Network Responses to Russia's Invasion of Ukraine in 2022

A Cautionary Tale for Internet Freedom

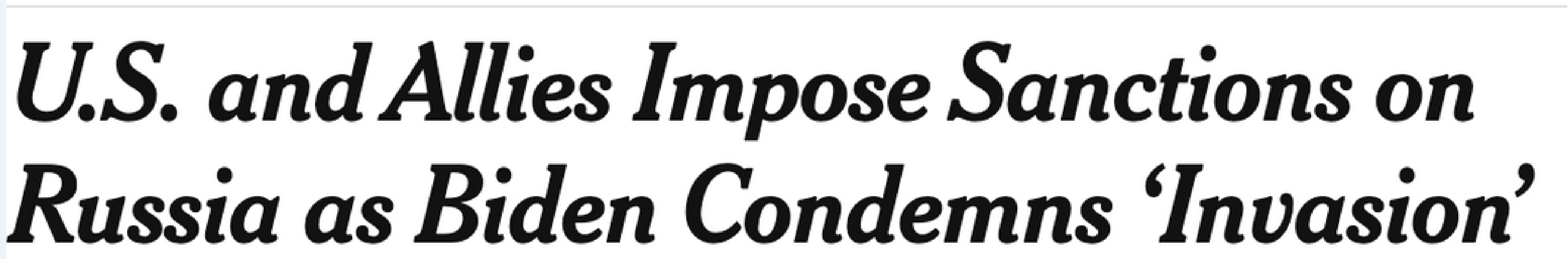
Reethika Ramesh, Ram Sundara Raman, Apurva Virkud, Alexandra Dirksen, Armin Huremagic, David Fifield, Dirk Rodenburg, Rod Hynes, Doug Madory, Roya Ensafi

USENIX Security '23

February 24, 2022:

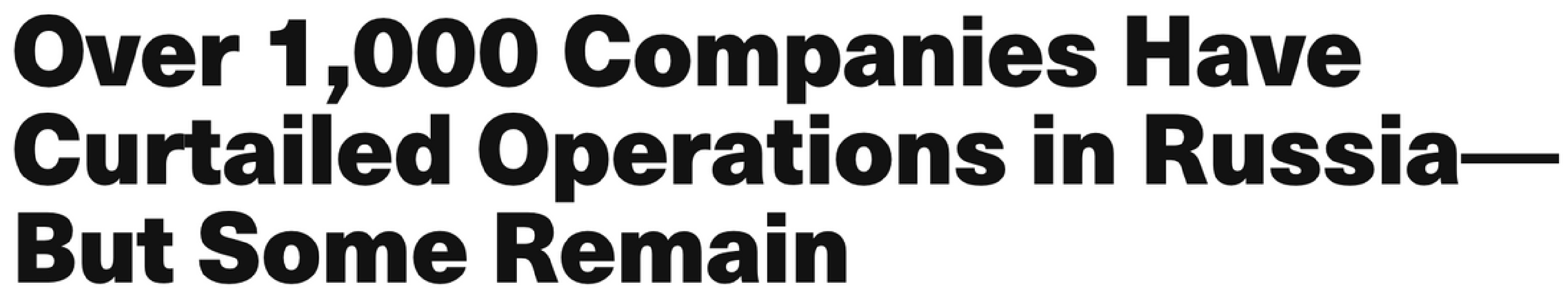
Russia escalates invasion into Ukraine

Sanctions



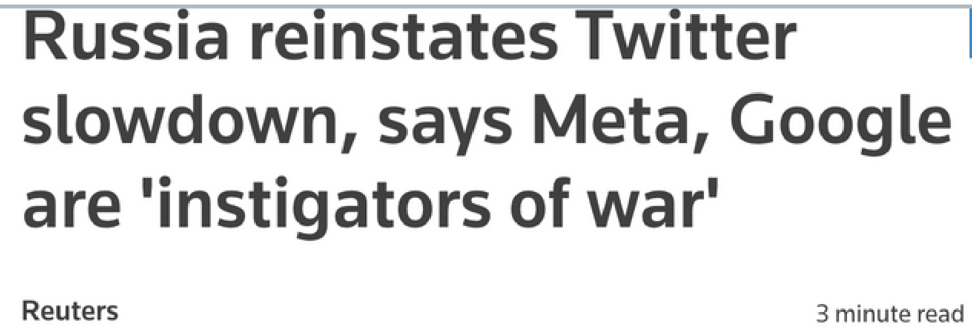
U.S. and Allies Impose Sanctions on Russia as Biden Condemns ‘Invasion’

Business Withdrawals



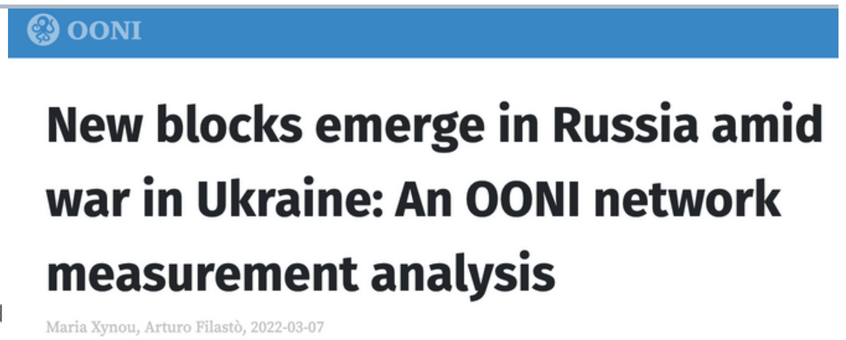
Over 1,000 Companies Have Curtailed Operations in Russia—But Some Remain

Internet Restrictions



Russia reinstates Twitter slowdown, says Meta, Google are 'instigators of war'

