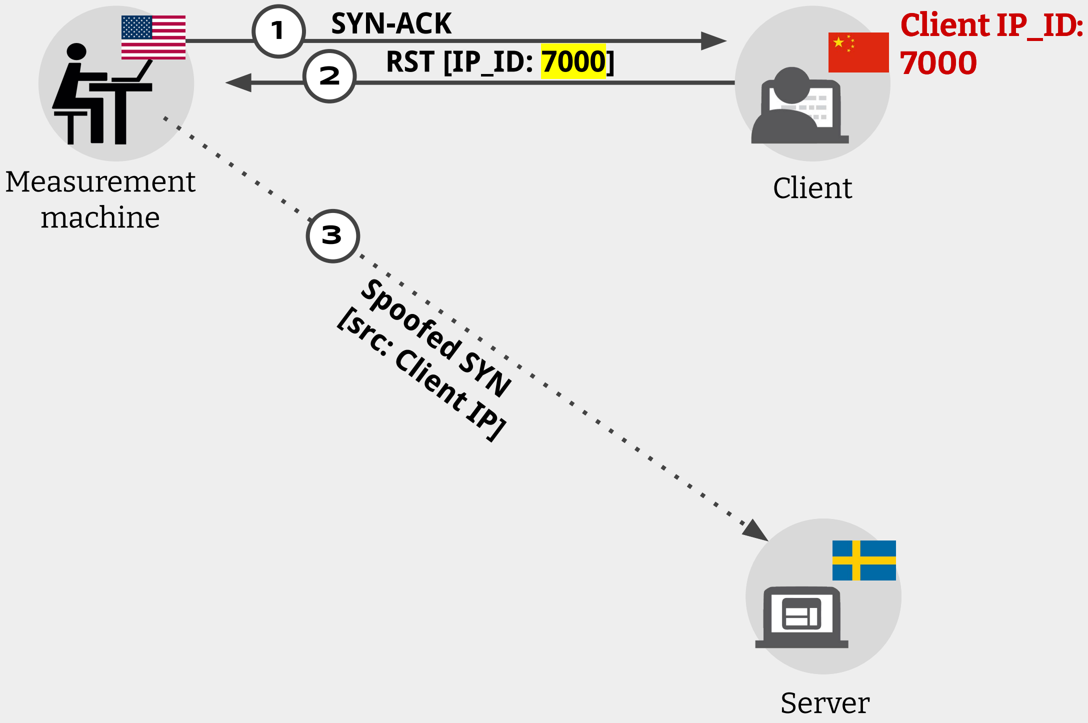
Spooky Scan

No direction blocked



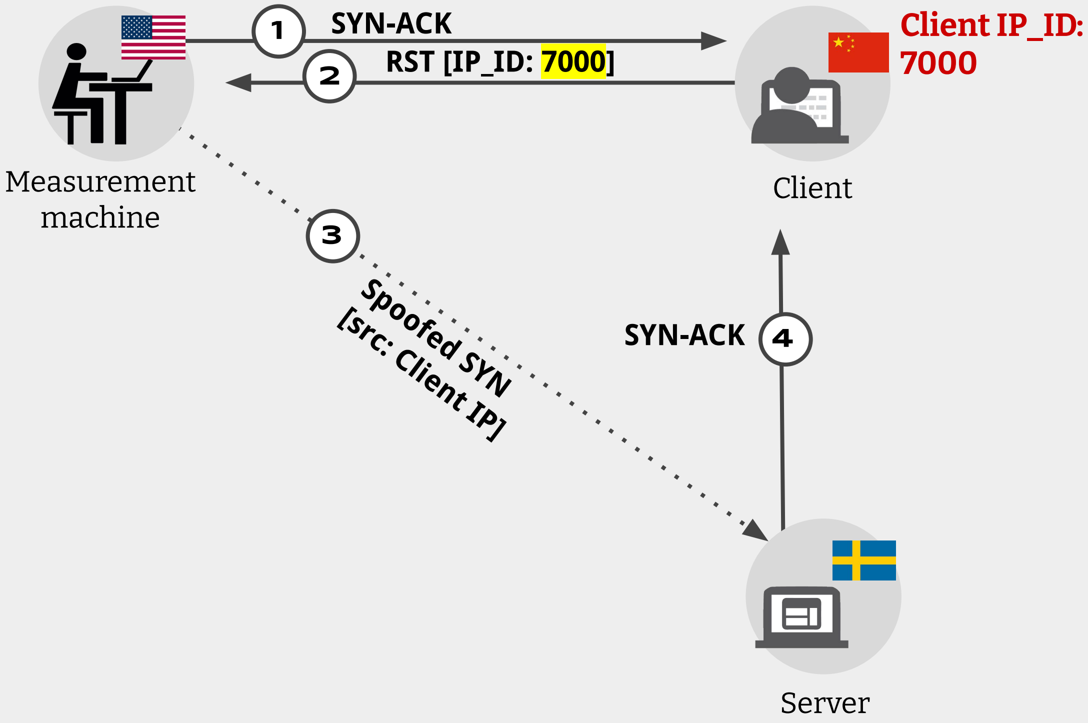
Spooky Scan

No direction blocked



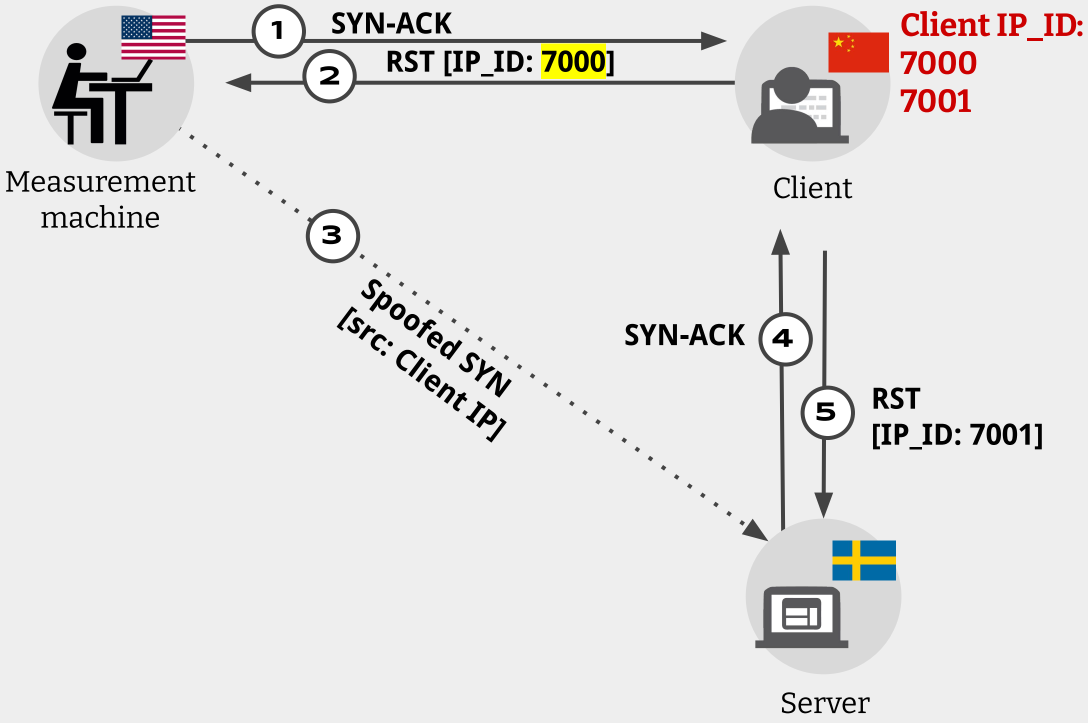
Spooky Scan

No direction blocked



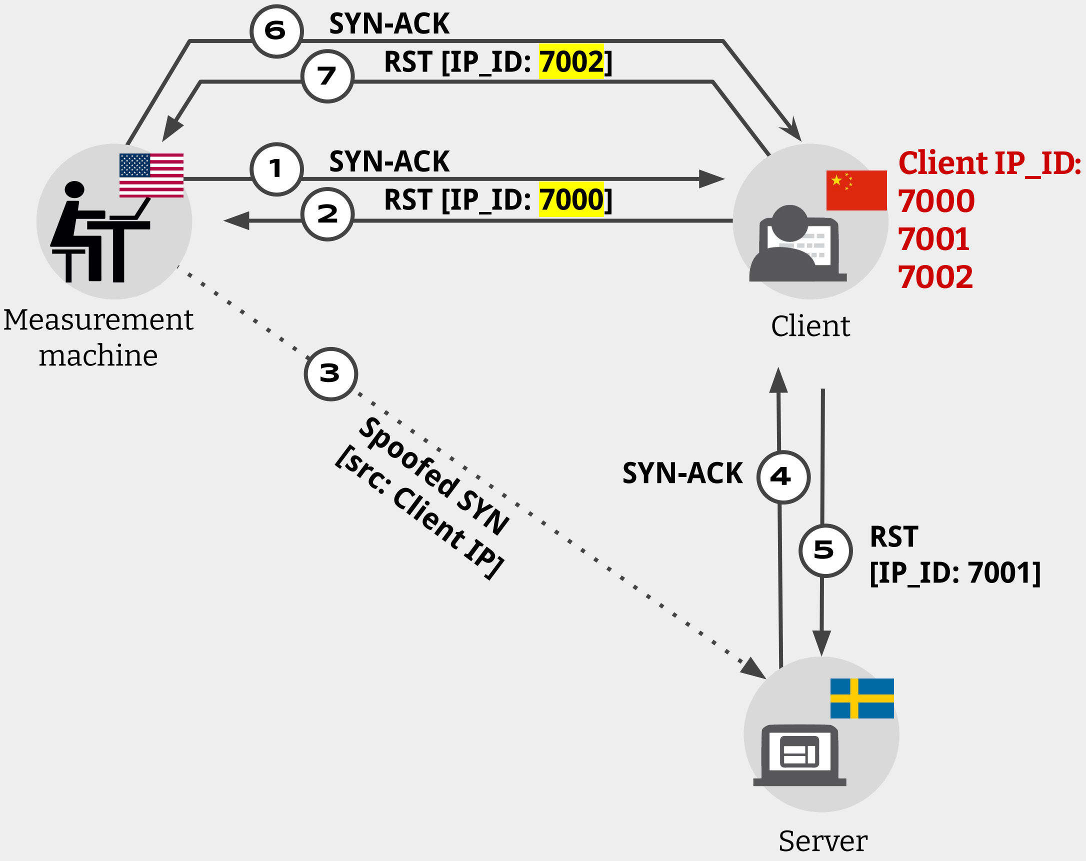
Spooky Scan

No direction blocked



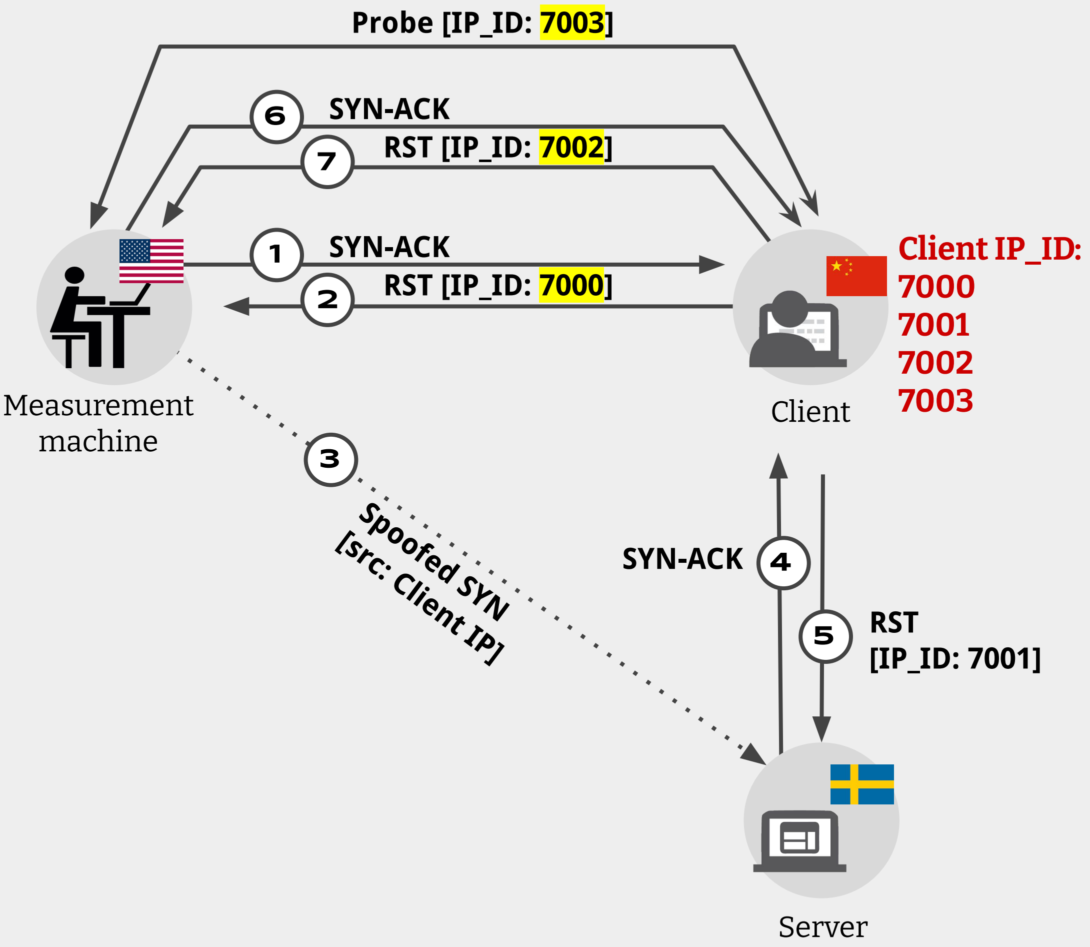
Spooky Scan

No direction blocked



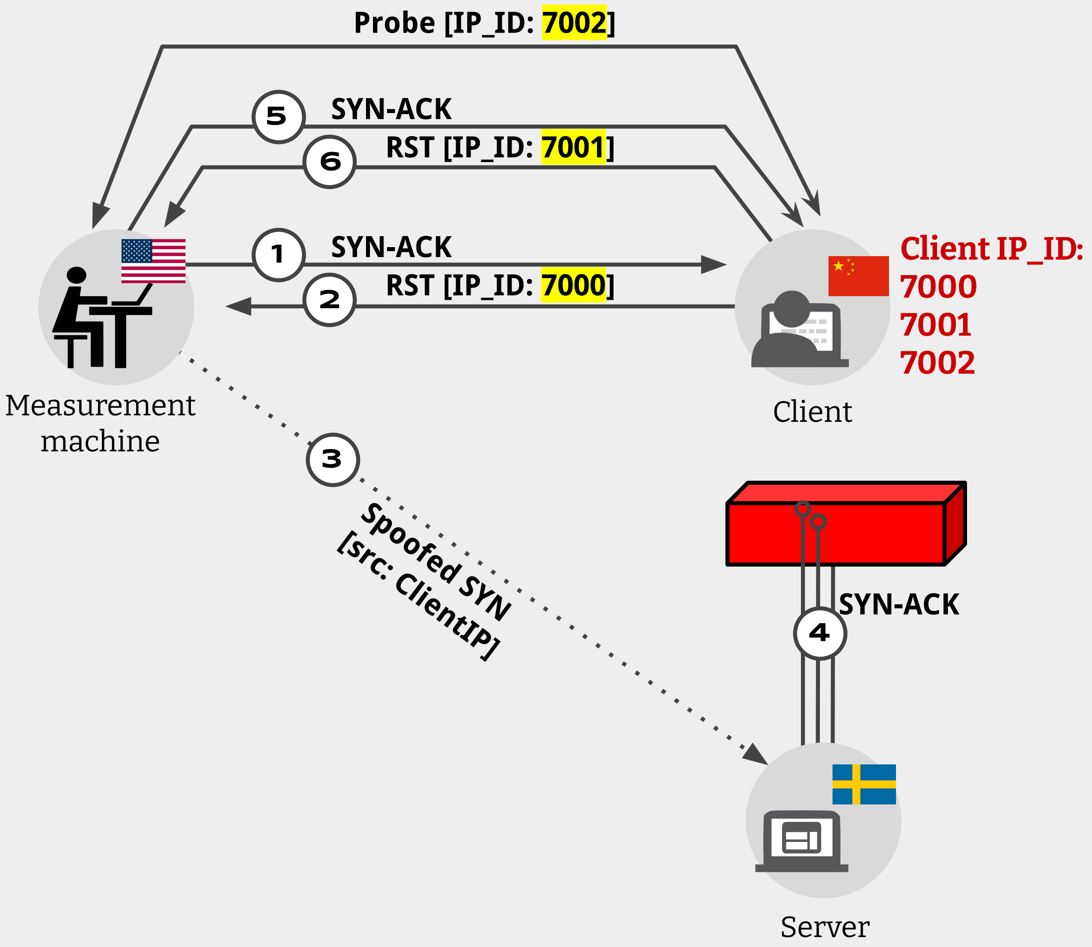
Spooky Scan

No direction blocked



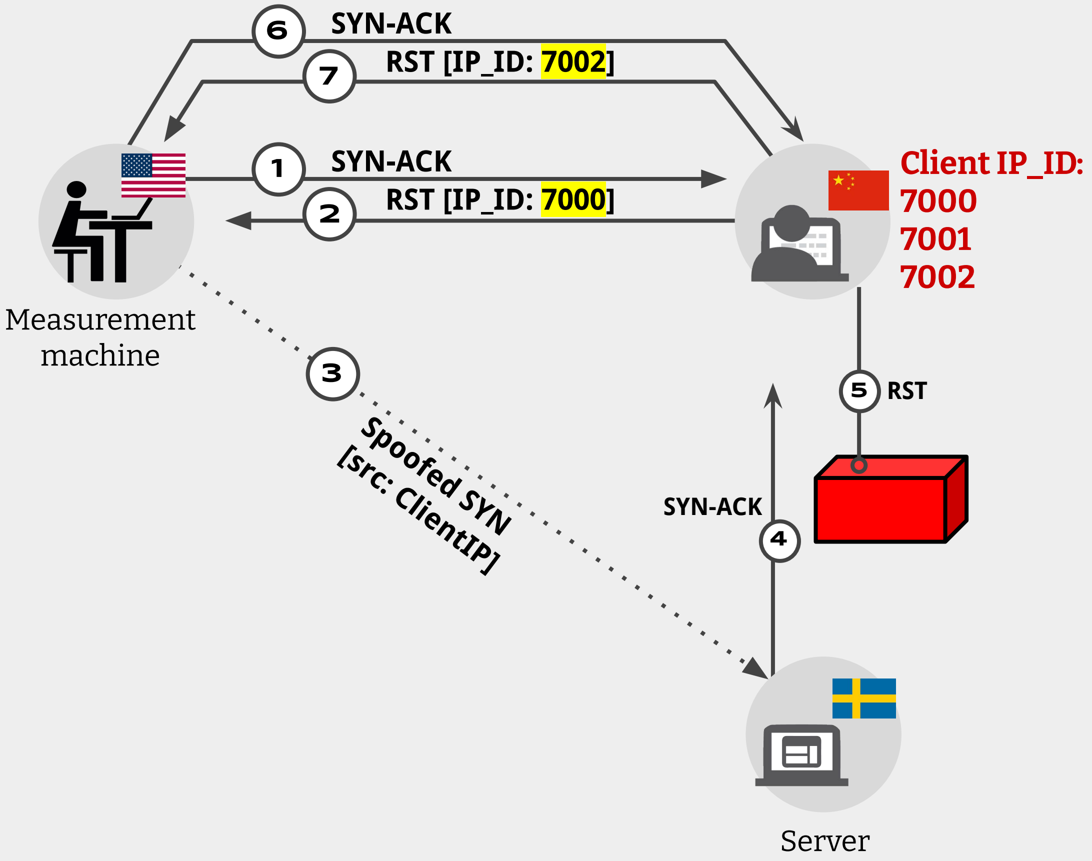
Spooky Scan

Server-to-Client blocked



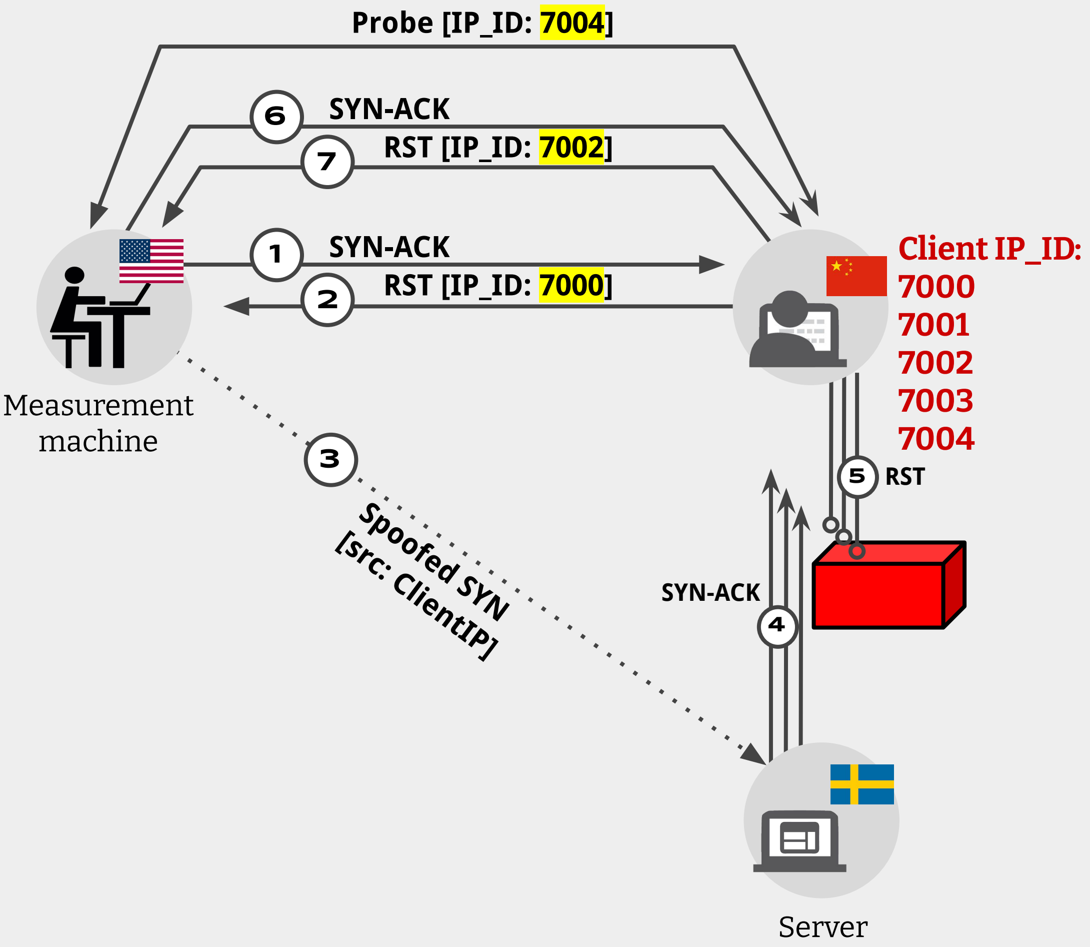
Spooky Scan

Client-to-Server blocked



Spooky Scan

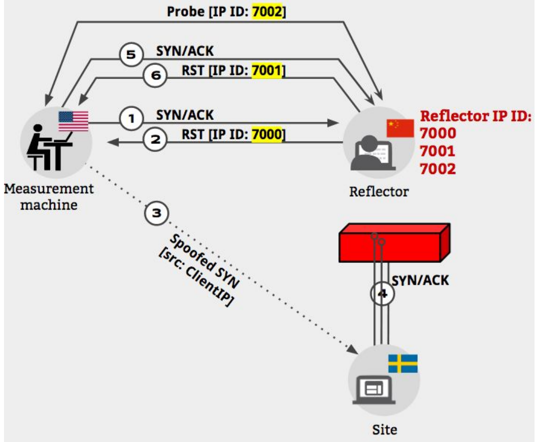
Client-to-Server
blocked



Spooky Scan

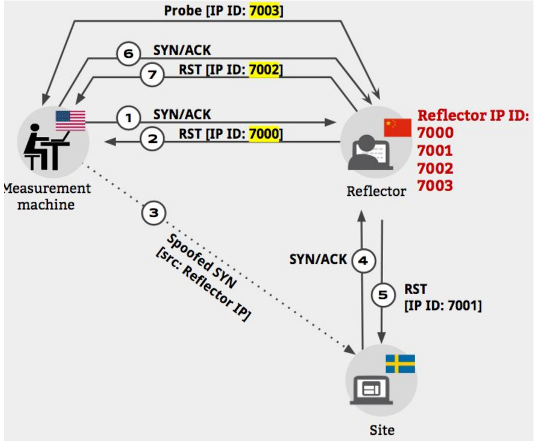
Server-to-Client Blocked

Δ IP_ID1 = 1
Δ IP_ID2 = 1



