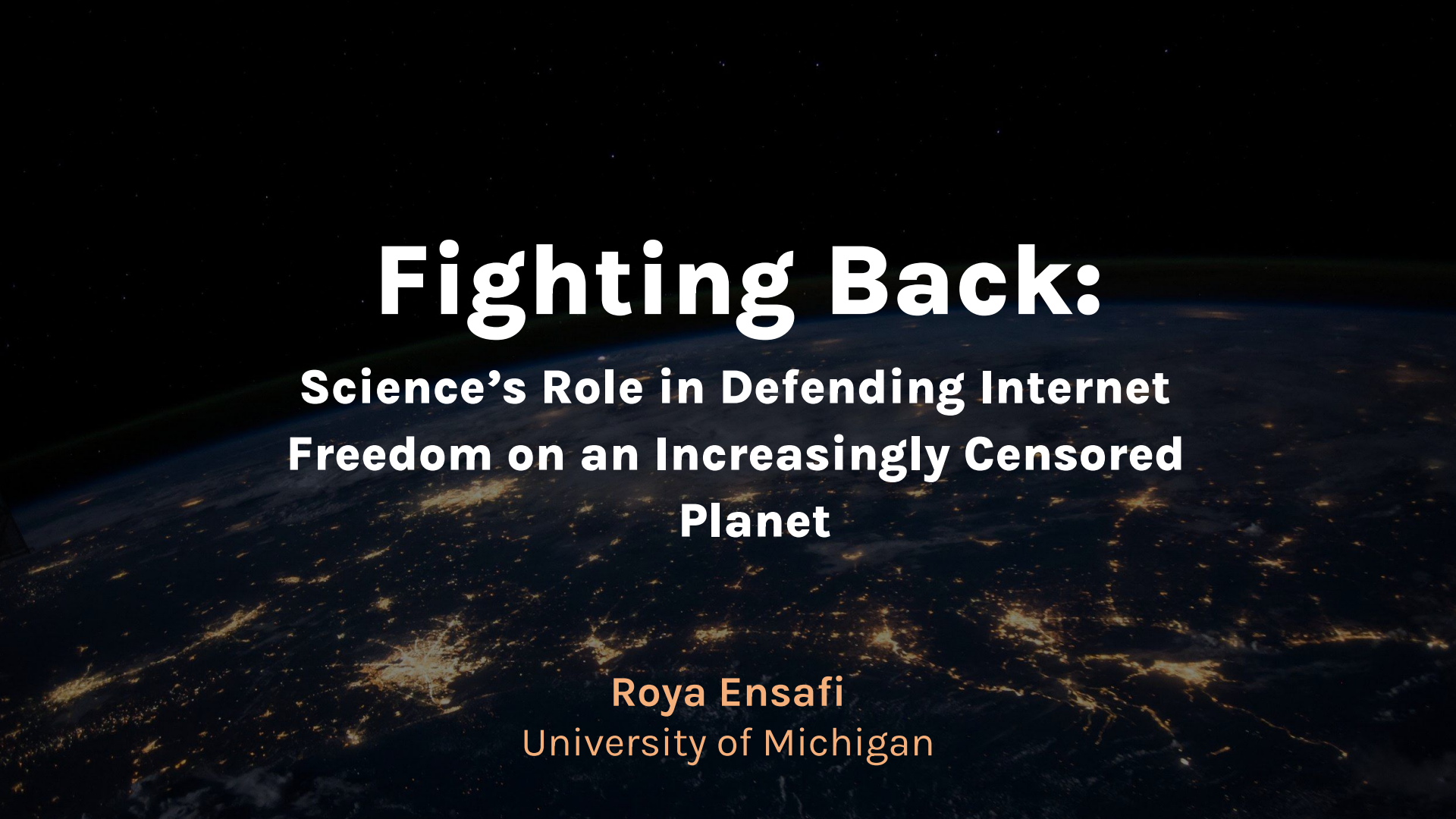
WISER (Women In SEcurity Research) Event

Join us for an inspiring evening of insights, networking, and community with women in security research!

When: Friday, November 15 at 3:30 pm EST
Where: Bob & Betty Beyster Building, Room 3725

Register at: https://tinyurl.com/uofm-wiser

Don't miss this chance to connect and learn!



Fighting Back:

Science's Role in Defending Internet Freedom on an Increasingly Censored Planet

Roya Ensafi
University of Michigan

Frequency and intensity of censorship is globally on the rise

In 2023, Access Now documented **283 shutdowns in 39 countries,** marking the highest number of shutdown incidents in a single year since they began monitoring in 2016.

41% increase from 2022.


How isolating and hopeless this must be for dissidents and activists. When protesters are killed, people cannot even upload pictures to bear witness. Democracy dies in such darkness.
AUX
DES
TORALE

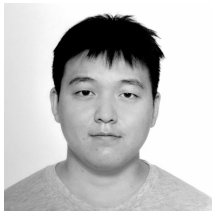
Censored Planet LAB

We build scalable techniques and systems to detect and defend against technologies and practices that impact users' freedom of expression online.

Armin Huremagic
Lead Engineer

Piyush Kumar
Postdoc

Hieu Le
Postdoc



Diwen Xue
PhD Candidate

Anna Ablove
PhD Student

Wayne Wang
PhD Student

Aaron Ortwein
PhD Student

Robert Stanley
Undergrad

Brennen Daudlin
Undergrad

Mayne Mei
Undergrad

Alumni

Ram Sundara Raman (→ *Assistant Prof UCSC*)

Reethika Ramesh (→ *Researcher, Palo Alto Networks*)

Renuka Kumar (→ *Software Engineer IV, Cisco*)

Muhammad Ikram (→ *Lecturer, Macquarie University*)

Gavin Li (→ *Graduate Student, Stanford*)

Apurva Virkud (→ *PhD Student, UIUC*)

Elisa Tsai (→ *PhD Student, Michigan*)

Arham Jain (→ *Software Engineer, Google*)

Yael Eiger (→ *PhD Student, Washington University*)

Anjali Vyas (→ *Graduate Student, Cornell Tech*)

Rose Ceccio (→ *PhD Student, Wisconsin - Madison*)

Victor Ongkowijaya (→ *Graduate Student, Princeton*)

Adrian Stoll (→ *Software Engineer, Google*)

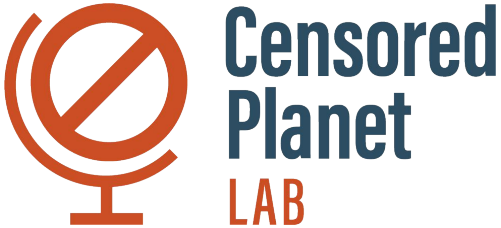
Prerana Shenoy (→ *Atlassian*)

Leonid Evdokimov

Elio Qoshi (→ *Ura Design*)

....