Reuters 3 minute read

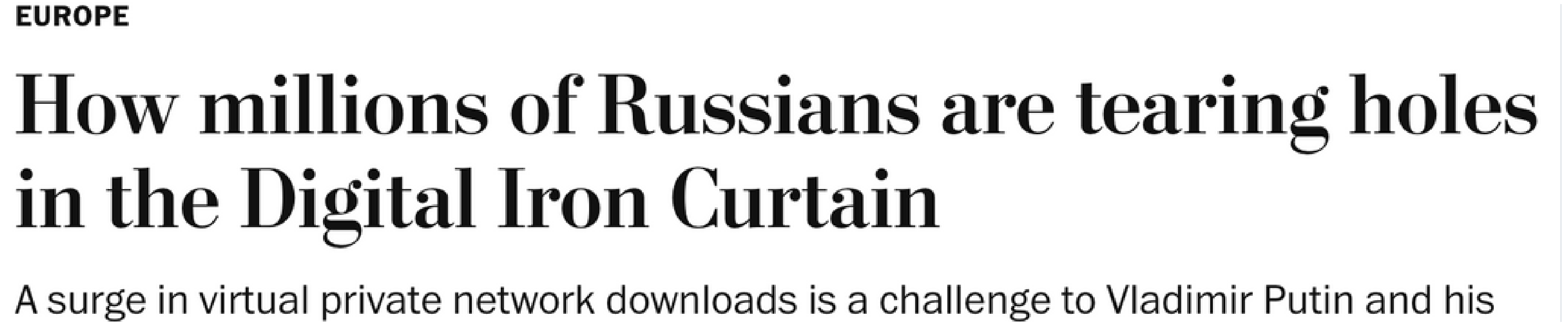


OONI

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

Maria Xynou, Arturo Filastò, 2022-03-07

Circumvention

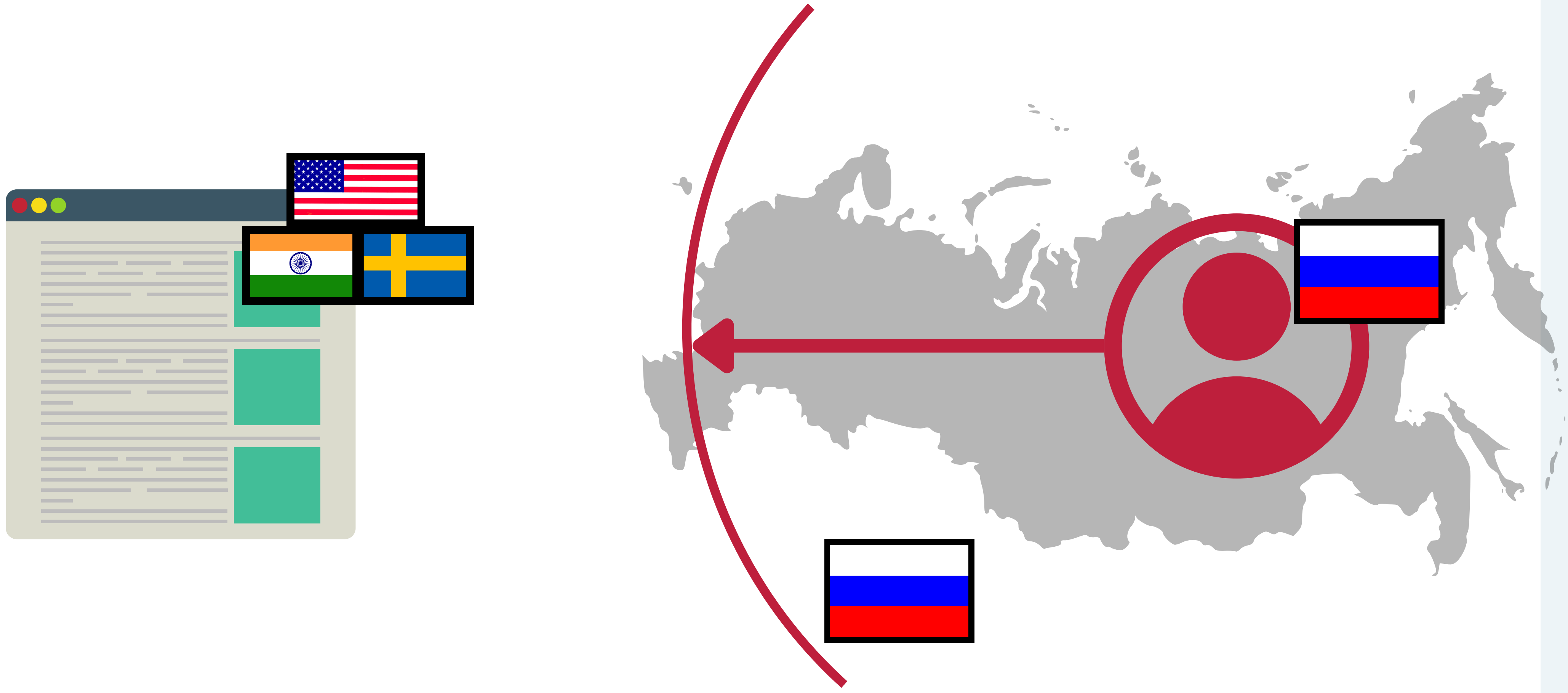


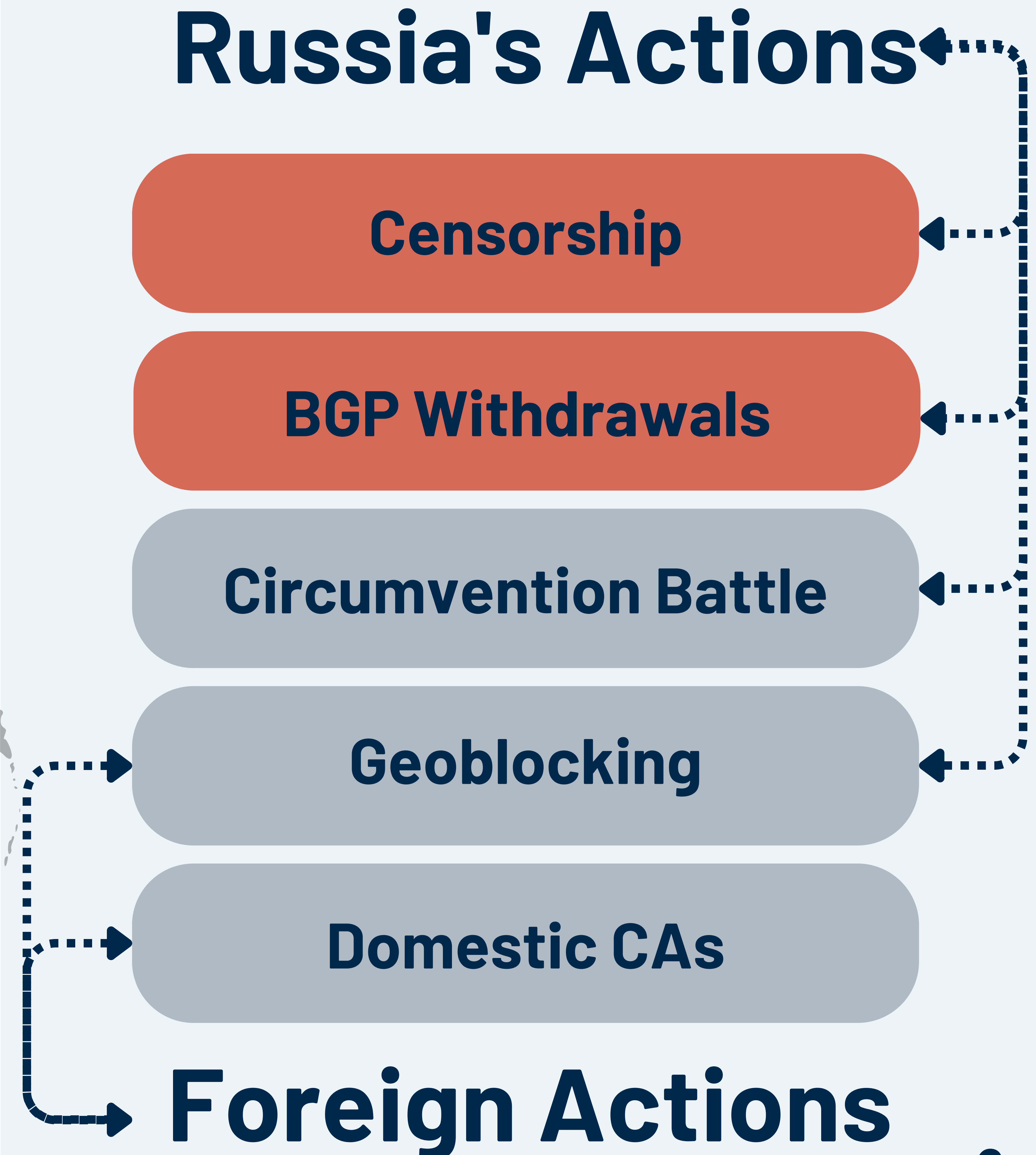
EUROPE

How millions of Russians are tearing holes in the Digital Iron Curtain

A surge in virtual private network downloads is a challenge to Vladimir Putin and his