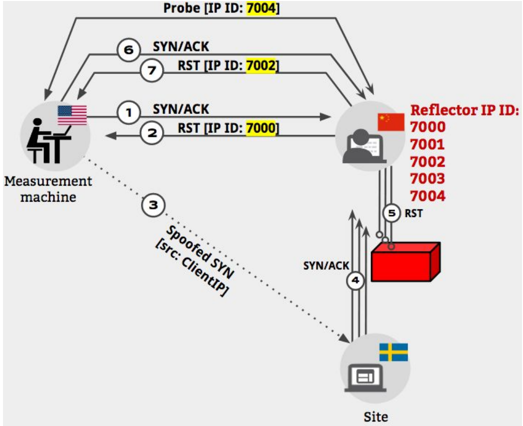
No Direction Blocked

Δ IP_ID1 = 2
Δ IP_ID2 = 1

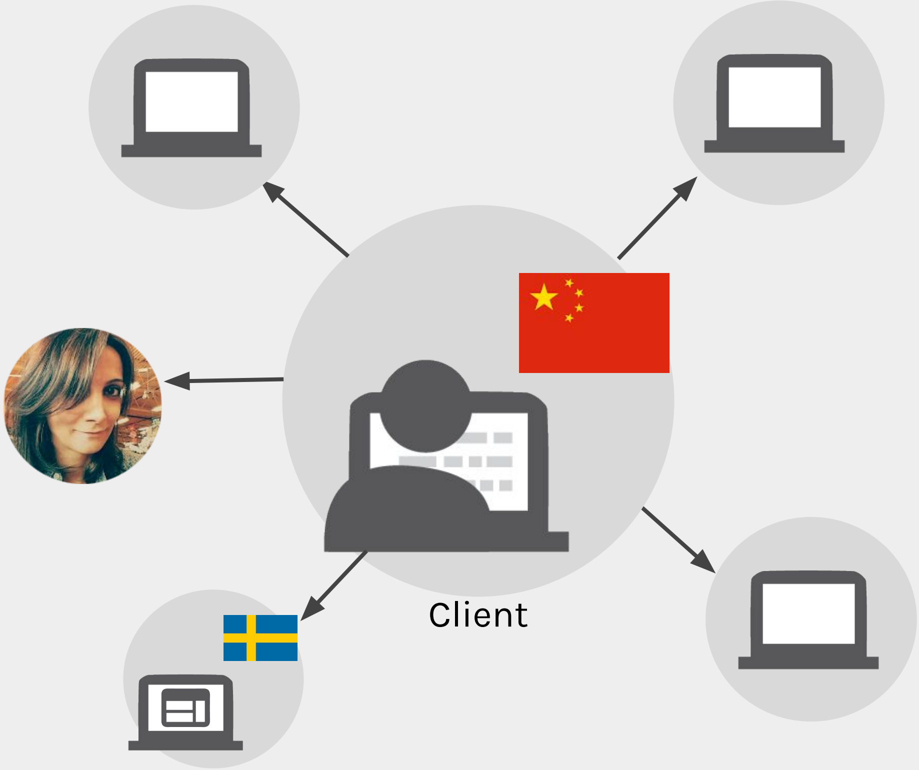


Client-to-Server Blocked

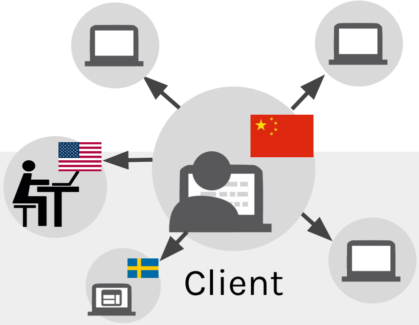
Δ IP_ID1 = 2
Δ IP_ID2 = 2



Client IP_ID Noise



Coping with Client IP_ID Noise

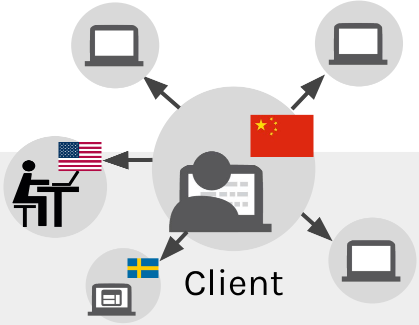


Amplifying the signal

Effect of sending *N* spoofed SYNs:

Server-to-Client Blocked	No Direction Blocked	Client-to-Server Blocked
Δ IP_ID1 = (1 + noise) Δ IP_ID2 = noise	Δ IP_ID1 = (1 + N + noise) Δ IP_ID2 = noise	Δ IP_ID1 = (1 + N + noise) Δ IP_ID2 = (1 + N + noise)

Coping with Client IP_ID Noise



Amplifying the signal

Effect of sending *N* spoofed SYNs:

Server-to-Client Blocked	No Direction Blocked	Client-to-Server Blocked
Δ IP_ID1 = (1 + noise) Δ IP_ID2 = noise	Δ IP_ID1 = (1 + N + noise) Δ IP_ID2 = noise	Δ IP_ID1 = (1 + N + noise) Δ IP_ID2 = (1 + N + noise)