Censored Planet



Join Us at Censored Planet Lab!

We’re looking for an undergraduate assistant.

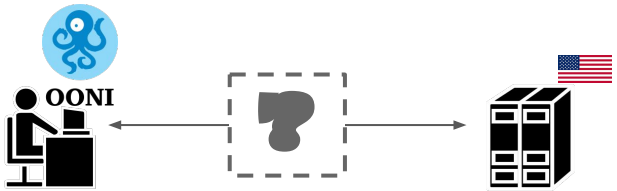
CHAPTER 1

Building a Censorship Observatory

State of Censorship Measurement

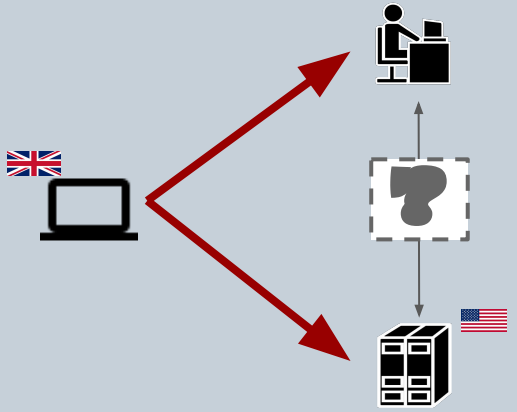
Direct measurement

Deploy hardware or software in censored region
(e.g. RIPE Atlas, OONI probe)



Remote measurement

Detect whether pairs of hosts around the world can talk to each other **by leveraging subtle** behavior of different Internet Protocols **without volunteer participation**



Side Channels Techniques for Remotely Measuring Interference

GOAL: Scalable, ethical system to continuously detect Censorship at any layer

TCP/IP Layer		**Spooky/Augur (2014-17)**	Routers with Global IP - ID Counters
DNS Layer		**IRIS (2017)** **Satellite (2018)** **Certainty (2022)**	Institutional open resolvers
Application Layer		**Quack (2018)** **HyperQuack (2020)**	Services that reflect data (e.g. Echo, HTTP, HTTPS)

Censored Planet

From (Raw) Data points to Understanding Censorship?

Side channels

TCP/IP Layer

→ Spooky
→ Augur

DNS Layer

→ Satellite
→ Iris
→ Certainty

Application Layer

→ Quack
→ HyperQuack

Challenges

- Disruption detection is not necessary censorship detection
- The techniques are each specialized to detect one type of censorship, and only reflect a single snapshot in time
- Labor-intensive to run & maintain
- Ambiguity in location and granularity of filtering → Prone for false positives

Censored Planet

Path forward

Business as usual

Take a risk

Build a censored Planet observatory for continuously monitoring global Internet censorship

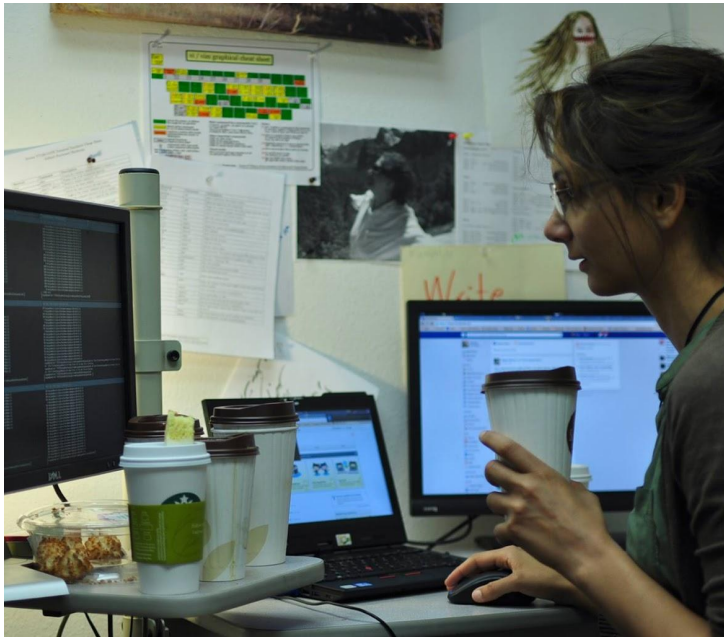
- ➔ **Orchestrate running remote measurement techniques**
- ➔ **Use data science to distill understanding**
- ➔ **Disseminate and facilitate data use**

Censored Planet

Path forward

Business as usual

Take a risk



We Built the Censored Planet Observatory

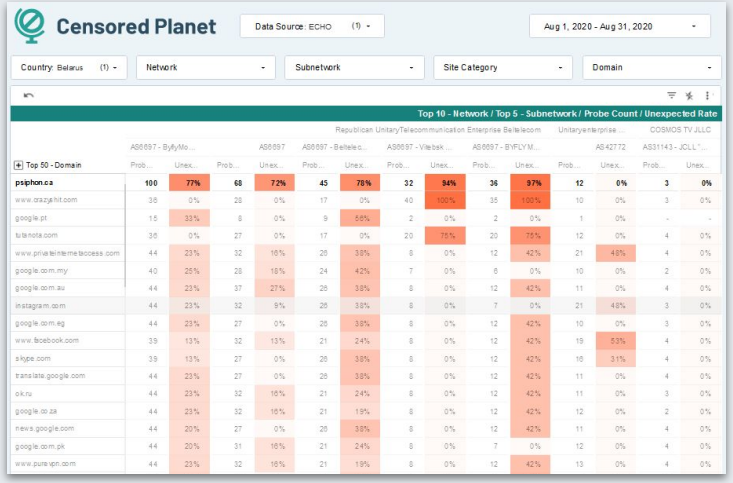
Largest public censorship dataset

From August 2018, we have been running these side channels in parallel and continuously

Censored Planet Dashboard

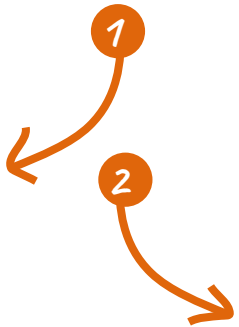
Developed in collaboration with Google's Jigsaw

Facilitate data use and enable easy visualizations
Provide free access to our data users.