Dangers to Internet Freedom



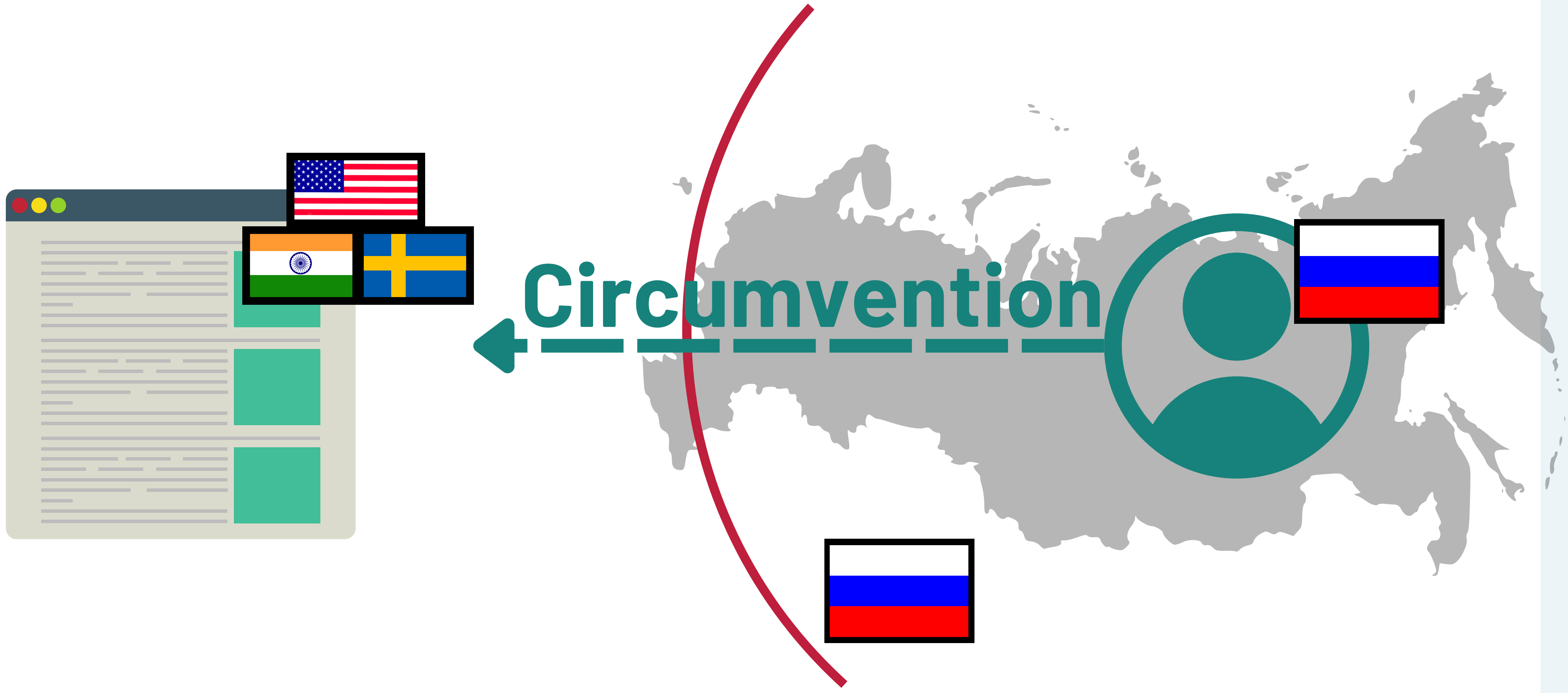


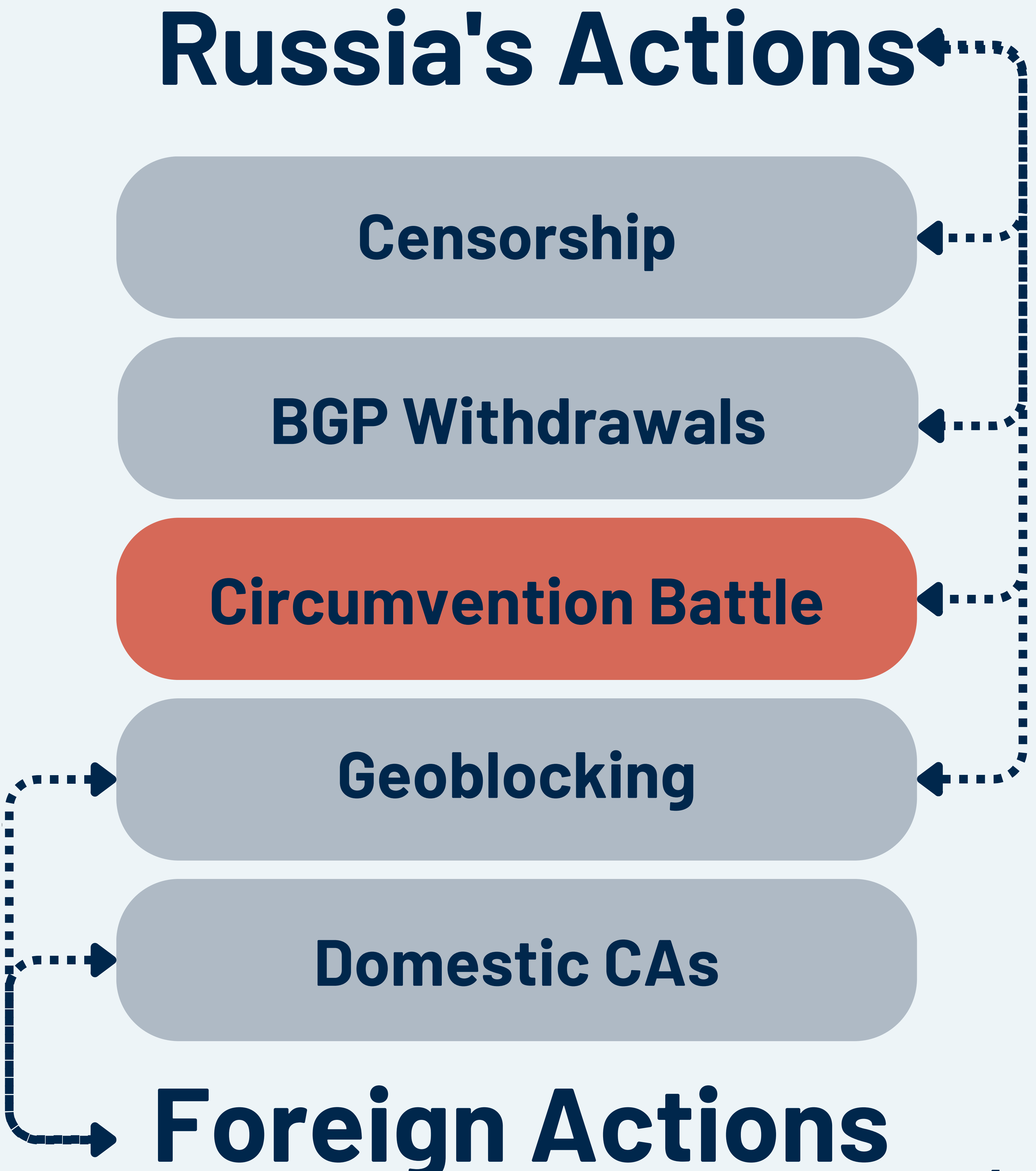
Russia's Actions

- Censorship
- BGP Withdrawals
- Circumvention Battle
- Geoblocking
- Domestic CAs