Repeating the experiment

To eliminate the effects of packet loss, sudden bursts of packets, …

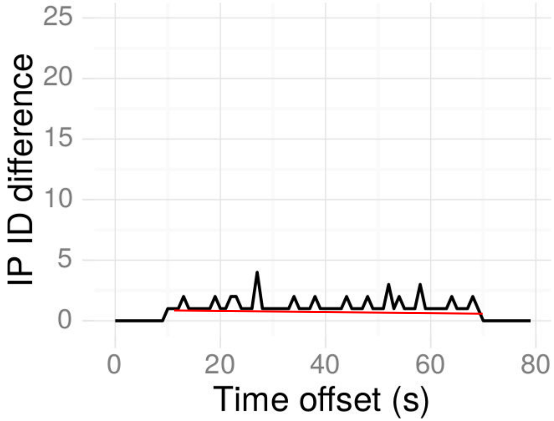
Spooky Scan with Noise: Visualization

Probing method

For first 30s, query IP_IDs. Then, for another 30s {
- Send 5 spoofed SYNs per second
- Query IP_ID once per second

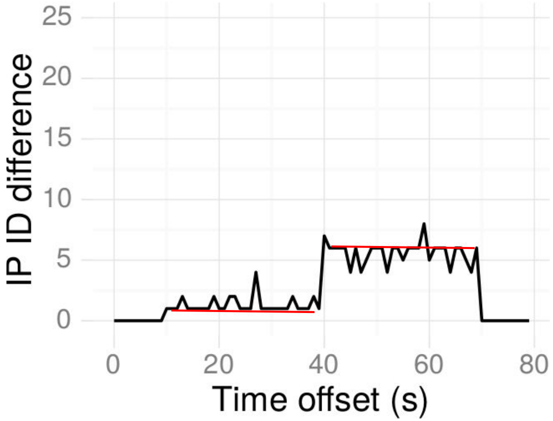
Server-to-Client Blocked

Tor relay (SE) to client (CN) blocked



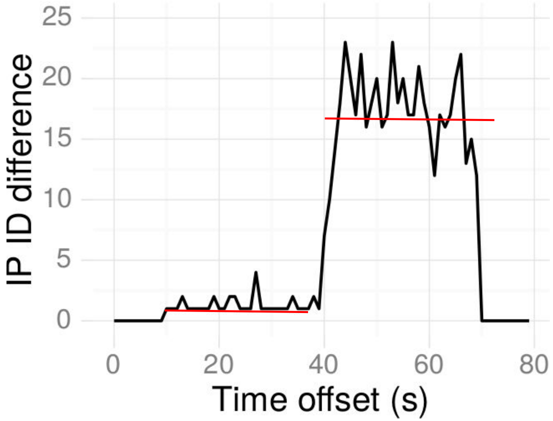
No Direction Blocked

No block btw client (US) and Tor relay (SE)

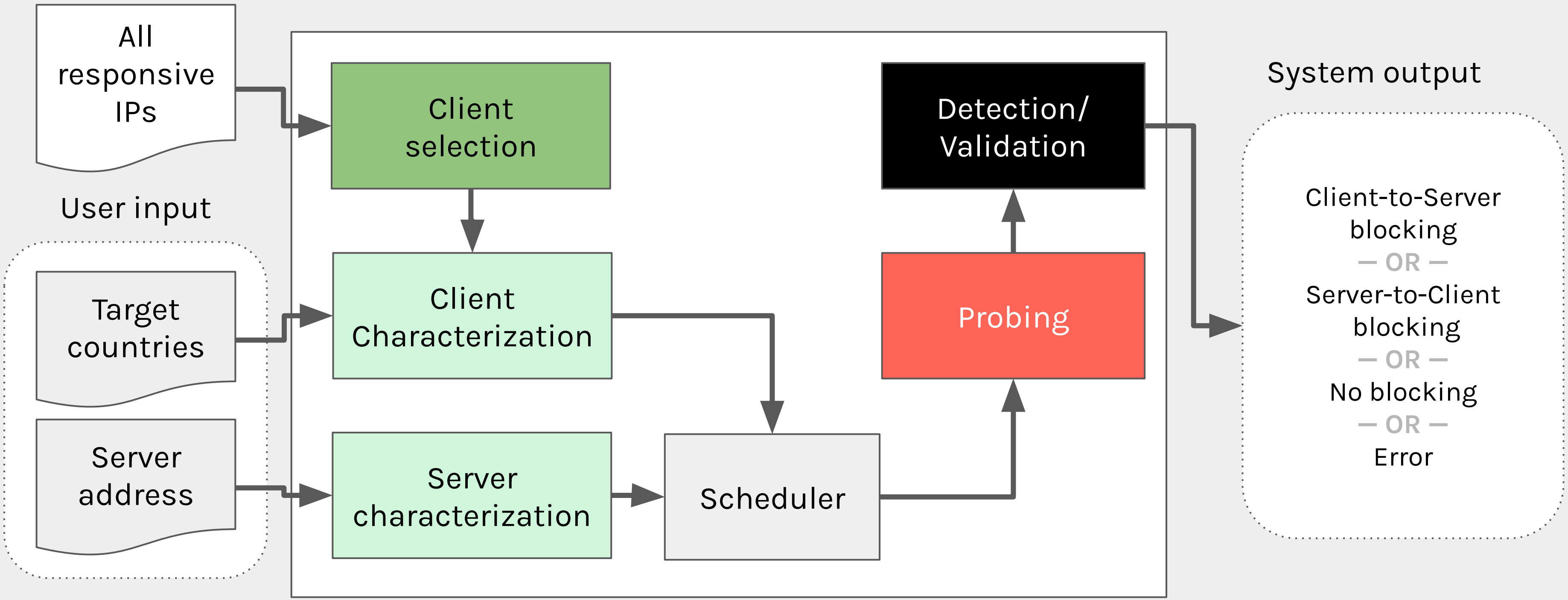


Client-to-Server Blocked

Client (AZ) to Tor relay (SE) blocked



Augur Framework



THREE KEY CHALLENGES:
✓ **Coverage, continuity, and ethics**

Coverage

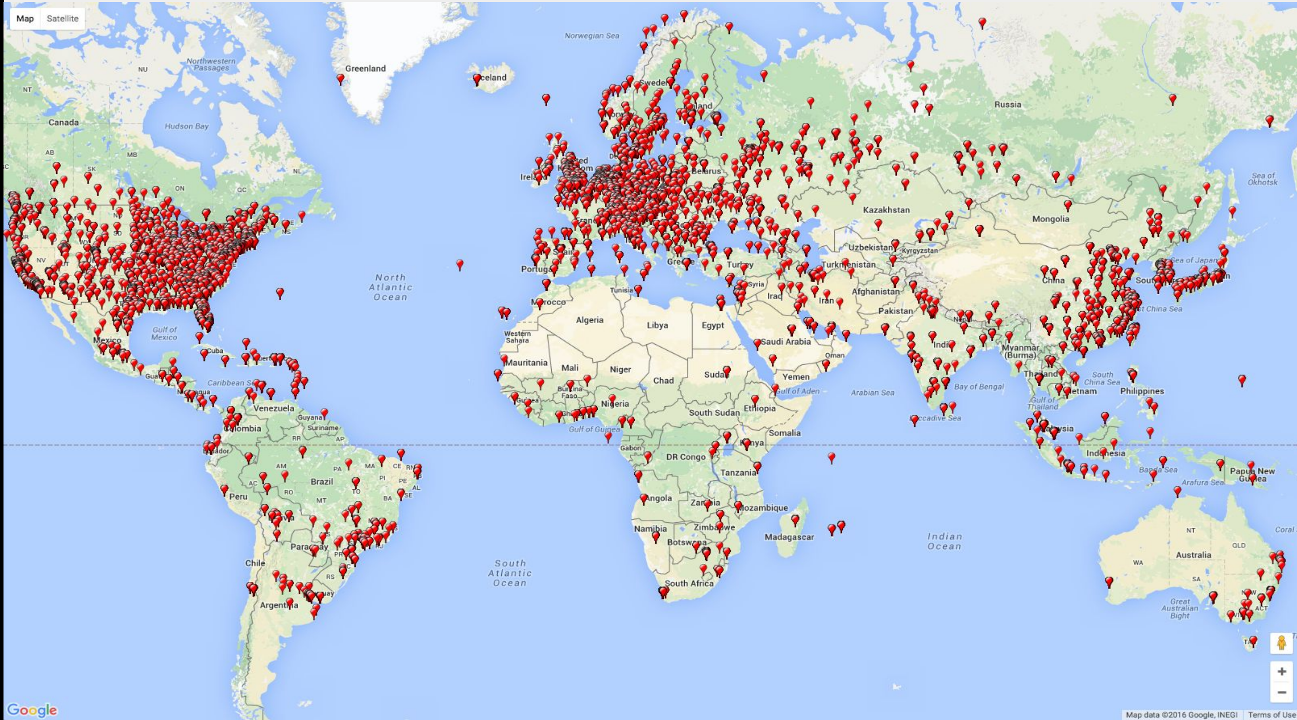
CHALLENGE:

Need global vantage points from which to measure

Scanning IPv4 on port 80:

22.7 million potential clients (with global IP_ID)

Compare: 10,000 in prior work (RIPE Atlas)



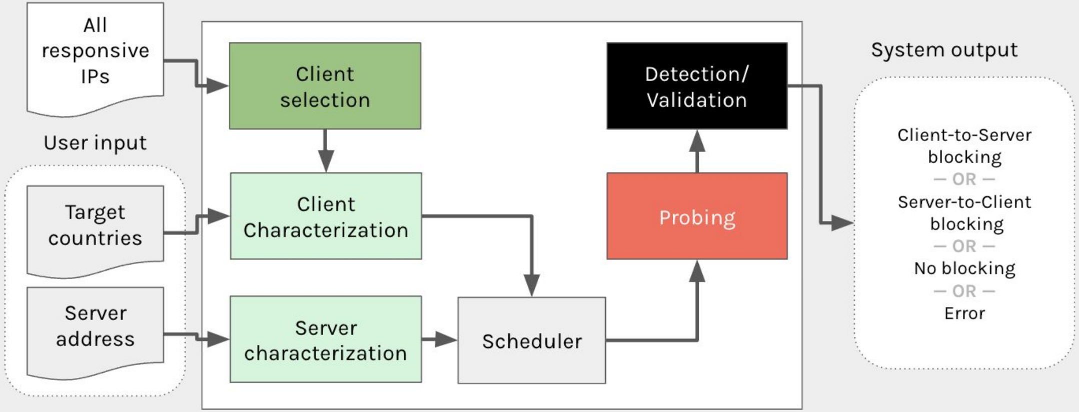
THREE KEY CHALLENGES:
Coverage ✓, continuity ✓, and ethics

Continuity

CHALLENGE:

Need to repeat measurements over time

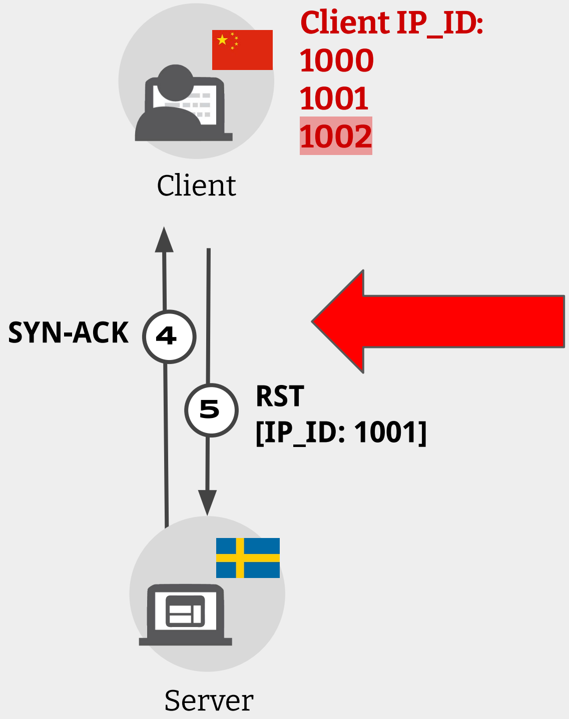
Augur doesn’t depend on end users’ participation, allowing us to collect measurements continuously.



Ethics

CHALLENGE:

Probing banned sites from users’ machines creates risk



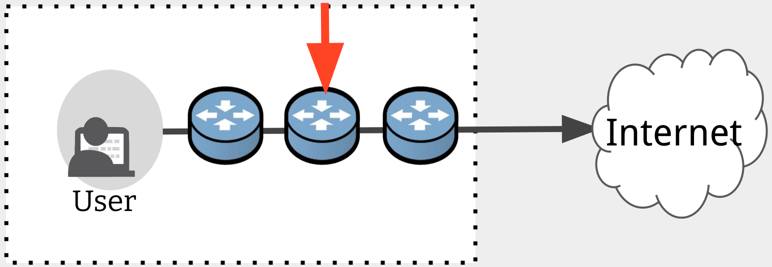
Ethics

CHALLENGE:

Probing banned sites from users' machines creates risk

THREE KEY CHALLENGES:
Coverage, continuity, and ethics ✓ ✓ ✓

Use only **infrastructure devices** to source probes



Global IP_ID	22.7 million	236 countries (and dependent territories)
Two hops back from end user	**53,000**	**180 countries**

From (Raw) Data points to Understanding Censorship?

Side channels

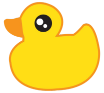
TCP/IP Layer

→ Spooky (2014)

→ Augur (2017)

DNS Layer

→ Satellite (2017)



Application Layer

→ Quack (2018)

→ HyperQuack (2020)

Challenges

- ➔ Disruption detection is not necessary censorship detection
- ➔ Ambiguity in location and granularity of filtering
- ➔ The techniques are each specialized to detect one type of censorship, and have only been used for a single snapshot in time

Building Censored Planet Observatory

NEED: A platform for continuously monitoring global Internet censorship

We build Censored Planet:

- ➔ **Orchestrate running remote measurement techniques**
- ➔ **Use data science to distill understanding**
- ➔ **Disseminate and facilitate data use**

Censored Planet

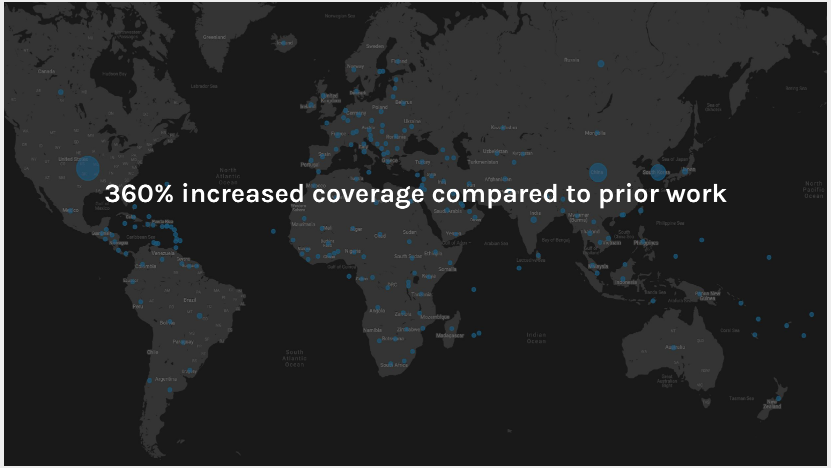
* **Censored Planet: An Internet-wide, Longitudinal Censorship Observatory**
R. Raman, P. Shenoy, K. Kohls, R. Ensafi
ACM CCS 2020

Orchestrate Running Side Channels

Censored Planet

From August 2018, **been running these side channels in parallel**

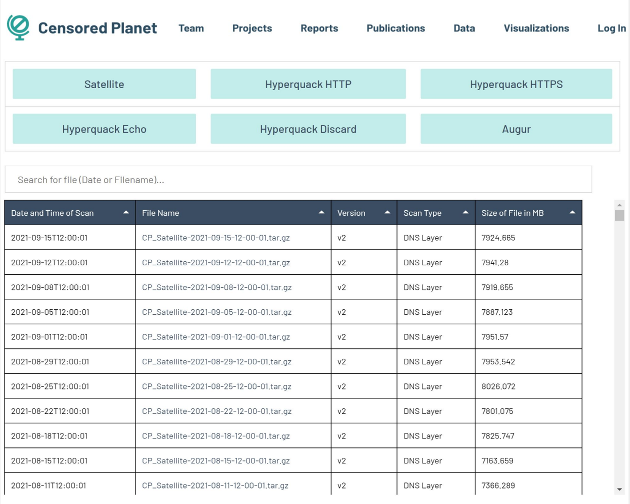
continuously testing reachability to 2000 sensitive domains from 95,000 vantage points!



360% increased coverage compared to prior work

49 billion data points

Largest public censorship dataset

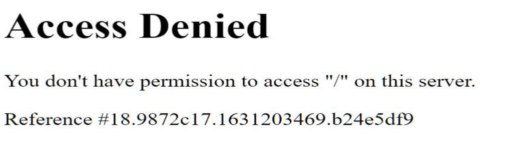


Date and Time of Scan	File Name	Version	Scan Type	Size of File in MB
2021-09-15T12:00:01	CP_Satellite-2021-09-15-12-00-01.tar.gz	v2	DNS Layer	7924.665
2021-09-12T12:00:01	CP_Satellite-2021-09-12-12-00-01.tar.gz	v2	DNS Layer	7941.28
2021-09-08T12:00:01	CP_Satellite-2021-09-08-12-00-01.tar.gz	v2	DNS Layer	7919.655
2021-09-05T12:00:01	CP_Satellite-2021-09-05-12-00-01.tar.gz	v2	DNS Layer	7887.123
2021-09-01T12:00:01	CP_Satellite-2021-09-01-12-00-01.tar.gz	v2	DNS Layer	7951.57
2021-08-29T12:00:01	CP_Satellite-2021-08-29-12-00-01.tar.gz	v2	DNS Layer	7953.542
2021-08-25T12:00:01	CP_Satellite-2021-08-25-12-00-01.tar.gz	v2	DNS Layer	8026.072
2021-08-22T12:00:01	CP_Satellite-2021-08-22-12-00-01.tar.gz	v2	DNS Layer	7801.075
2021-08-18T12:00:01	CP_Satellite-2021-08-18-12-00-01.tar.gz	v2	DNS Layer	7825.747
2021-08-15T12:00:01	CP_Satellite-2021-08-15-12-00-01.tar.gz	v2	DNS Layer	7163.659
2021-08-11T12:00:01	CP_Satellite-2021-08-11-12-00-01.tar.gz	v2	DNS Layer	7366.289

Challenges with Analyzing Censorship

Unexpected anomalies

1. CDN behavior

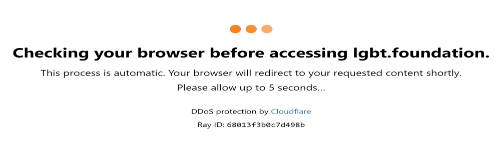


Access Denied

You don't have permission to access "/" on this server.

Reference #18.9872c17.1631203469.b24e5df9

2. Bot detection

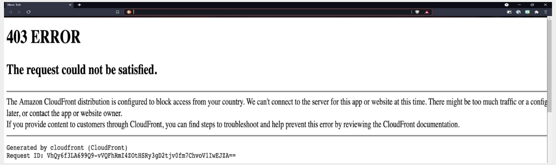


Checking your browser before accessing lgbt.foundation.

This process is automatic. Your browser will redirect to your requested content shortly.
Please allow up to 5 seconds...

DDoS protection by Cloudflare
Ray ID: 68013f3b0c7d498b

3. Geoblocking



403 ERROR

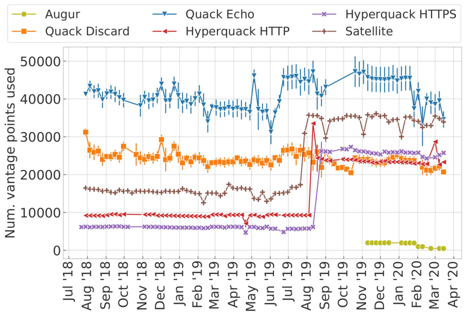
The request could not be satisfied.

The Amazon CloudFront distribution is configured to block access from your country. We can't connect to the server for this app or website at this time. There might be too much traffic or a config
later, or contact the app or website owner.
If you provide content to customers through CloudFront, you can find steps to troubleshoot and help prevent this error by reviewing the CloudFront documentation.

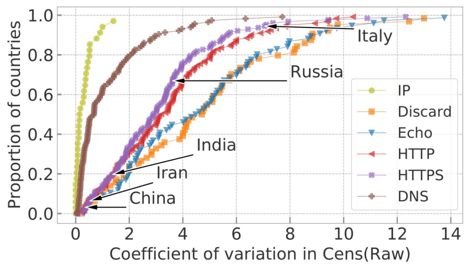
```
Generated by cloudfront (CloudFront)
Request ID: VhQy6f3LA699Q9-vVQFhRmI4ZOtHSRy3gD2tjv0fm7ChvoV1IwEJZA==
```

Temporal & Spatial Variance

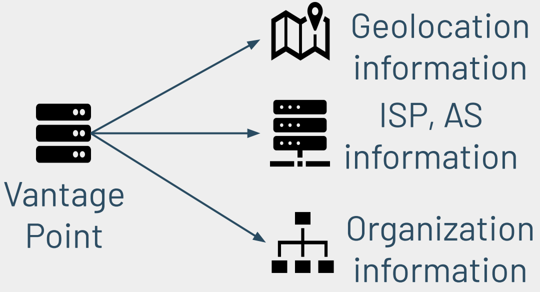
1. Vantage Point Changes



2. Organizational Policies



Insufficient Metadata



Vantage Point

Geolocation information

ISP, AS information

Organization information

Variance in Errors

Error Types
Resets
Timeout
DNS errors
TLS/HTTP errors

Analyzing Censorship

Building universal data schema

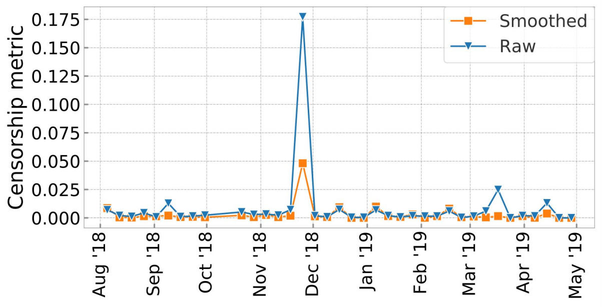
— that covers all techniques

Obtain a representative metric of censorship

— not every vantagepoint is equally weighted within a country

Dealing with outlier vantage points

— apply an **optimization model** (Nelder-Mead) to obtain a weight for each Autonomous System that smooths the metric.