Censored Planet

The side-benefits of building an observatory



Arsenal of robust tools

- Capability of rapidly acting upon censorship events as they happen → shed light on the evolving censorship landscape over several years (e.g. Russia)

Advocate for data usage

- Forced us to step out of the “academic bubble”
- Allowed us to build solid relationships with civil societies and gain first hand insights on key technical needs and challenges for activists on the ground

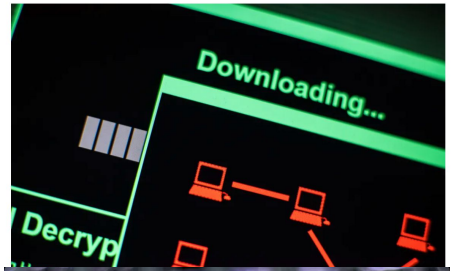
Censored Planet Rapid Response

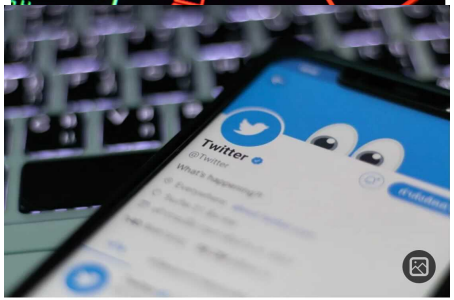
Censored Planet team has exposed **significant new government censorship tactics**,
and our results have been highlighted in more than 100 popular press articles.

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





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

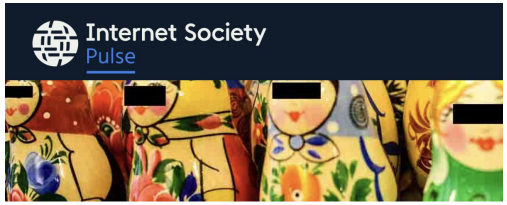
01:36, April 8, 2021
Source: Meduza

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



Home / Blog / How Isolated is the Russian Internet? Consequenc of the war in Ukraine.

How Isolated is the Russian Internet? Consequences of the war in Ukraine.

Amreesh Phokeer
Internet Resilience Insights, Internet Society

Categori
Shutdow

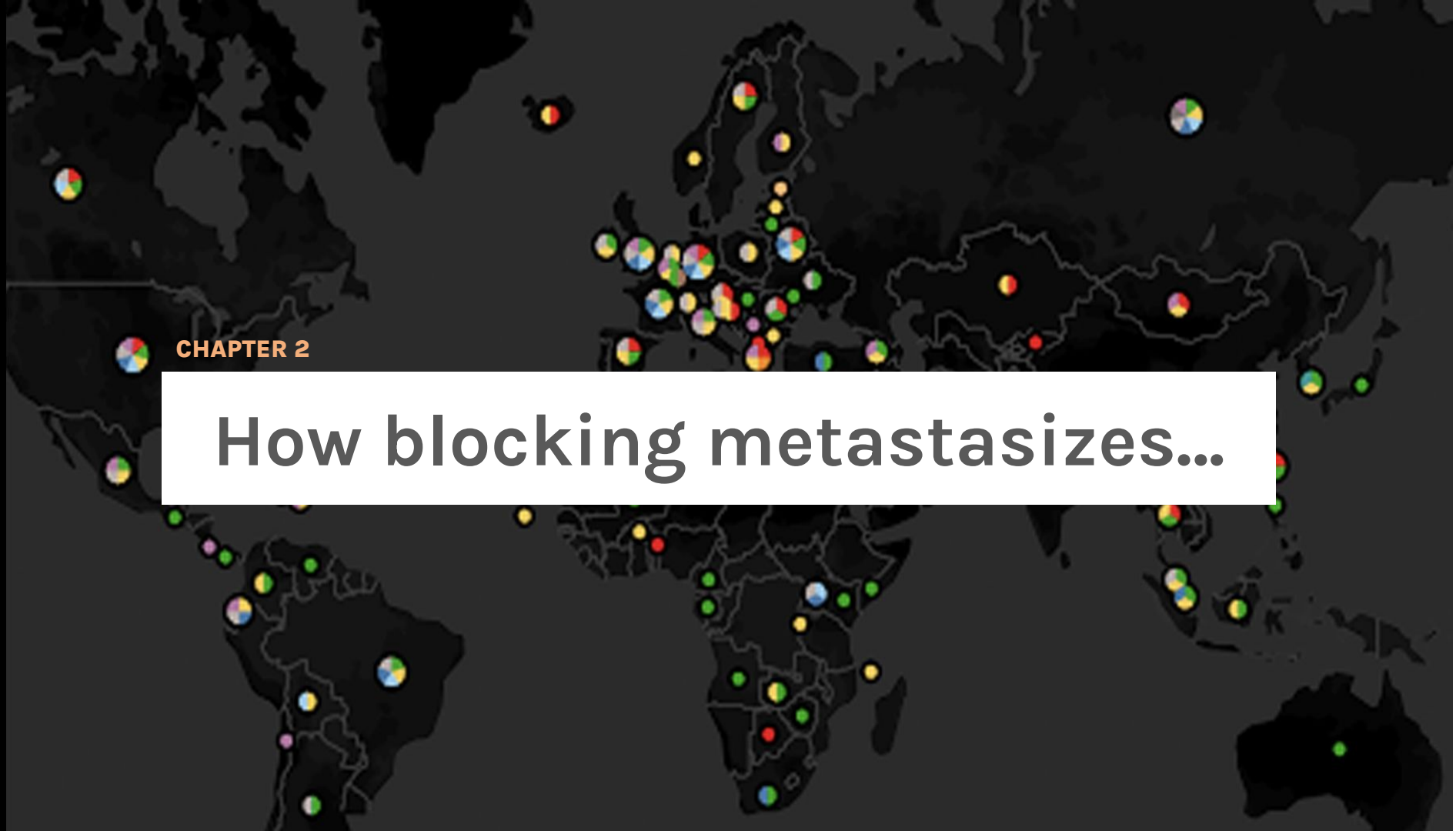
KEY LESSONS

1. **Rapid responses** help keeps thread models honest.
2. **Establishing Trust & communication** in advance insures effective collaboration as events unfold.
3. **Civil society needs our help** to bring research into practice as events unfold

LEARN MORE:

35C3 (2018)

MADWeb (2023)



CHAPTER 2

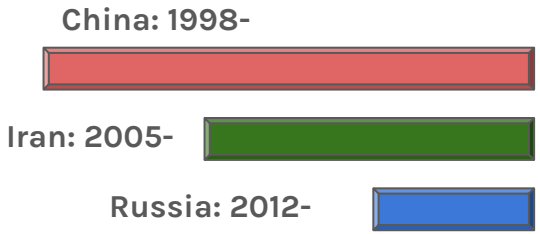
How blocking metastasizes...

Russia's Escalating Control as a Cautionary Tale

Russia case describes how quickly a country's Internet can transition from open to isolated.

A Newcomer to Nation-state censorship

- Russia maintained **relatively open Internet** until ~10 years ago (around Arab Spring)



A Commercialized Domestic Internet

- Similar to many western countries
- Hundreds of **privately-owned ISPs**, different motivations.