Foreign Actions

Dangers to Internet Freedom





Russia's Actions

Censorship

BGP Withdrawals

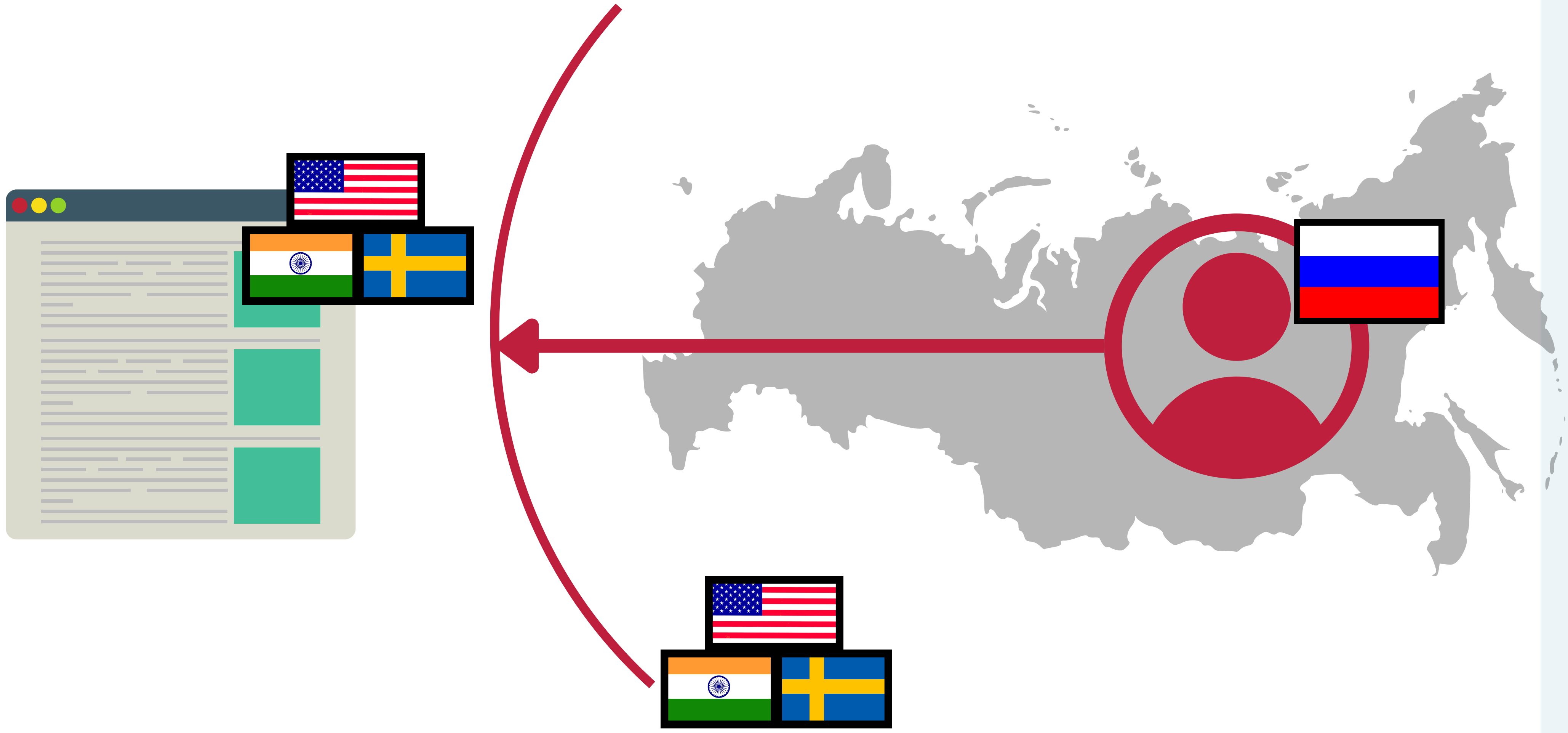
Circumvention Battle

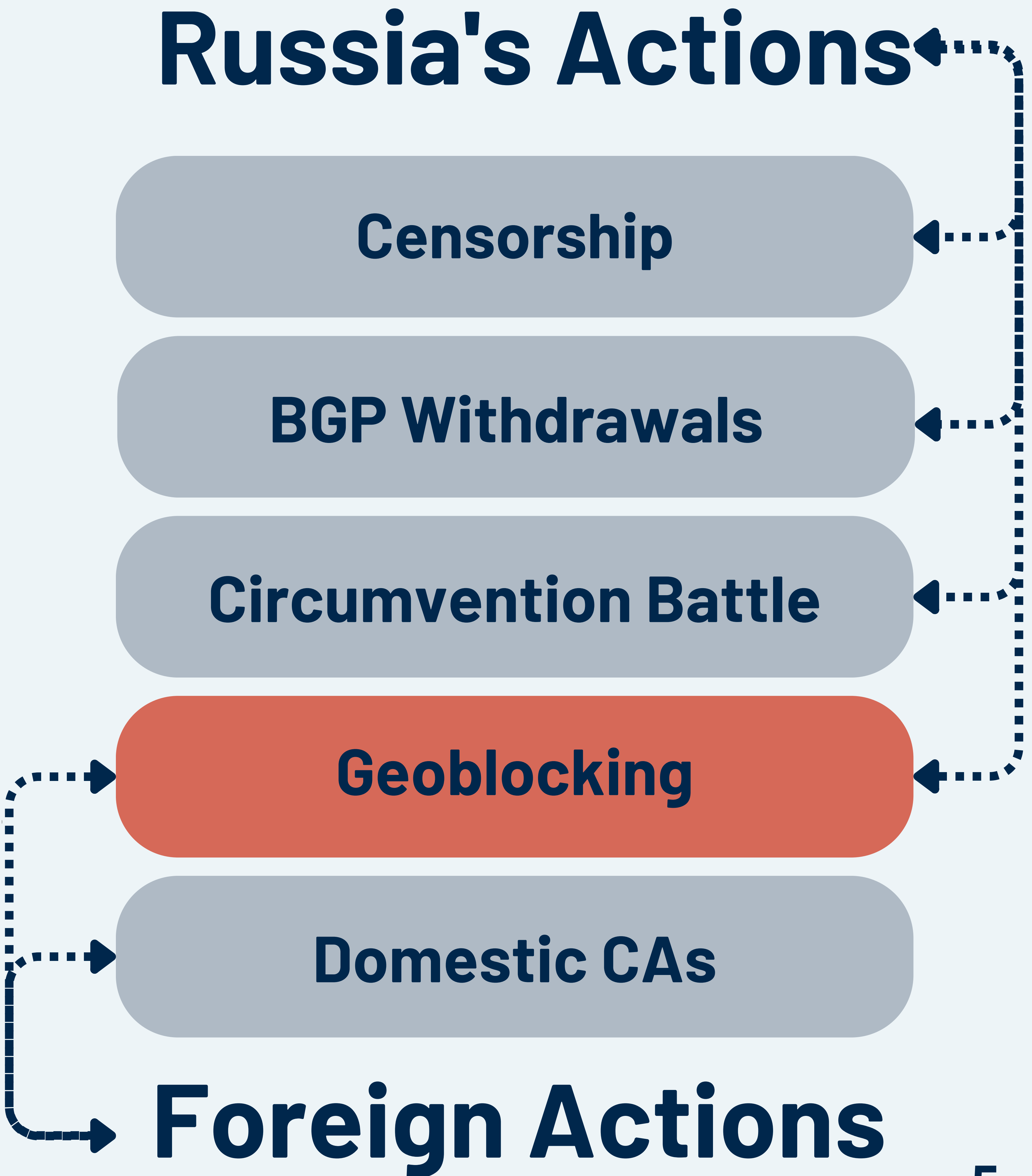
Geoblocking

Domestic CAs

Foreign Actions

Dangers to Internet Freedom





Russia's Actions

Censorship

BGP Withdrawals

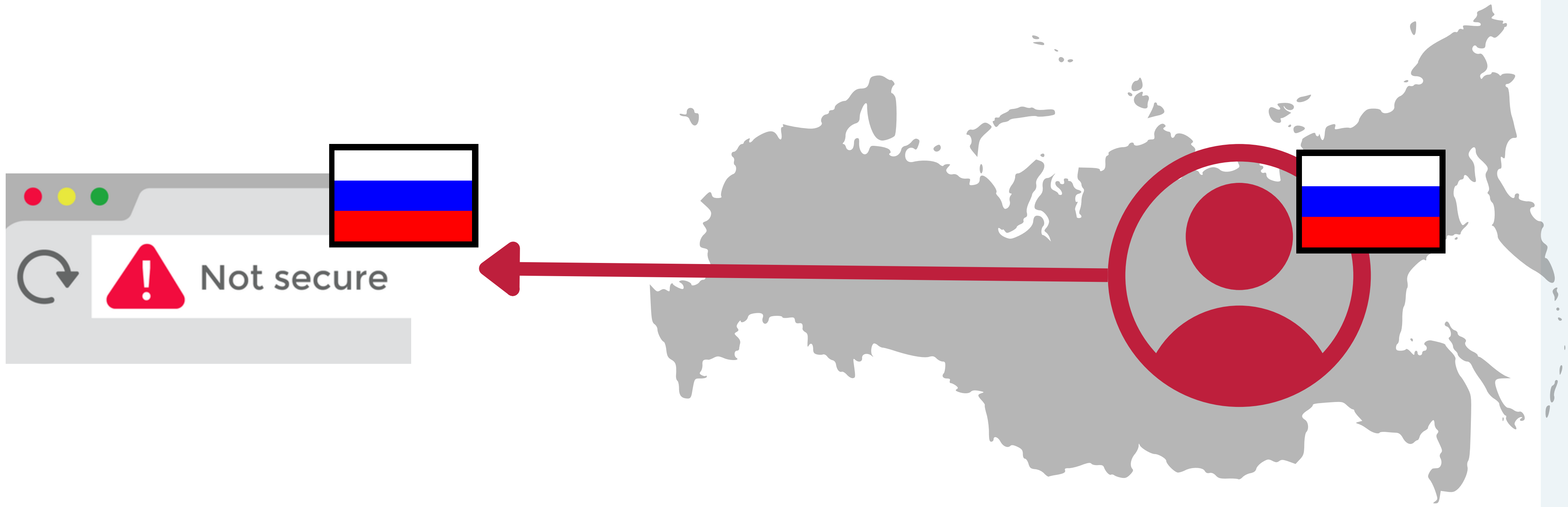