Trend Analysis - Mann-Kendall test

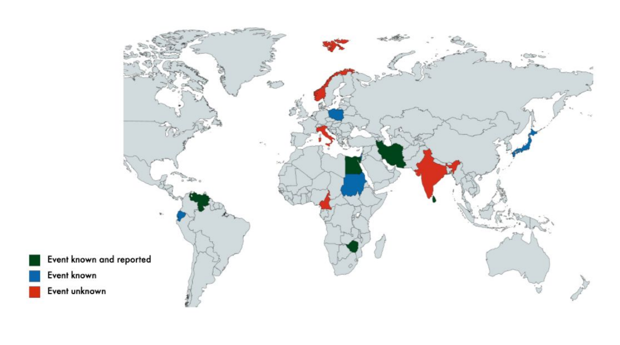
— Increasing levels of DNS censorship >100 countries.

— HTTPS censorship showing increasing trend.

— 11 categories of domains increasingly blocked e.g., News Media, Provocative Attire.

Anomaly Detection - Bitmap-based detection

— Identified 15 key censorship events

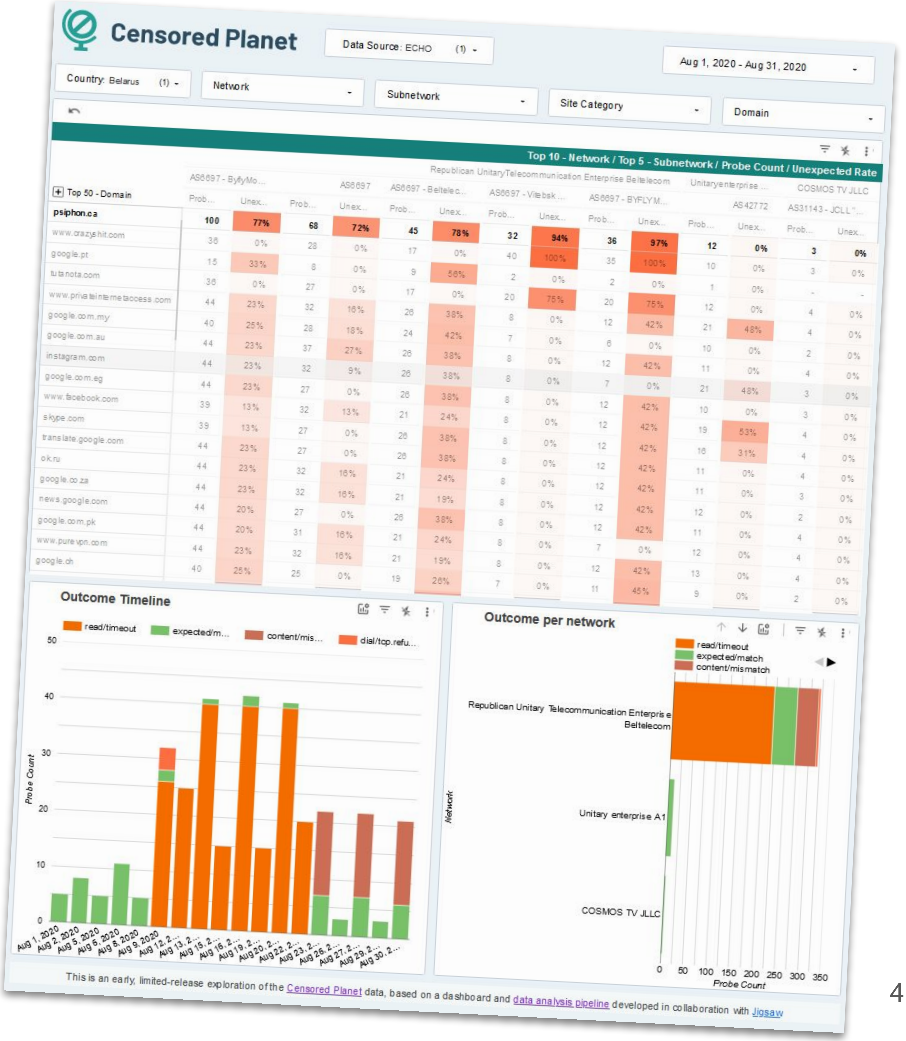


Censored Plant Dashboard

Developed in collaboration with Google's Jigsaw

To facilitate data use and enable easy visualizations, we built our dashboard that automatically gets updates after each scans.

We provide free access to our data users.



Censored Planet

Data Source: ECHO (1)

Aug 1, 2020 - Aug 31, 2020

Country: Belarus (1)

Network

Subnetwork

Site Category

Domain

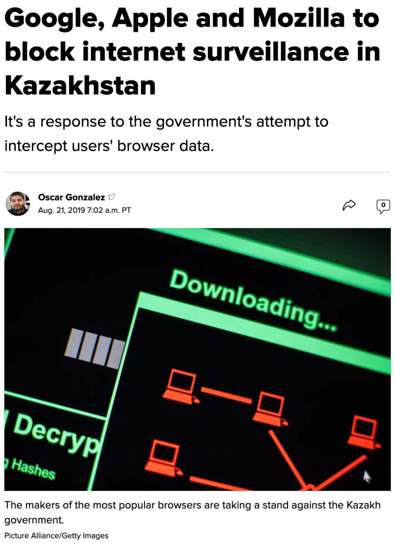
Top 10 - Network / Top 5 - Subnetwork / Probe Count / Unexpected Rate

Top 50 - Domain	Republican UnitaryTelecommunication Enterprise Beltelecom										Unitaryenterprise ...		COSMOS TV JLLC	
	AS6697 - ByflyMo...		AS6697		AS6697 - Beltelec...		AS6697 - Vitebsk ...		AS6697 - BYFLY M...		AS42772		AS31143 - JCLL "...	
	Prob...	Unex...	Prob...	Unex...	Prob...	Unex...	Prob...	Unex...	Prob...	Unex...	Prob...	Unex...	Prob...	Unex...
psiphon.ca	**100**	**77%**	**68**	**72%**	**45**	**78%**	**32**	**94%**	**36**	**97%**	**12**	**0%**	**3**	**0%**
www.crazyshit.com	36	0%	28	0%	17	0%	40	100%	35	100%	10	0%	3	0%
google.pt	15	33%	8	0%	9	56%	2	0%	2	0%	1	0%	-	-
tutanota.com	36	0%	27	0%	17	0%	20	75%	20	75%	12	0%	4	0%
www.privateinternetaccess.com	44	23%	32	16%	26	38%	8	0%	12	42%	21	48%	4	0%
google.com.my	40	25%	28	18%	24	42%	7	0%	6	0%	10	0%	2	0%
google.com.au	44	23%	37	27%	26	38%	8	0%	12	42%	11	0%	4	0%
instagram.com	44	23%	32	9%	26	38%	8	0%	7	0%	21	48%	3	0%
google.com.eg	44	23%	27	0%	26	38%	8	0%	12	42%	10	0%	3	0%
www.facebook.com	39	13%	32	13%	21	24%	8	0%	12	42%	19	53%	4	0%
skype.com	39	13%	27	0%	26	38%	8	0%	12	42%	16	31%	4	0%
translate.google.com	44	23%	27	0%	26	38%	8	0%	12	42%	11	0%	4	0%
ok.ru	44	23%	32	16%	21	24%	8	0%	12	42%	11	0%	3	0%
google.co.za	44	23%	32	16%	21	19%	8	0%	12	42%	12	0%	2	0%
news.google.com	44	20%	27	0%	26	38%	8	0%	12	42%	11	0%	4	0%
google.com.pk	44	20%	31	16%	21	24%	8	0%	7	0%	12	0%	4	0%
www.purevpn.com	44	23%	32	16%	21	19%	8	0%	12	42%	13	0%	4	0%
google.ch	40	25%	25	0%	19	26%	7	0%	11	45%	9	0%	2	0%

This is an early, limited-release exploration of the Censored Planet data, based on a dashboard and data analysis pipeline developed in collaboration with Jigsaw

Censored Planet Rapid Response

Censored Planet team has exposed significant new government censorship tactics, and our results have been highlighted in more than 100 popular press articles.



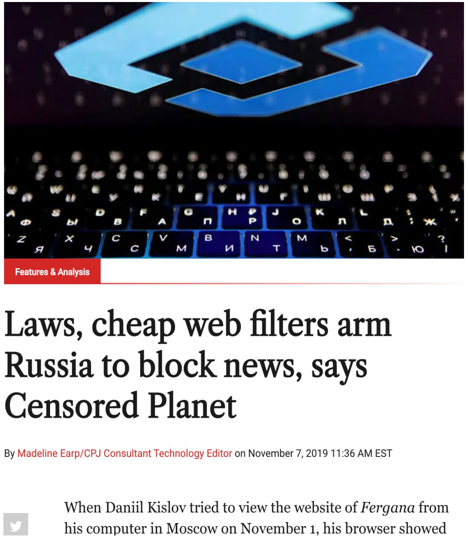
Google, Apple and Mozilla to block internet surveillance in Kazakhstan

It's a response to the government's attempt to intercept users' browser data.

Oscar Gonzalez
Aug. 21, 2019 7:02 a.m. PT

The makers of the most popular browsers are taking a stand against the Kazakh government.

Picture Alliance/Getty Images

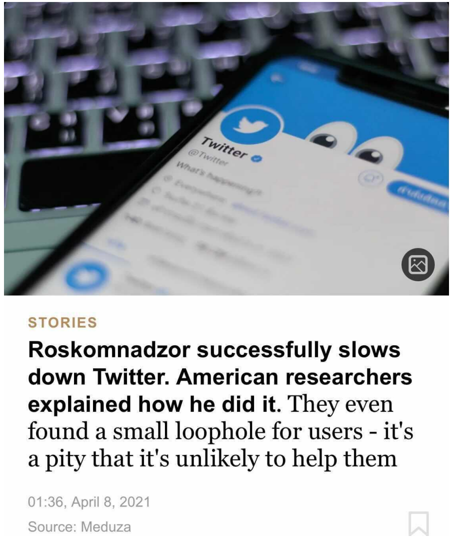


Features & Analysis

Laws, cheap web filters arm Russia to block news, says Censored Planet

By Madeline Earp/CPJ Consultant Technology Editor on November 7, 2019 11:36 AM EST

When Daniil Kislov tried to view the website of *Fergana* from his computer in Moscow on November 1, his browser showed

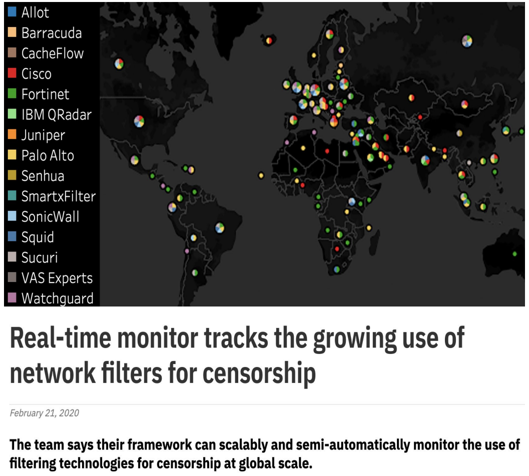


STORIES

Roskomnadzor successfully slows down Twitter. American researchers explained how he did it. They even found a small loophole for users - it's a pity that it's unlikely to help them

01:36, April 8, 2021

Source: Meduza



Real-time monitor tracks the growing use of network filters for censorship

February 21, 2020

The team says their framework can scalably and semi-automatically monitor the use of filtering technologies for censorship at global scale.