Censored Planet investigated Russia's censorship apparatus

2019

Decentralized Control: A Case Study of Russia

Reethika Ramesh*, Ram Sundara Raman*, Matthew Bernhard*, Victor Ongkowijaya*,
Leonid Evdokimov†§, Anne Edmundson†, Steven Sprecher*, Muhammad Ikram‡, Roya Ensafi*
*University of Michigan, {reethika, ramaks, matber, victorwj, swsprec, ensafi}@umich.edu
§Macquarie University, †Independent, ‡leon@darkk.net.ru

Abstract—Until now, censorship research has largely focused on highly centralized networks that rely on technical choke-points, such as the Great Firewall. Although it was previously thought to be [illegible] large-scale censorship in decentralized [illegible] rise. Our in-depth investigation of the mo decentralized information control in Russ large-scale censorship can be achieved in de through inexpensive commodity equipment information control presents a host of prol measurement, including difficulty identifying quiring measurements from diverse perspec censorship mechanisms that require signific in a robust manner.

By working with activists on the groun tained five leaked blocklists signed by Roskon government's federal service for mass co with seven years of historical blocklist data, contains domains, IPs, and subnets that ISPs have been required to block since November 1st, 2012. We used the blocklist from

decades, receiving significant global and academic attention as [illegible], [84]. As more citizens of the world begin [illegible]d social media, and political tensions begin [illegible]es with less centralized networks have also [illegible] to exert control over the Internet. Recent [illegible]y unsophisticated attempts to wrestle with [illegible]ks, such as Internet shutdowns which, due [illegible]e of execution, have become the *de facto* [illegible] of choice in some countries [14], [36], [illegible]reliminary studies investigating information [illegible]ized networks have examined India [89], [illegible]gal [60], [61], and other countries, there has [illegible]th multifaceted exploration of the specific [illegible]ms used by governments for decentralized [illegible] as they evolve over time.

[illegible]cking to implement a homogeneous national [illegible] in pursue one of two intuitive options. The first is a centralized control that relies on government-run

2021

Throttling Twitter: An Emerging Censorship Technique in Russia

Diwen Xue
University of Michigan

Reethika Ramesh
University of Michigan

ValdikSS
Independent

Leonid Evdokimov
Independent

Andrey Viktorov
Independent

Arham Jain
University of Michigan

Eric Wustrow
University of Colorado Boulder

Simone Basso
OONI

Roya Ensafi
University of Michigan

ABSTRACT

In March 2021, the Russian government starte[illegible] on a national level, marking the first ever use o[illegible] throttling for censorship purposes. The slow[illegible] to pressure Twitter to comply with content re[illegible] the Russian government.

In this paper, we take a first look at this e[illegible] technique. We work with local activists in [illegible] measure the throttling and reverse engineer t[illegible] country vantage points. We find that the th[illegible] by Twitter domains in the TLS SNI extension[illegible] limits both upstream and downstream traffic[illegible] 130 kbps and 150 kbps by dropping packets [illegible] We also find that the throttling devices appea[illegible] to end-users, and that the throttling behaviors[illegible] different ISPs suggesting that they are centrally coordinated. No-

1 INTRODUCTION

[illegible]censorship relies on targeted blocking of con-[illegible]Censors implement blocking using network [illegible]s as IP [8, 12, 13], DNS [6, 16, 30, 37], key-[illegible]or protocol fingerprints [3, 7, 11, 56]. In ex-[illegible]s have also used Internet shutdowns to com-[illegible]ction to the Internet to prevent unwanted ac-

[illegible]s a common tool for censors, less has been [illegible]otling connections as a means for censorship. [illegible]ng, throttling aims to degrade bandwidth to a [illegible]e its use while still allowing some access. This [illegible]chnique for censors as it is more difficult for [illegible]nitors to detect or attribute the slowdown to [illegible]nnections may be a natural result of network congestion and not intentional throttling.

2022

TSPU: Russia's Decentralized Censorship System

Diwen Xue
University of Michigan

Benjamin Mixon-Baca
ASU/Breakpointing Bad

ValdikSS
Independent

Anna Ablove
University of Michigan

Beau Kujath
ASU/Breakpointing Bad

Jedidiah R. Crandall
ASU/Breakpointing Bad

Roya Ensafi
University of Michigan

ABSTRACT

Russia's Sovereign RuNet was designed to build a Russian national firewall. Previous anecdotes and isolated events in the past two years reflected centrally coordinated censorsh[illegible] multiple ISPs, suggesting the deployment of "sp[illegible] networks, colloquially known as "TSPU". Dee[illegible] prising a critical part of the technical stack of [illegible] known about its design, its capabilities, or the [illegible] ment.

In this paper, we develop novel techniques [illegible] and remote measurements to discover the *how*, [illegible] TSPU's interference with users' Internet traffic[illegible] ent types of blocking mechanisms triggered by [illegible] and we find the TSPU to be in-path and stat[illegible] unique state-management characteristics. Usin[illegible] haviors as fingerprints, we identify over one [illegible] Russia from 650 ASes that are behind TSPU d[illegible] 70% of them are at most two hops away from the [illegible] that TSPU devices progressed from ideation to [illegible] years, we fear that the emerging TSPU architecture may become a blueprint for other countries with similar network topology.

1 INTRODUCTION

Since 2012, the Russian government has been developing both legal and technical frameworks to construct its censorship apparatus [17]. [illegible]overeign RuNet" law was signed, requiring tele-[illegible]install a home-grown DPI system, colloquially [illegible]on their networks free of charge [20]. This pro-[illegible]ent with an extraordinary ability to centrally [illegible]ntrol the traffic passing through thousands of distributed ISPs. This centralized control was [illegible]ate Russia's internal Internet ecosystem from [illegible]orld to "protect" Russia in the face of foreign

[illegible]s independently point to the deployment of the [illegible]021, Russia pressured Twitter to comply with [illegible]l requests with targeted throttling and threats [illegible]g [29]. Xue *et al.* showed that throttling behav-[illegible]a high degree of uniformity and coordination [illegible]SPs [98]. Subsequently, Roskomnadzor, Russia's [illegible]ency, publicly confirmed that the TSPU, which comprises the technical stack of RuNet, was used for throttling [28]. In March 2022, censorship observatory OONI reported that many

2023

Network Responses to Russia's Invasion of Ukraine in 2022: A Cautionary Tale for Internet Freedom

Reethika Ramesh†* Ram Sundara Raman†* Apurva Virkud† Alexandra Dirksen△
Armin Huremagic† David Fifield Dirk Rodenburg‡ Rod Hynes‡ Doug Madory◇ Roya Ensafi†

†*University of Michigan* △*TU Braunschweig* ‡*Psiphon* ◇*Kentik*

Abstract

Russia's invasion of Ukraine in February 2[illegible] by sanctions and restrictions: by Russia a[illegible] by Russia against the world, and by forei[illegible] Russia. Reports suggested a torrent of incr[illegible] geoblocking, and network events affecting[illegible]

This paper is an investigation into the [illegible] that occurred in the weeks following this es[illegible] ties. It is the result of a rapid mobilization [illegible] activists, examining the problem from multiple perspectives. We develop GeoInspector, and conduct measurements to iden-[illegible]

[illegible] of government reactions, sanctions, busi-[illegible] and general confusion concerning the state [illegible]ntrols. In Russia, the government's desire [illegible]ing about the invasion led it to increase [illegible]rnative sources of information and limit [illegible]vention tools [51]. Isolation increased in [illegible]th network resources in Russia being made outside the country [35], and entities out-[illegible] Russian users off from network access through sanctions and geoblocking, a phe-nomenon in which server operators intentionally deny access to users from particular regions [28, 54, 82].