Circumvention Battle

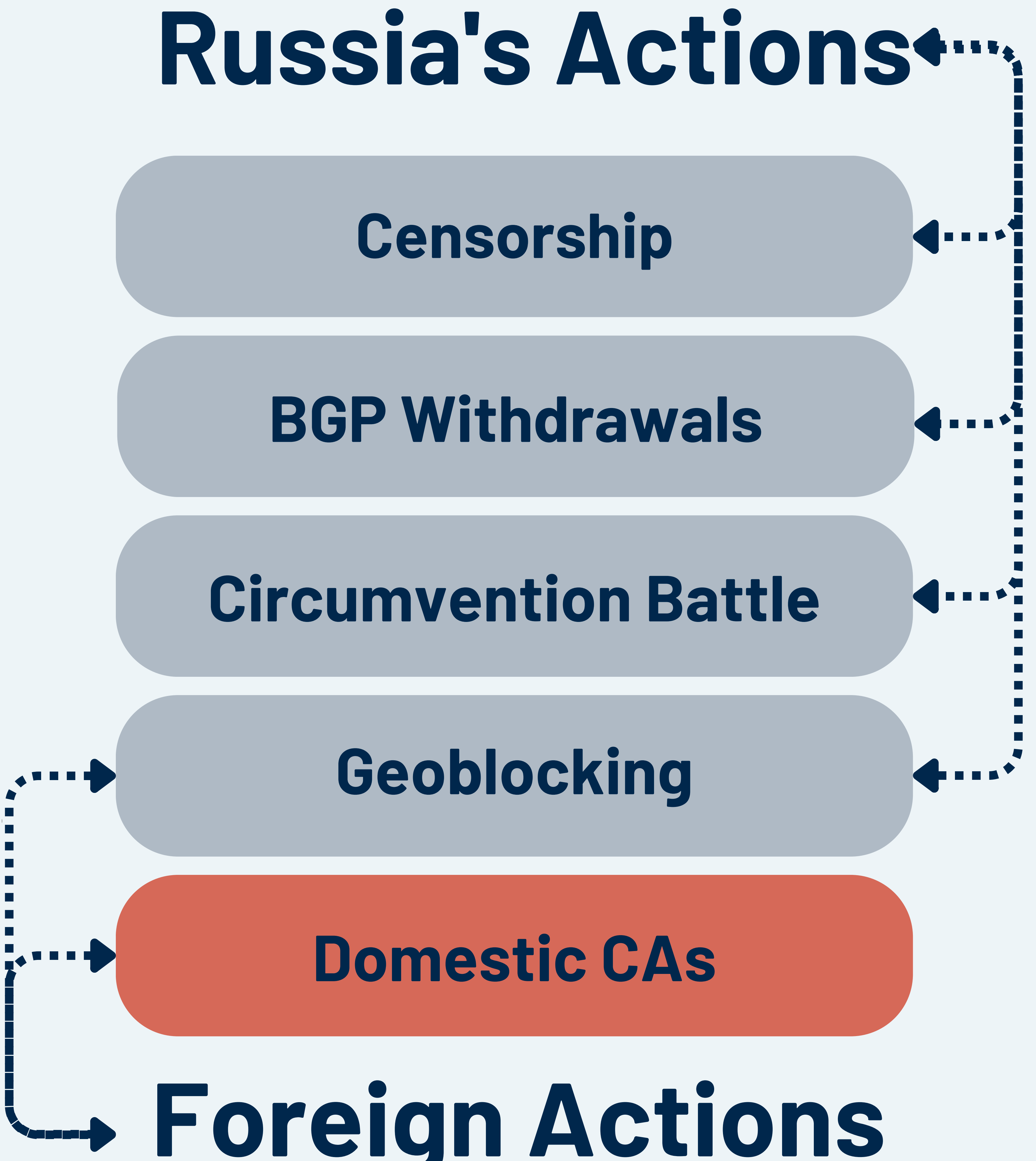
Geoblocking

Domestic CAs

Foreign Actions

Dangers to Internet Freedom





Russia's Actions

Censorship

BGP Withdrawals

Circumvention Battle

Geoblocking

Domestic CAs

Foreign Actions

Dangers to

Inte

Russia

Foreig

Increased isolation, control over messaging, and information unavailability