Censored Planet

Research papers

IMC '21
Throttling Twitter: an emerging censorship technique in Russia

FC '21
Lost in Transmission: Investigating Filtering of COVID-19 Websites

CCS '20
Censored planet: an internet-wide, longitudinal censorship observatory

IMC '20
Investigating large scale HTTPS interception in Kazakhstan

NDSS '20
Decentralized Control: A Case Study of Russia

NDSS '20
Measuring the deployment of network censorship filters at global scale

USENIX '18
Quack: Scalable Remote Measurement of {Application-Layer} Censorship

S&P '17
Augur: Internet-wide detection of connectivity disruptions

IEEE Security & Privacy '18
Toward continual measurement of global network-level censorship

USENIX '17
Global measurement of {DNS} manipulation

IMC '17
A look at router geolocation in public and commercial databases

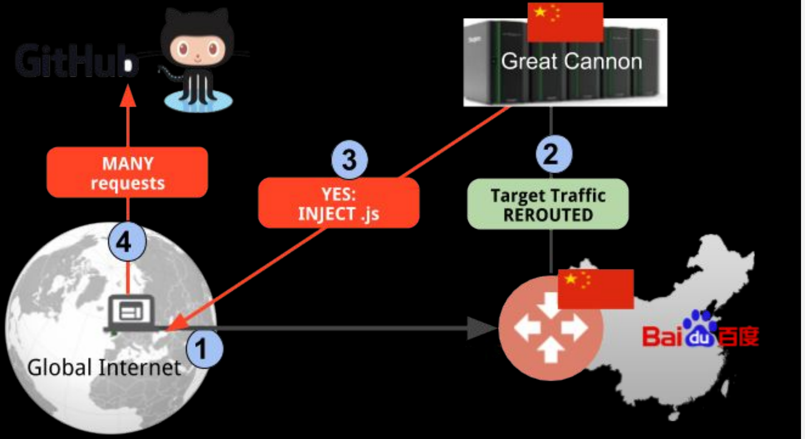
NS ETHICS '15
Ethical Concerns for Censorship Measurement

PETS '15
Analyzing the Great Firewall of China Over Space and Time.

PAM '14
Detecting intentional packet drops on the Internet via TCP/IP side channels

Other work:

Understanding the Technology of Interference



TSPU: Russia's Decentralized Censorship System
In: ACM IMC , October 2022

Measurement Methods for Locating & Examining Censorship Devices
CoNEXT 2023 🏆 IRTF Applied Networking Research Prize winner

Throttling Twitter: An Emerging Censorship Technique in Russia
In: ACM IMC, November 2021

Decentralized Control: A Case Study of Russia
In: NDSS, February 2020

Censorship in Russia
Report: https://censoredplanet.org/russia

Examining How the Great Firewall Discovers Hidden Circumvention Servers
ACM Internet Measurement Conference (IMC), October 2015
IRTF (IETF) Applied Networking Research Prize winner

Analyzing the Great Firewall of China Over Space and Time
Privacy Enhancing Technologies Symposium (PETS), July 2015

An Analysis of China's Great Cannon
USENIX FOCI, August 2015

VPNalyzer

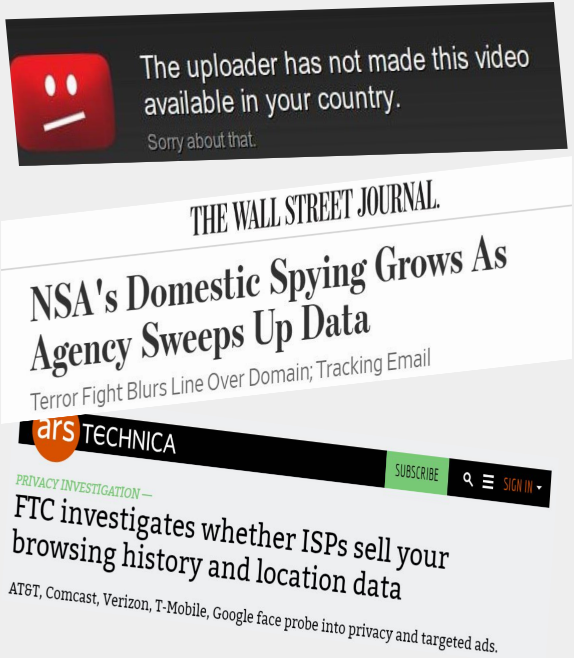
Safeguarding the consumer VPN ecosystem

"All of them claim to be the best": Multi-perspective study of VPN users and VPN providers
R. Ramesh, A. Vyas, R. Ensafi
Under submission

OpenVPN is Open to VPN Fingerprinting
D. Xue, R. Ramesh, M. Kallitsis, J. Halderman, J. Crandall, R. Ensafi
USENIX Security, August 2022
🏆 Distinguished paper award
🏆 Won First Prize in the 2022 Internet Defense Prize

VPNalyzer: Systematic Investigation of the VPN Ecosystem
R. Ramesh, L. Evdokimov, D. Xue,R. Ensafi
NDSS, Apr 2022

VPNs are on the Rise



The uploader has not made this video available in your country.

Sorry about that.

THE WALL STREET JOURNAL.

NSA's Domestic Spying Grows As Agency Sweeps Up Data

Terror Fight Blurs Line Over Domain; Tracking Email

ars TECHNICA

PRIVACY INVESTIGATION —

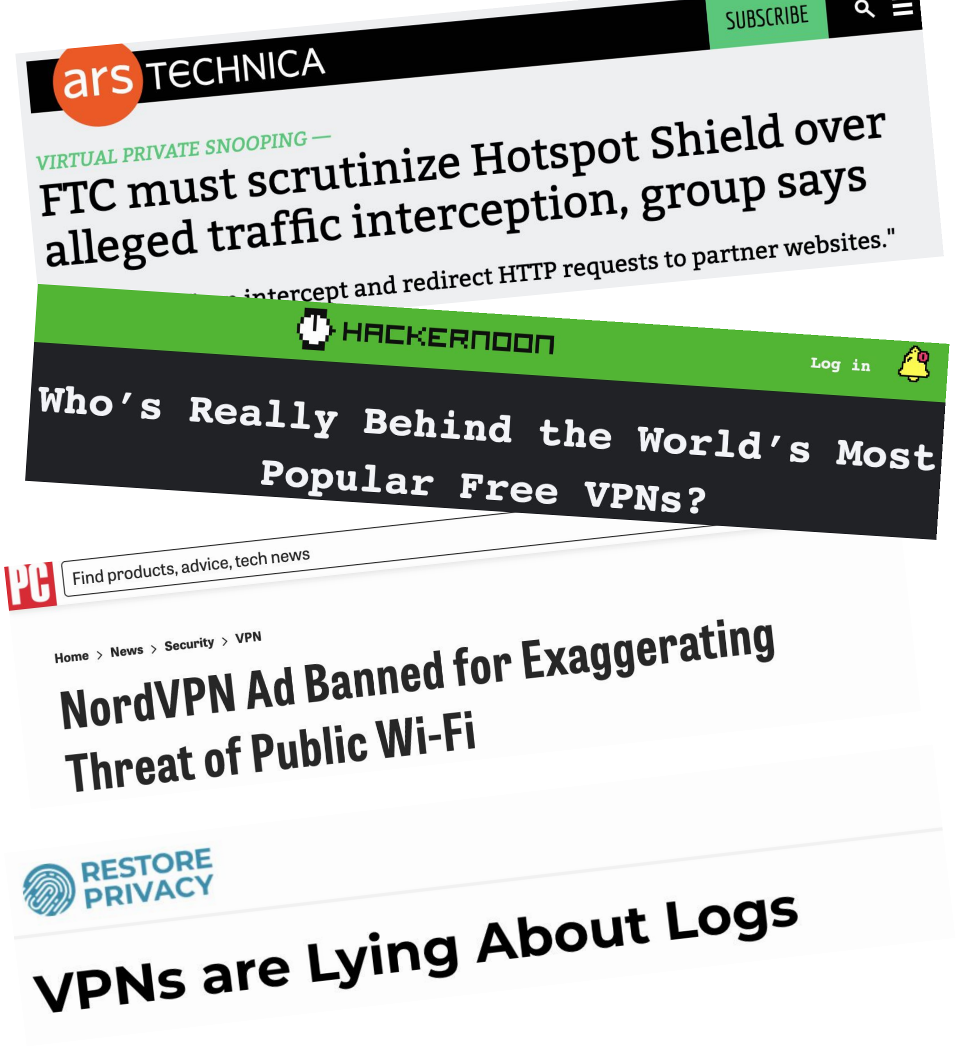
FTC investigates whether ISPs sell your browsing history and location data

AT&T, Comcast, Verizon, T-Mobile, Google face probe into privacy and targeted ads.

“From 2010 to year-end 2019, the use of VPNs has increased by **approximately four times”**
American cybersecurity company PC Matic

“VPN usage increased 3% week over week and hit a new peak at 81% higher than a typical pre-COVID day”
Verizon Network Report, May, 2020

Reasons:
Protection from surveillance, censorship circumvention, accessing work/school/university resources, circumventing geo-blocking, entertainment, etc



ars TECHNICA

SUBSCRIBE

VIRTUAL PRIVATE SNOOPING —

FTC must scrutinize Hotspot Shield over alleged traffic interception, group says

intercept and redirect HTTP requests to partner websites."

HACKERNOON

Log in

Who's Really Behind the World's Most Popular Free VPNs?

PC

Find products, advice, tech news

Home > News > Security > VPN

NordVPN Ad Banned for Exaggerating Threat of Public Wi-Fi

RESTORE PRIVACY

VPNs are Lying About Logs

This multibillion-dollar industry includes many snakeoil products, hyperbolic claims, is laxly regulated, and remains severely understudied.

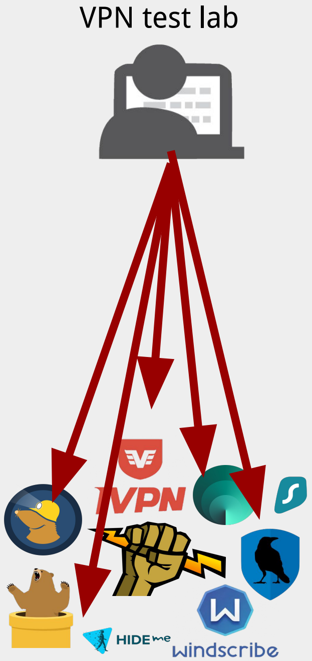
Challenges to Investigating VPNs

Previous reports are lab-based:

- Used inconsistent heuristics that prevent monitoring of issues over time (unsystematic investigation)
- Limited in the scale and types of VPN products (covering only a small slice of the market)
- Involved a large amount of manual effort

KEY CHALLENGE:

Rigor, Scale, Automation



We built VPNalyzer

to address these challenges

Building VPNalyzer to Address Key Challenges

Repeated VPN evaluations over time **should not require** starting from scratch

Testing and validating VPN providers’ fixes for issues reported as disclosures requires an easily updatable test suite

VPNalyzer must adopt a modular, extensible test suite implementation

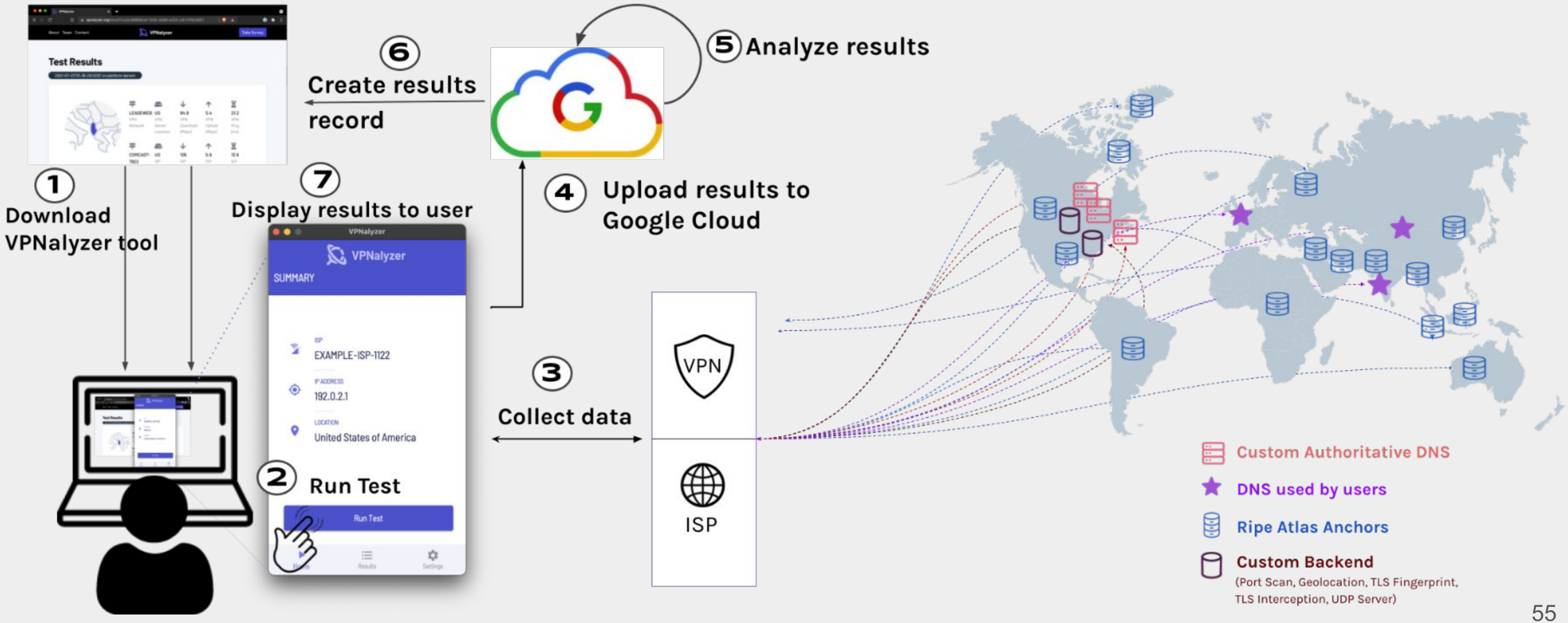
VPN ecosystem has increasing:

- number of VPN providers
- number of users w/ varied threat models
- use cases

VPNalyzer must facilitate large-scale crowd-sourced measurements

VPNalyzer System Design

User-friendly tool with a one-click install process for Windows, MacOS, and Linux



ISP
EXAMPLE-ISP-1122

IP ADDRESS
192.0.2.1

LOCATION
United States of America

- 🟥 Custom Authoritative DNS
- ★ DNS used by users
- 🛢 Ripe Atlas Anchors
- 🛢 Custom Backend (Port Scan, Geolocation, TLS Fingerprint, TLS Interception, UDP Server)

What do we test with VPNalyzer?