Censored Planet

Timeline of Russia's Escalating Control

July 2012
139-FZ "Blocklist Law" signed

November 2019
"RuNet" law came into force requiring installation of "special equipment"

2019 - 2020
"ISPs received letters from RKN.

March, 2021
The Twitter Throttling incident.

2021-present
TSPU successfully in use

Feb, 2022
Russia Invaded Ukraine

139-FZ "Blocklist Law" was signed in 2012

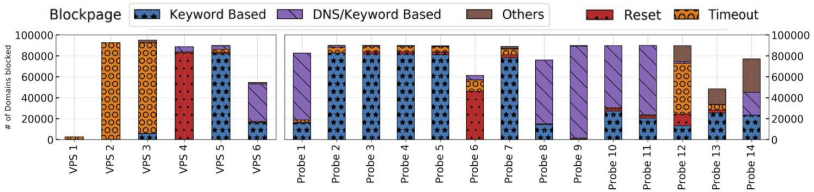
Roskomnadzor maintains "the Registry of Blocking Sites".

- IP, subnets, domain names, without court's approval
- ISPs are required to block websites from the list.

Censored Planet studied Russia (2017-2019)

In-country measurements from data centers & residential networks.

- Blocking Registry grows to 132K domains and 324K IPs
- Different blocking mechanisms (DNS/Keyword/Blockpage)
- Varying extent of enforcement



Timeline of Russia's Escalating Control

July 2012
139-FZ "Blocklist Law" signed

November 2019
"RuNet" law came into force requiring installation of "special equipment"

2019 - 2020
"ISPs received letters from RKN.

March, 2021
The Twitter Throttling incident.

2021-present
TSPU successfully in use

Feb, 2022
Russia Invaded Ukraine

The President signed the law on sustainable Runet

Newsroom - 02.05.2019

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

Appoints Roskomnadzor to guard the "stability, security, and integrity" of Russia's Internet.

Provides legal grounds for requiring ISPs to install "special equipment" to counter "threats" to Russia's Internet

Censored Planet

Timeline of Russia's Escalating Control

July 2012
139-FZ "Blocklist Law" signed

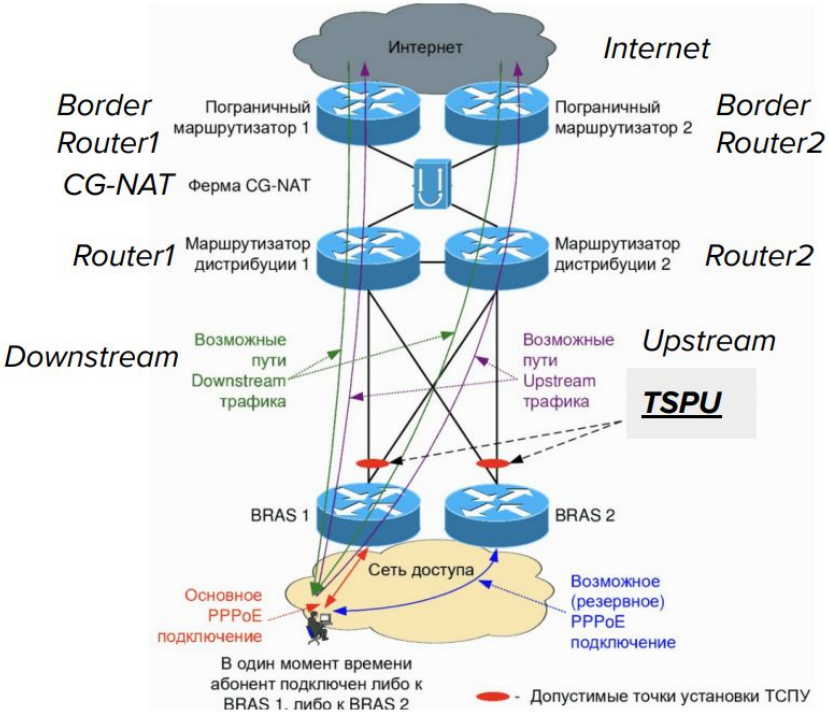
November 2019
"RuNet" law came into force requiring installation of "special equipment"

2019 - 2020
"ISPs received letters from RKN.

March, 2021
The Twitter Throttling incident.

2021-present
TSPU successfully in use

Feb, 2022
Russia Invaded Ukraine



Russian ISPs started to receive letters from Roskomnadzor, requesting information on their networks.

This figure is an example of leaked document by an ISP on where in the network these devices need to be installed.

Timeline of Russia's Escalating Control

July 2012
139-FZ "Blocklist Law" signed

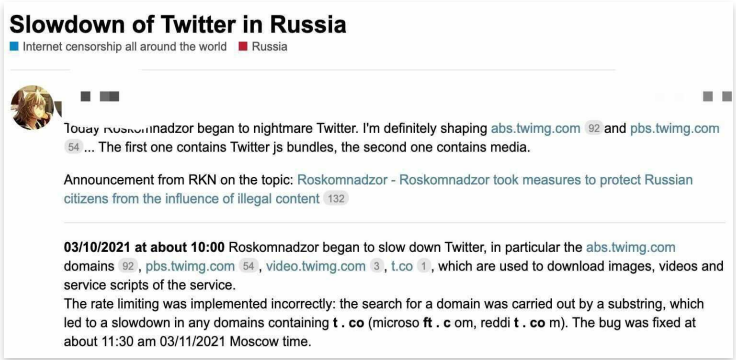
November 2019
"RuNet" law came into force requiring installation of "special equipment"

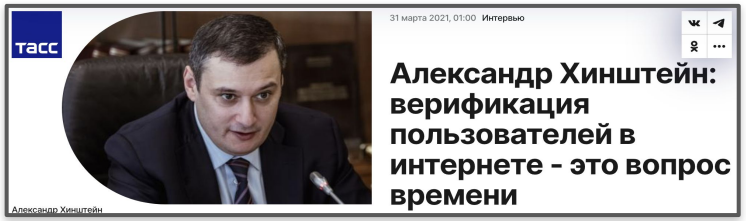
2019 - 2020
"ISPs received letters from RKN.