ls

attle

Our Study

Goal: Systematic study of network restrictions following invasion

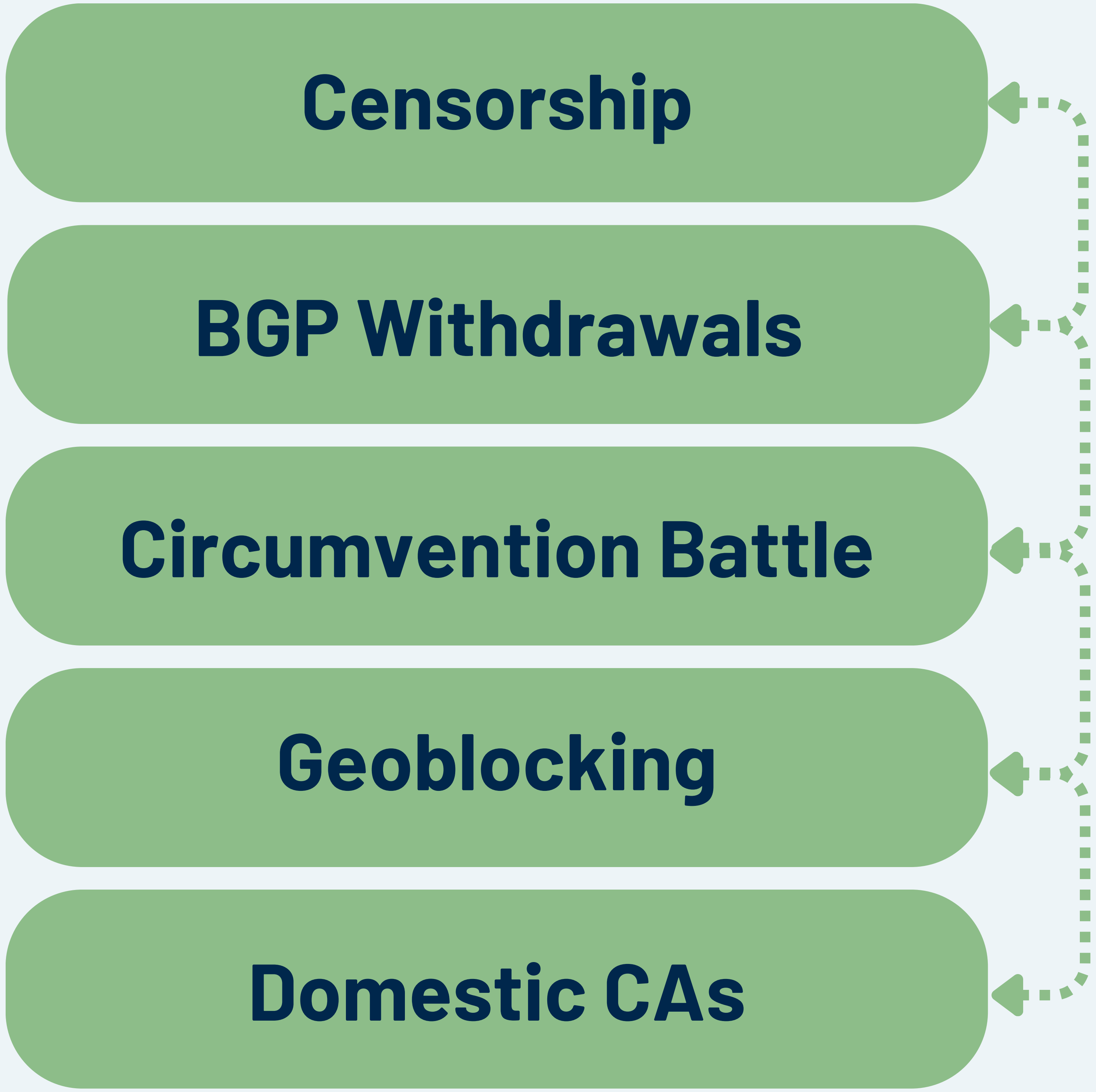
- Censorship
- BGP Withdrawals
- Circumvention Battle
- Geoblocking
- Domestic CAs

Our Study

Goal: Systematic study of network restrictions following invasion

Challenges:

1. Synthesis of multi-perspective data



Censorship