VPNalyzer has a modular, extensible test suite covering aspects of performance, security, and privacy

Aspects of Service

Bandwidth and latency

Geolocation

RPKI validation

Misconfiguration and Leakages

DNS leaks

IPv6 leaks

Data leaks during tunnel failure

Security and Privacy Essentials

Lack of support for DoH

TLS Interception

Port scanning

Router interface reachability

Presence of DNS proxy

QNAME minimization

Testing VPNalyzer

We tested VPNalyzer with **80 popular VPNs** and uncovered dozens of previously unreported problems

We tested random servers in each VPN provider, on Windows and MacOS for VPN default and secure mode:

- **58 paid** VPN providers
- **18 free** VPN providers
- **4 self-hosted** VPN solutions (Algo, OpenVPN Access Server on AWS, Outline, Streisand)

VPNalyzer Findings: Misconfiguration and Leakages

VPNalyzer found evidence of many traffic leaks, which seriously risk exposing sensitive user data.

IPV6 traffic

Only 14% support IPv6

Five VPNs leak IPv6 traffic to the ISP by default

UMich VPN is among them

VPNalyzer Findings: Misconfiguration and Leakages

VPNalyzer found evidence of many traffic leaks, which seriously risk exposing sensitive user data.

IPV6 traffic

Only 14% support IPv6

Five VPNs leak IPv6 traffic to the ISP by default

UMich VPN is among them

During tunnel failure

In default configuration, **33% of providers leak traffic** to the user's ISP

Even in their most secure setting, 10 providers leak traffic to the user's ISP

VPNalyzer Findings: Misconfiguration and Leakages

VPNalyzer found evidence of many traffic leaks, which seriously risk exposing sensitive user data.

IPV6 traffic

Only 14% support IPv6

Five VPNs leak IPv6 traffic to the ISP by default

UMich VPN is among them

During tunnel failure

In default configuration, **33% of providers leak traffic** to the user’s ISP

Even in their most secure setting, 10 providers leak traffic to the user’s ISP

Insecure default configuration

Misleading default configuration caused (non-browser) traffic to be exposed to the ISP

Astrill VPN and Psiphon tunneled only browser traffic by default

VPNalyzer team filed 26 disclosure to these VPNs due to security and privacy risk exposing sensitive user data through traffic leaks

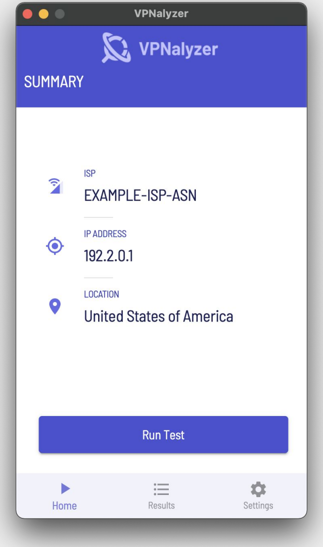
Filed Responsible Disclosures

What’s Next: Deployment and Crowdsourcing

VPNalyzer.org/beta

Crowdsourced study:

- Help scale coverage to many hundreds of providers
- Study region-specific VPNs that are often overlooked



VPNalyzer

VPNalyzer

SUMMARY

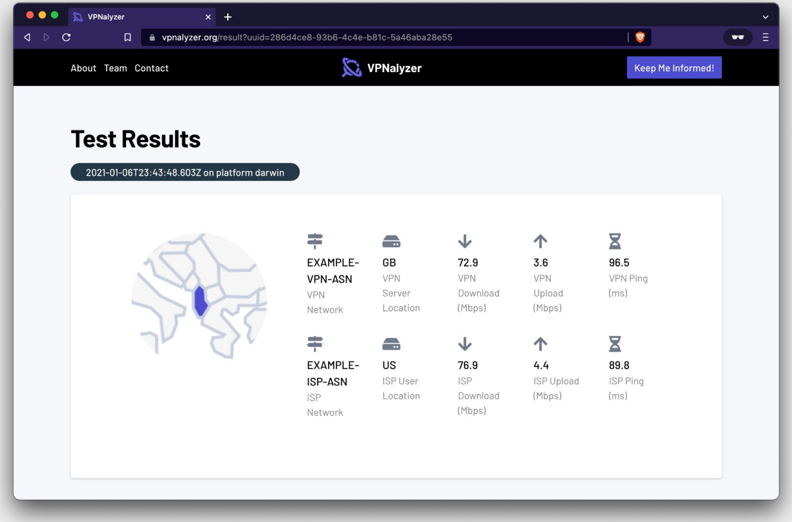
ISP
EXAMPLE-ISP-ASN

IP ADDRESS
192.2.0.1

LOCATION
United States of America

Run Test

For the future, crowdsourcing will provide continuous data from users to spot new problems, monitor fixes for known issues, and keep findings up to date



VPNalyzer

vpnalyzer.org/result?uuid=286d4ce8-93b6-4c4e-b81c-5a46aba28e55

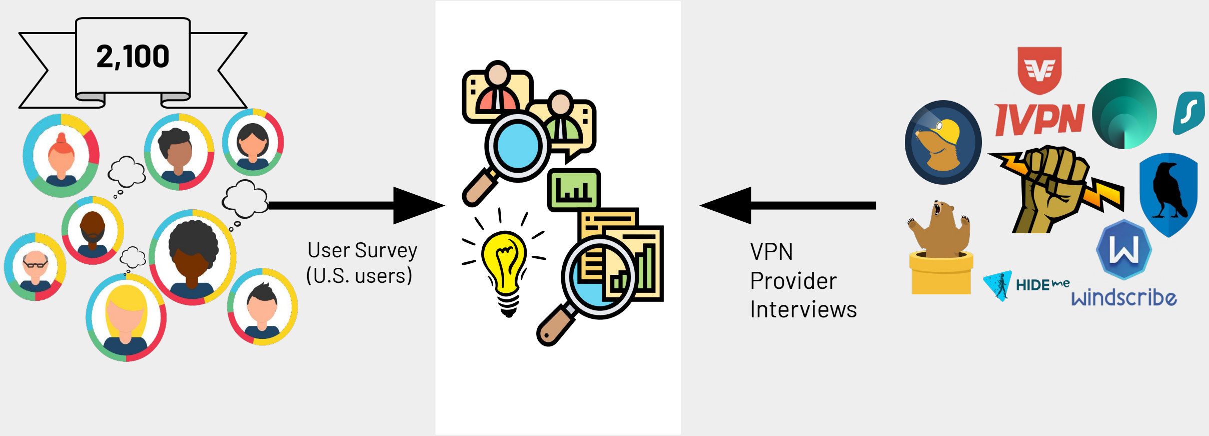
Test Results

2021-01-06T23:43:48.603Z on platform darwin

EXAMPLE-VPN-ASN VPN Network	GB VPN Server Location	72.9 VPN Download (Mbps)	3.6 VPN Upload (Mbps)	96.5 VPN Ping (ms)
EXAMPLE-ISP-ASN ISP Network	US ISP User Location	76.9 ISP Download (Mbps)	4.4 ISP Upload (Mbps)	89.8 ISP Ping (ms)

Measuring the Efficacy of Currently Deployed Tools

Understanding the user needs and considerations, and VPN providers to bridge gaps and highlight (mis)aligned incentives



2,100

User Survey
(U.S. users)

VPN
Provider
Interviews

"All of them claim to be the best": Multi-perspective study of VPN users and VPN providers R. Ramesh, A. Vyas, R. Ensafi, USENUX 2023

Multi-perspective study of VPN users and VPN providers

With support from Consumer Reports, our survey received 2,100 responses from > 40 countries

User study highlight:

86.7% of users feel somewhat/very safe using a VPN

40% of users have a flawed mental model of the security their VPN provides (no significant difference between users of different expertise)

57% of users are highly reliant on VPN recommendation sites (of whom 94% rate them trustworthy)

Multi-perspective study of VPN users and VPN providers

With support from Consumer Reports, our survey received 2,100 responses from > 40 countries

User study highlight:

86.7% of users feel somewhat/very safe using a VPN

40% of users have a flawed mental model of the security their VPN provides (no significant difference between users of different expertise)

Price is a big criteria for limited-to-moderate expertise users → exploited by malicious marketing

57% of users are highly reliant on VPN recommendation sites (of whom 94% rate them trustworthy)

VPN provider highlight:

VPN providers reveal recommendation sites are largely **not objective** and instead are **motivated by profit**

“You honestly cannot find even one ranking site that is honest, if you just tell people that…so that people know”

Multi-perspective study of VPN users and VPN providers

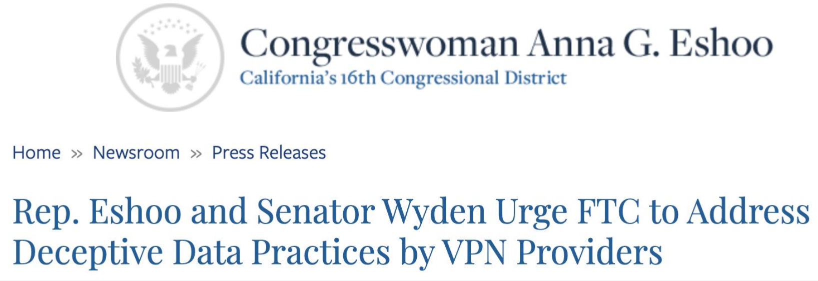
With support from Consumer Reports, our survey received 2,100 responses from > 40 countries

Big lesson:

- Prioritizing user education
- Oversight on advertisements and marketing surrounding VPNs
- Regulations to curb misleading marketing that leads to flawed mental models

VPNalyzer Impact

Consumer Reports used our **VPNalyzer tool** for their own investigation to help recommend VPNs to their millions of subscribers

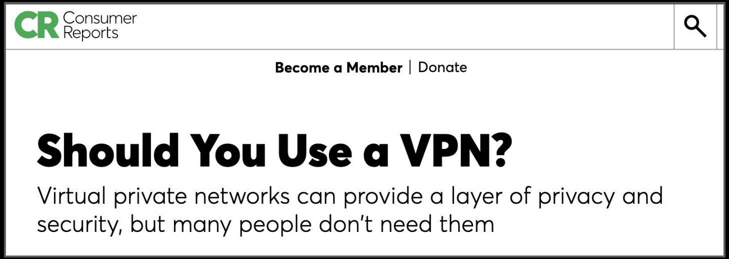


Congresswoman Anna G. Eshoo

California's 16th Congressional District

Home » Newsroom » Press Releases

Rep. Eshoo and Senator Wyden Urge FTC to Address Deceptive Data Practices by VPN Providers

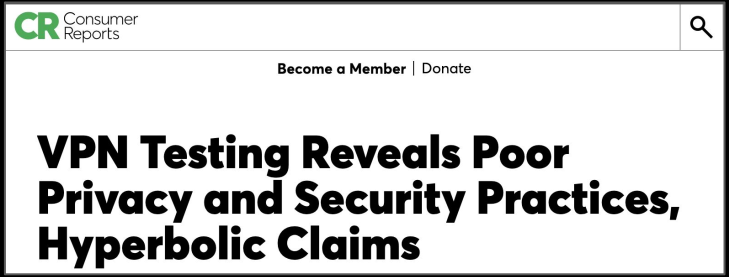


Consumer Reports

Become a Member | Donate

Should You Use a VPN?