March, 2021
The Twitter Throttling incident.

2021-present
TSPU successfully in use

Feb, 2022
Russia Invaded Ukraine

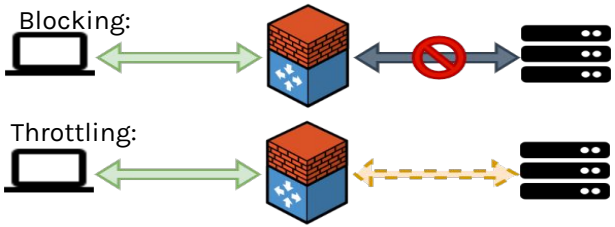




Censored Planet investigate throttling (IMC 2021)

First-ever instance of targeted throttling as censorship technique:

- Easy for censors but hard for users to attribute or circumvent.
- Detecting it is tricky → censorship detection platforms aren't yet well equipped to spot it.



Censored Planet

Timeline of Russia's Escalating Control

July 2012
139-FZ "Blocklist Law" signed

November 2019
"RuNet" law came into force requiring installation of "special equipment"

2019 - 2020
"ISPs received letters from RKN.

March, 2021
The Twitter Throttling incident.

2021-present
TSPU successfully in use

Feb, 2022
Russia Invaded Ukraine

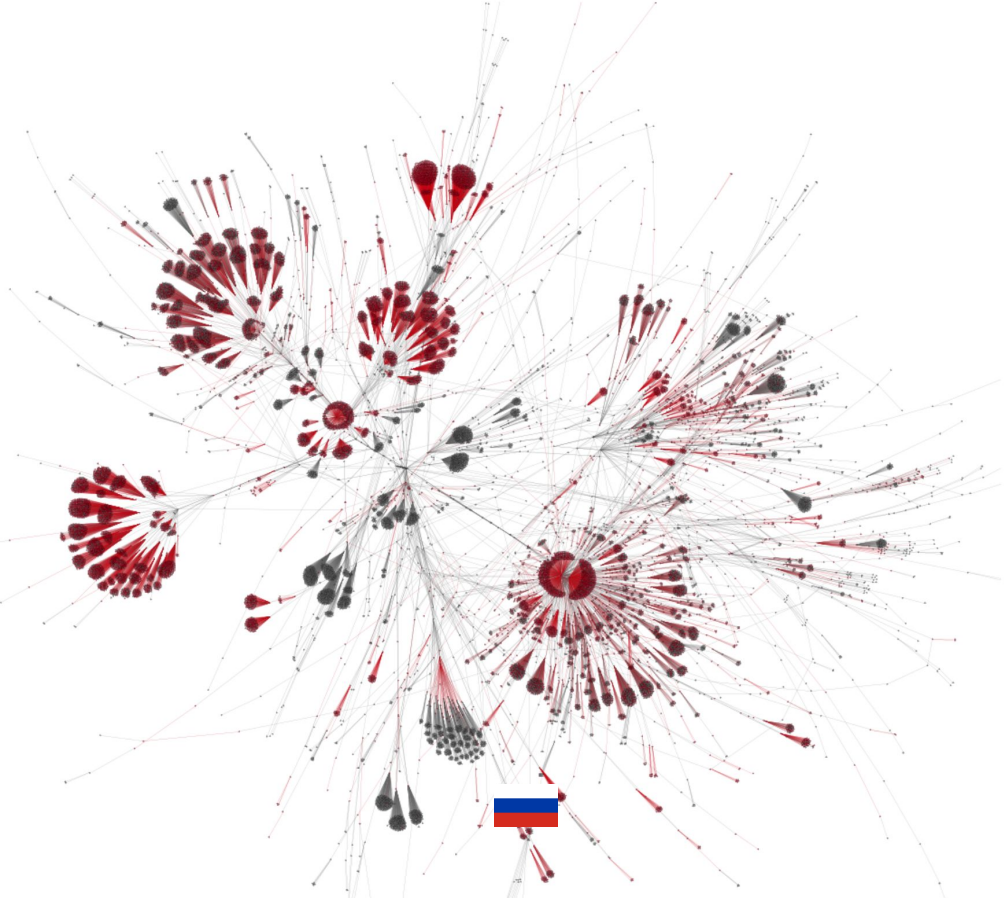
технические средства противодействия угрозам (Technical Measures to Combat Threats)

DPI devices that are...
Centrally controlled by RKN, Decentrally deployed in ISP networks

Censored Planet & Prof. Crandall team investigate TSPU

- **Local measurement:**
  - Acquire Vange point in many ISPs & reverse engineer TSPU
  - **Challenges:** Limited in scale.

- **Remote measurement:**
  - **Challenge:** TSPU only applies blocking to RU
  - Not symmetric.
  - **Solution:** IP Fragmentation Side Channels.



- Four million traceroutes identified **6,871 unique TSPU devices**.
- >70% cases, TSPU is within two hops away
  - **In-path + close to edges**
- Architecture for targeted surveillance/ interception
- Russia has now established a **complex, decentralized national firewall**

KEY LESSONS

1. Russia has now established **a complex, decentralized national firewall** on top of commercial ISPs using commodity DPIs.

We need to look out how Russia and China are helping other countries building their firewall...

2. From 2023, Russia is testing **disconnecting itself** from the global Internet

We need to revisit what technologies we need to build to sustain open internet when shutdowns happen → we are behind..

CHAPTER 3

International Sanctions and Geoblocking are Hurting Internet Freedom.

Censored Planet

Timeline of Russia's Escalating Control

July 2012
139-FZ "Blocklist Law" signed

November 2019
"RuNet" law came into force requiring installation of "special equipment"

2019 - 2020
"ISPs received letters from RKN.

March, 2021
The Twitter Throttling incident.

2021-present
TSPU successfully in use

Feb, 2022
Russia Invaded Ukraine

Russia invasion into Ukraine

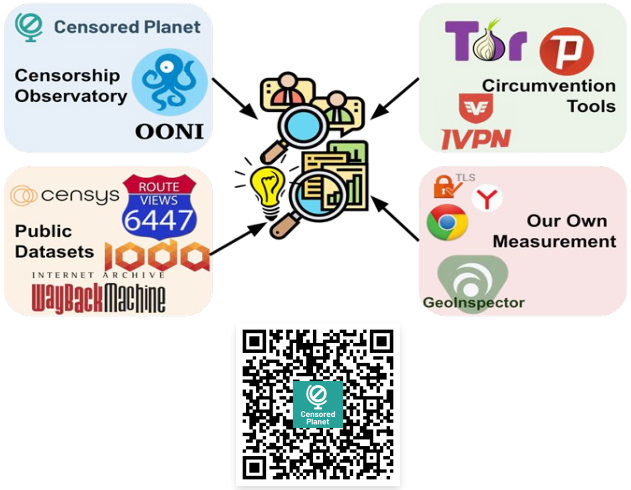
Increased censorship:

Blocking of Circumvention Tools

Business Withdrawals:

Sanctions:

Censored Planet and collaborators investigated Network Responses to Russia's Invasion of Ukraine



Censored Planet

Timeline of Russia's Escalating Control

July 2012
139-FZ "Blocklist Law" signed

November 2019
"RuNet" law came into force requiring installation of "special equipment"

2019 - 2020
"ISPs received letters from RKN.