BGP Withdrawals

Circumvention Battle

Geoblocking

Domestic CAs

Our Study

Goal: Systematic study of network restrictions following invasion

Challenges:

1. Synthesis of multi-perspective data
2. New measurement techniques and diverse VPs

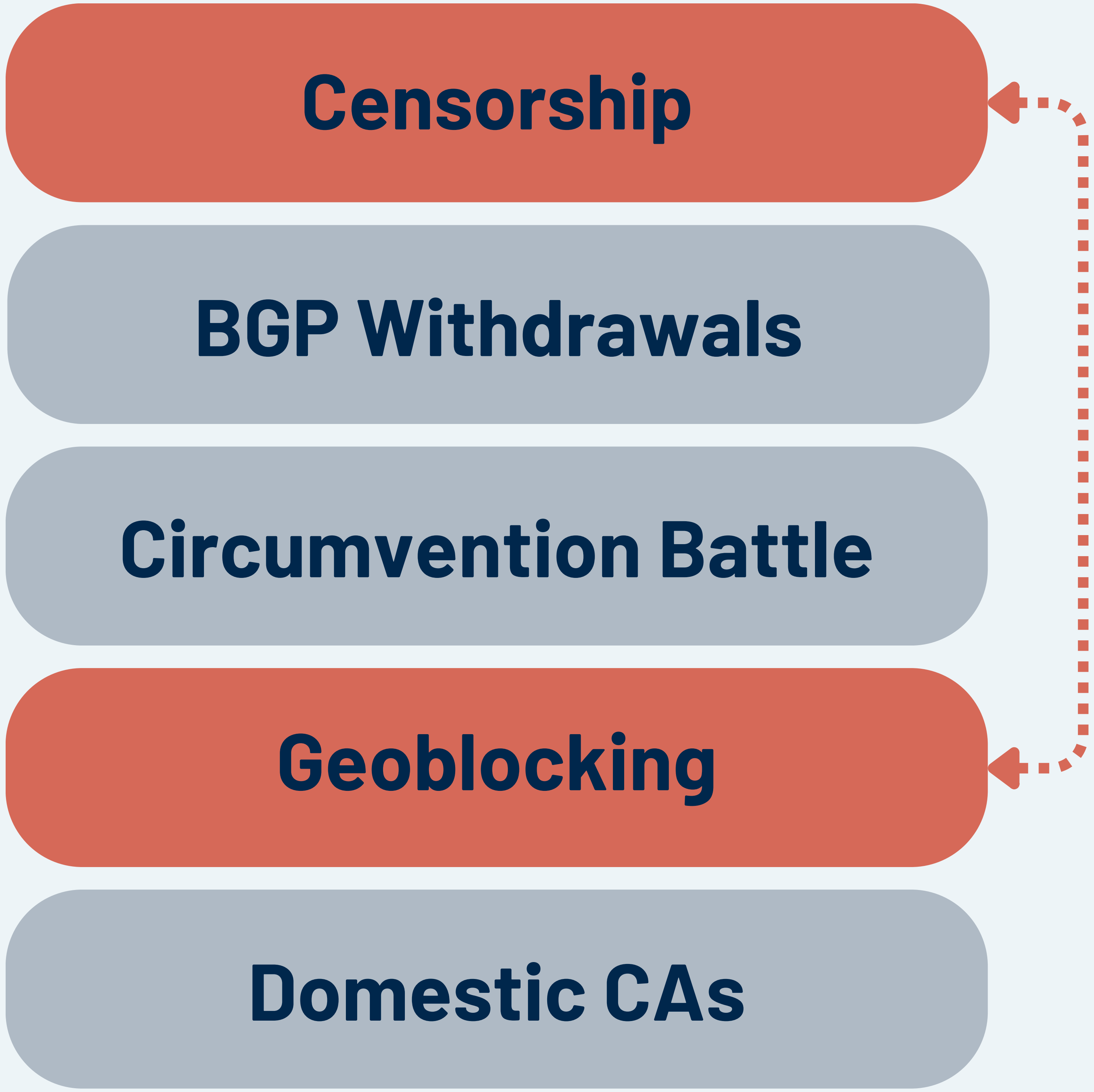
- Censorship
- BGP Withdrawals
- Circumvention Battle
- Geoblocking
- Domestic CAs