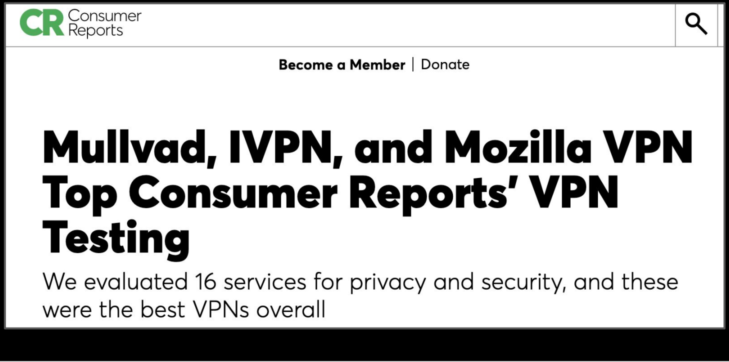
Virtual private networks can provide a layer of privacy and security, but many people don't need them



Consumer Reports

Become a Member | Donate

VPN Testing Reveals Poor Privacy and Security Practices, Hyperbolic Claims



Consumer Reports

Become a Member | Donate

Mullvad, IVPN, and Mozilla VPN Top Consumer Reports' VPN Testing

We evaluated 16 services for privacy and security, and these were the best VPNs overall

Other work:

Investigating the Geo-inequity of users’ online experiences

splintering.net

Understanding the effect of server-side blocking and embargo sanctions to daily life of Iranians and Cubans

R Sundra Ramen, R Ramesh, G. Li, D. Madory, R. Ensafi

Under progress

A large-scale investigation into geo-differences in mobile apps.

R. Kumar, A. Virkud, R. Sundara Raman,A. Prakash,R. Ensafi.

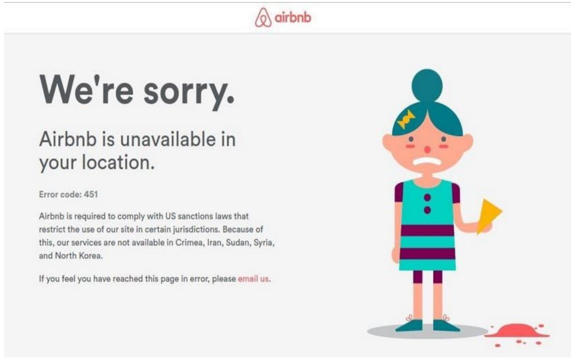
In USENIX Security, 2022.

403 Forbidden: A Global View of CDN Geoblocking

A. McDonald, M. Bernhard, B. VanderSloot, W. Scott, A. Halderman, R. Ensafi

ACM Internet Measurement Conference (IMC), November 2018

Server-side geo-discrimination is on the rise→ Balkanization of Internet



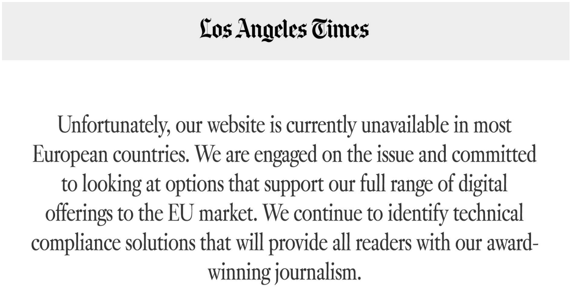
We're sorry.

Airbnb is unavailable in your location.

Error code: 451

Airbnb is required to comply with US sanctions laws that restrict the use of our site in certain jurisdictions. Because of this, our services are not available in Crimea, Iran, Sudan, Syria, and North Korea.

If you feel you have reached this page in error, please email us.



Unfortunately, our website is currently unavailable in most European countries. We are engaged on the issue and committed to looking at options that support our full range of digital offerings to the EU market. We continue to identify technical compliance solutions that will provide all readers with our award-winning journalism.

Measuring geo-blocking

Why do sites Geoblock?

Sites may attempt to minimize fraud or **combat abuse.**

Iran, Syria, Sudan, North Korea and Cuba are under **U.S. sanctions**, some companies block access to comply.

Increasingly CDNs make it easy to block sites by a click by offering a easy accable country-level blocking tool in their client's portal.

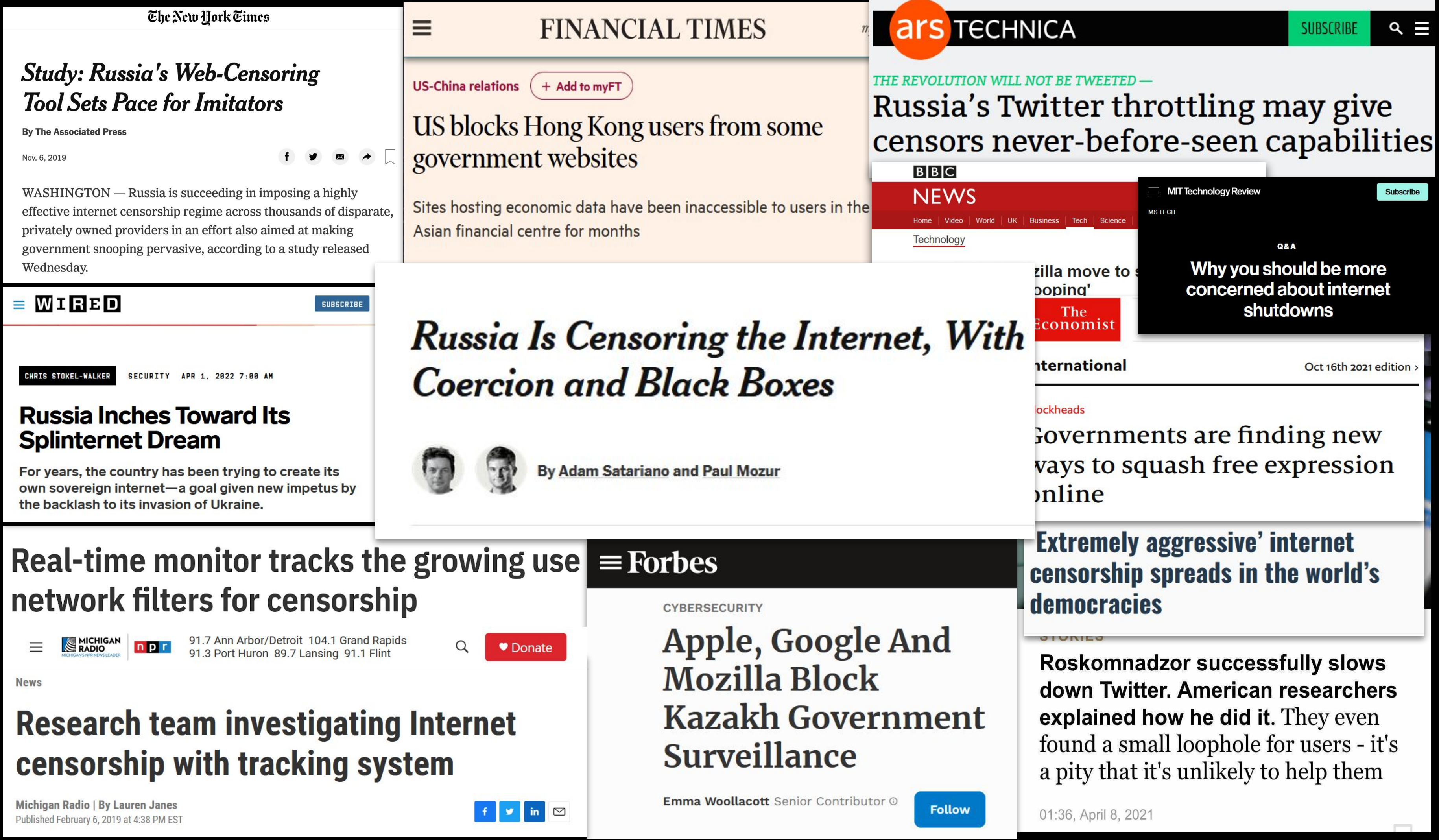
Impact: Subsequent to our study, **CloudFlare disabled geoblocking** for all but Enterprise customers.

CLOUDFLARE®

What next:

A first large-scale investigation into geo-differences in mobile apps. **[USENIX Security 2022]**

Understanding the effect of server-side blocking and embargo sanctions to daily life of Iranians and Cubans



The New York Times

Study: Russia's Web-Censoring Tool Sets Pace for Imitators

By The Associated Press

Nov. 6, 2019

WASHINGTON — Russia is succeeding in imposing a highly effective internet censorship regime across thousands of disparate, privately owned providers in an effort also aimed at making government snooping pervasive, according to a study released Wednesday.

FINANCIAL TIMES

US-China relations + Add to myFT

US blocks Hong Kong users from some government websites

Sites hosting economic data have been inaccessible to users in the Asian financial centre for months

ars TECHNICA SUBSCRIBE

THE REVOLUTION WILL NOT BE TWEETED —

Russia's Twitter throttling may give censors never-before-seen capabilities

BBC NEWS

Home | Video | World | UK | Business | Tech | Science

Technology

zilla move to s
ooping'

MIT Technology Review Subscribe

MS TECH

Q&A

Why you should be more concerned about internet shutdowns

Russia Is Censoring the Internet, With Coercion and Black Boxes

By Adam Satariano and Paul Mozur

WIRED SUBSCRIBE

CHRIS STOKEL-WALKER SECURITY APR 1, 2022 7:00 AM

Russia Inches Toward Its Splinternet Dream

For years, the country has been trying to create its own sovereign internet—a goal given new impetus by the backlash to its invasion of Ukraine.

The Economist

nternational Oct 16th 2021 edition ›

lockheads

Governments are finding new ways to squash free expression online

Extremely aggressive' internet censorship spreads in the world's democracies

Real-time monitor tracks the growing use network filters for censorship

MICHIGAN RADIO npr 91.7 Ann Arbor/Detroit 104.1 Grand Rapids 91.3 Port Huron 89.7 Lansing 91.1 Flint Donate

News

Research team investigating Internet censorship with tracking system

Michigan Radio | By Lauren Janes
Published February 6, 2019 at 4:38 PM EST

Forbes

CYBERSECURITY

Apple, Google And Mozilla Block Kazakh Government Surveillance

Emma Woollacott Senior Contributor Follow

STORIES

Roskomnadzor successfully slows down Twitter. American researchers explained how he did it. They even found a small loophole for users - it's a pity that it's unlikely to help them

01:36, April 8, 2021

SUMMIT FOR DEMOCRACY
TRUEPIC
TRUEPIC
PARK CITY · UTAH

U.S.-GERMAN FUTURES FORUM
DEUTSCH-AMERIKANISCHES ZUKUNFTSFORUM
The Future of Democracy in a Digital World
November 2-
Münster

Auswärtiges Amt
BertelsmannStiftung
AICGS American Institute for Contemporary German Studies
U.S.-GERMAN FUTURES FORUM
DEUTSCH-AMERIKANISCHES ZUKUNFTSFORUM
The Future of Democracy in a Digital World
November 2-3, 2022
Münster, Germany

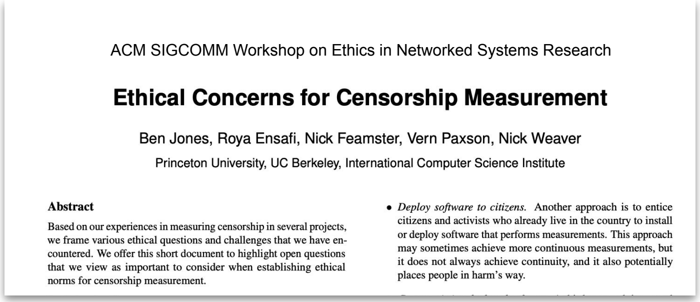
Protecting Users from Adversarial Networks

Roya Ensafi
University of Michigan

Ethics in Censorship Measurement

More generally, censorship research frequently raises ethical considerations.

E.g., under what conditions is it safe enough to use remote vantage points?



ACM SIGCOMM Workshop on Ethics in Networked Systems Research

Ethical Concerns for Censorship Measurement

Ben Jones, Roya Ensafi, Nick Feamster, Vern Paxson, Nick Weaver

Princeton University, UC Berkeley, International Computer Science Institute

Abstract

Based on our experiences in measuring censorship in several projects, we frame various ethical questions and challenges that we have encountered. We offer this short document to highlight open questions that we view as important to consider when establishing ethical norms for censorship measurement.

- *Deploy software to citizens.* Another approach is to entice citizens and activists who already live in the country to install or deploy software that performs measurements. This approach may sometimes achieve more continuous measurements, but it does not always achieve continuity, and it also potentially places people in harm's way.

IRBs are often not positioned to help.

Common Rule (45 CFR 46.102(f)) defines a human subject as "a living individual about whom an investigator conducting research obtains (1) data through intervention or interaction with the individual or (2) identifiable private information."

We turn to authorities such as the **Belmont and Menlo Reports** to guide ethical thinking.

Frequently consult with colleagues to check our reasoning and conclusions.

Questions we regularly consider include:

- **What populations of users are affected?**
- **Is informed consent feasible?**
- **Have we considered all anticipatable risks?**
- **Do humans incur no more than minimal risk?**
- **Can we take steps to further reduce risks?**
- **Do benefits accrue to the population that is subjected to the risk?**