March, 2021
The Twitter Throttling incident.

2021-present
TSPU successfully in use

Feb, 2022
Russia Invaded Ukraine

Due to sanctions, two CAs stopped issuing certificates to RU TLDs (.ru, .by, .su, .рф)

Reaction: Russia created a free domestic CA
(CN=Russian Trusted Root)

Ambiguous sanctions have unfortunate consequences.

The end of end-to-end as we know it

Censored Planet

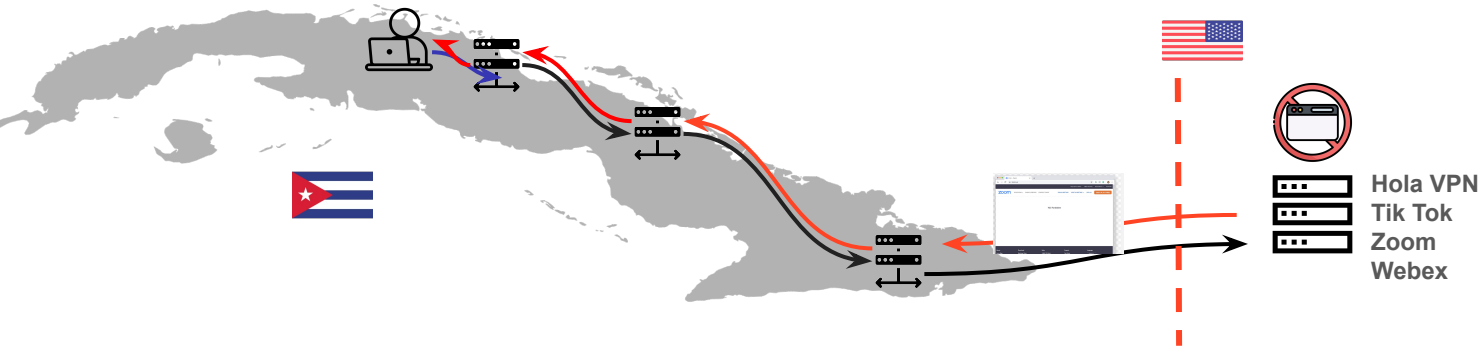
Sanctions on the Net: Cuba as a Case Study

Goal: Understanding the effect of policy and embargo sanctions

- Combined **small-scale user study** with **systematic measurements** to characterize day to day impact of geoblocking

"Blocked sites only affect the people who need the knowledge, not the government."

"...it makes it impossible for us to create projects that can be used internationally."



FORTHCOMING PAPER:

Digital Discrimination of Users in Sanctioned States: The Case of the Cuba Embargo
USENIX Security, August 2024

Censored Planet

Can we Independently Audit Overblocking? Obstacles:

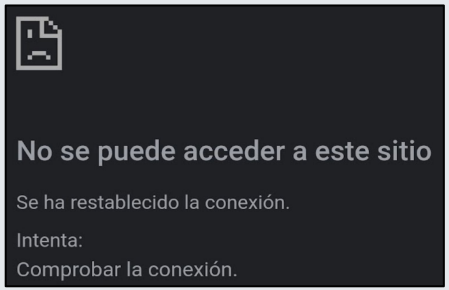
Overblocking is common

71.6% (388) of geoblocking domains are in categories promoted by the U.S. Gov as exempt from sanctions (ex. Information Tech, Education).

44% of these block in spite of free-tier offerings (ex. gitlab.com, adobe.net).

Poor user transparency

88% of geoblocking domains **do not** serve informative notice of why they are blocked



Lack of standardization

Found over 30 instances of blockpages served with **200 OK**

→Extensive attribution processes include manual verification

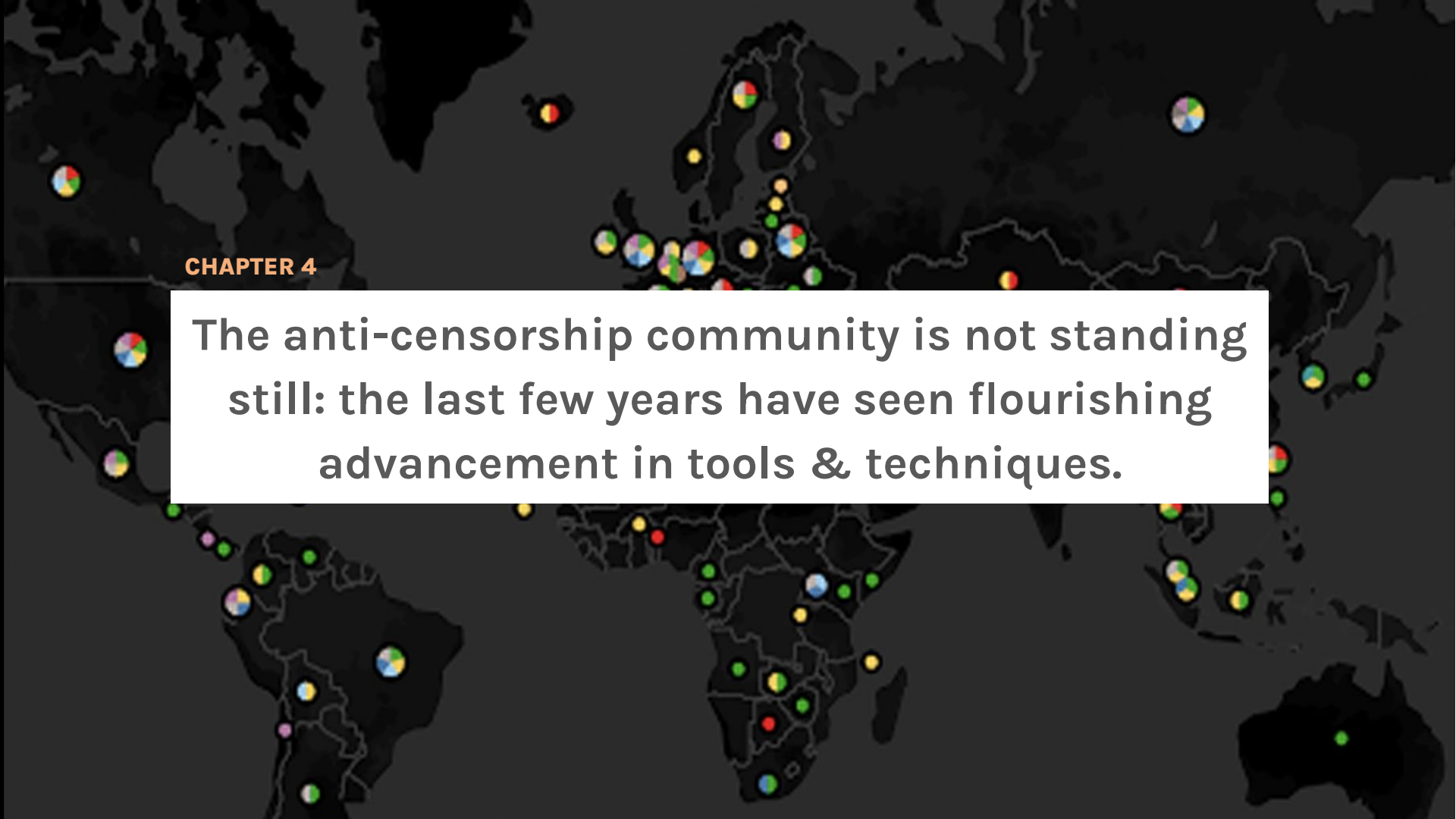
```
"user_geo_blocked":
  "blocked": true,
  "country": "CU",
```

KEY LESSONS

1. **Sanctions** that target internet infrastructures are counter productive

2. From policy to implementation is a huge gap and misunderstanding often lead to **overblocking** that is hard to correct

3. Lets not give an authoritarian government an **excuse** to further splintering the internet



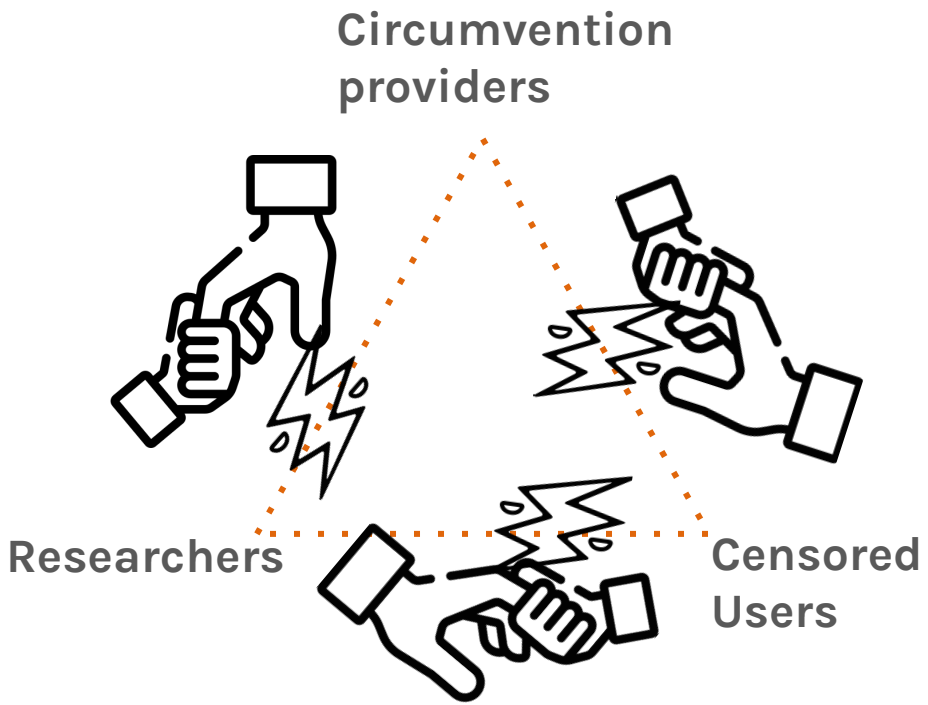
CHAPTER 4

The anti-censorship community is not standing still: the last few years have seen flourishing advancement in tools & techniques.

Bridging Barriers: A Survey of Challenges and Priorities

One of the most **opaque** ecosystems

- Risks to those directly involved in operating & using **circumvention tools**
- **Inherently adversarial**
- **Limited communication** between stakeholders



Study of Circumvention Providers and Censored Users

Goal

Illuminate dynamics and challenges of the circumvention ecosystem.

- Outline key challenges currently facing
- Highlight priorities for concerted efforts.

Ethics

Directly engaging with circumvention providers & users involved significant ethical complexities.

Interviews

19 individuals from 12 organizations operating circumvention tools

(Psiphon, GreatFire, Outline, Proton, etc.)

24 user-facing interviews.

Research Questions:

How do **users** find about circumvention tools?

- ↪ Specifically in censored environment with active adversary

How do **providers** sustain their operations?

- ↪ Funding, disruption from censor, etc

How do **users and providers** manage risks?

- ↪ What significance does **trust** hold, and how do providers establish trust with users?

What can **we** do?

- ↪ Funding agency, academia, big tech

FORTHCOMING PAPER:

Bridging Barriers: A Survey of Challenges and Priorities in the Censorship Circumvention Landscape D. Xue*, A. Ablove*, R. Ramesh, G. Kwak-Danciu, R. Ensafi, USENIX'24

Study of Circumvention Providers and Censored Users

Trust:

- **A pervasive distrust within the ecosystem**
  - **Misbehaving players**
  - **Yet users knowingly expose themselves, driven by need for access**

"They [other providers] keep logs and IDs so that if the government comes knocking, they have something to bribe - like saying
*'**Don't put me in jail, put these people in jail**' "*
— Anonymous provider

*"I use whatever tool that gets me connected. I don't know how it works, but since **I had to use it, I had to trust it**."*

— Anonymous user

Study of Circumvention Providers and Censored Users

Bootstrapping:

- **The initial bootstrapping as a critical yet often overlooked issue, complicating adoption and security**

"They keep becoming unusable, but there's nothing to fix."
"I use a free shady VPN from the Chinese appstore to find better tools ... I can search from Google, but I need to have access to Google first."

— Anonymous users

"It took us a month to develop a patch, but the ***users are not willing to come back because they think it won't work****"*

— Anonymous provider

Study of Circumvention Providers and Censored Users

Funding:

- **Limited funding lead to unintended competition among providers, impeding knowledge sharing**

*"There's a competition mentality, particularly in **competing for the same funding dollars**."*

*"It's difficult to monetize the service in a way that doesn't **expose developers and providers** to addition risk."*

— Anonymous provider

Fighting Back:

1. Engage with censorship measurement research to understand the capabilities of authoritarian regimes and how they're metastasizing (check out censorbib.nymity.ch/)

2. Design tools that rise to the challenge of these heightened threat environments and adversarial capabilities

3. Join with our community to bring your ideas into the hands of vulnerable people living under censorship worldwide

Roya Ensafi
University of Michigan