Our Study

Goal: Systematic study of network restrictions following invasion

Challenges:

1. Synthesis of multi-perspective data
2. New measurement techniques and diverse VPs
3. Differentiating restriction types



Censorship

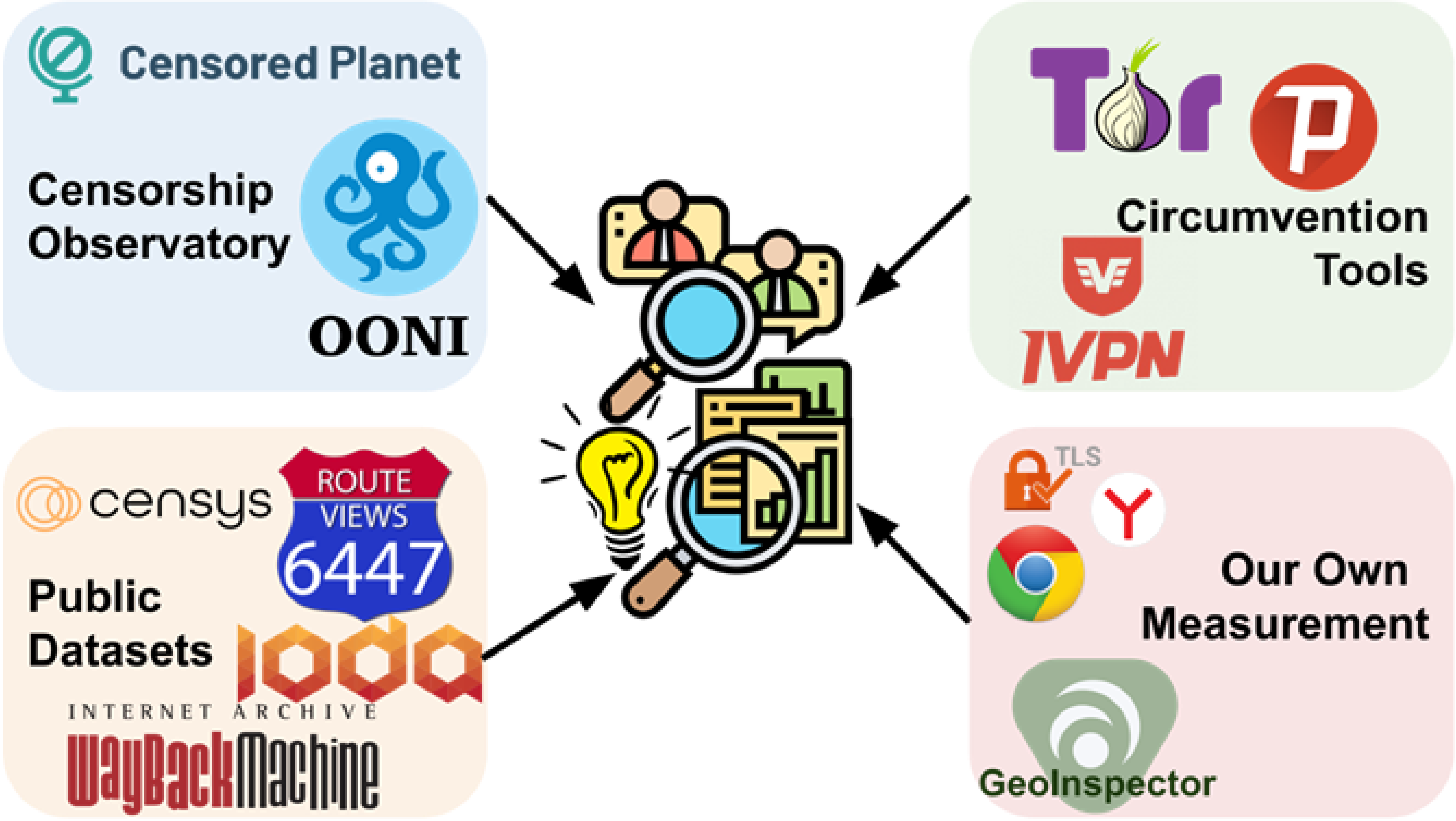
BGP Withdrawals

Circumvention Battle

Geoblocking

Domestic CAs

Our Study



New measurement tools for:

- Measuring geoblocking (GeoInspector)
- Crawling domestic TLS certificates

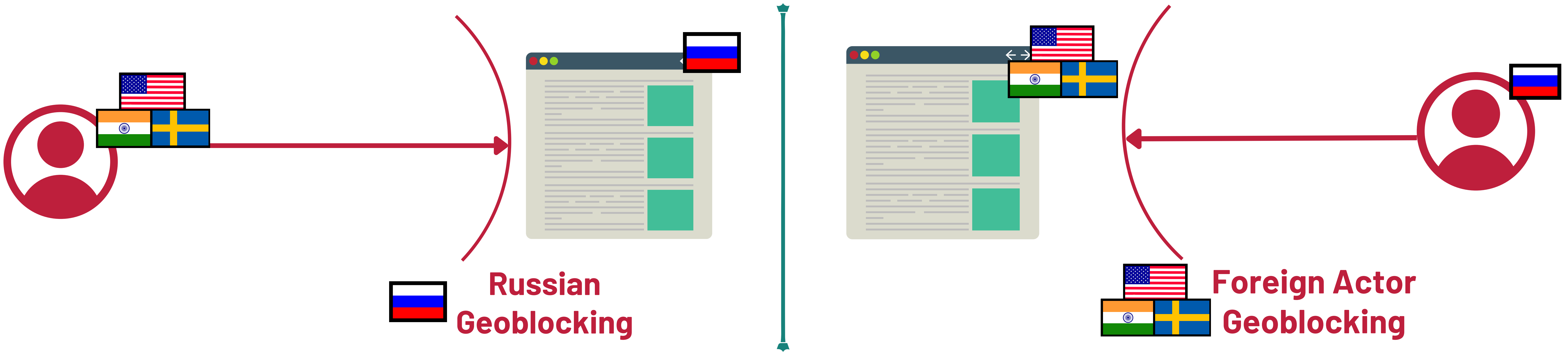
Distributed measurements from:

- 4 VPs in Russia (residential and datacenter)
- 15 VPs in other countries

Data from 9 data sources:

- Censorship Data (Censored Planet, OONI)
- BGP withdrawals (Routeviews, IODA)
- Historical data (Censys, Internet Archive)
- Circumvention Tools (Tor, Psiphon, IVPN)

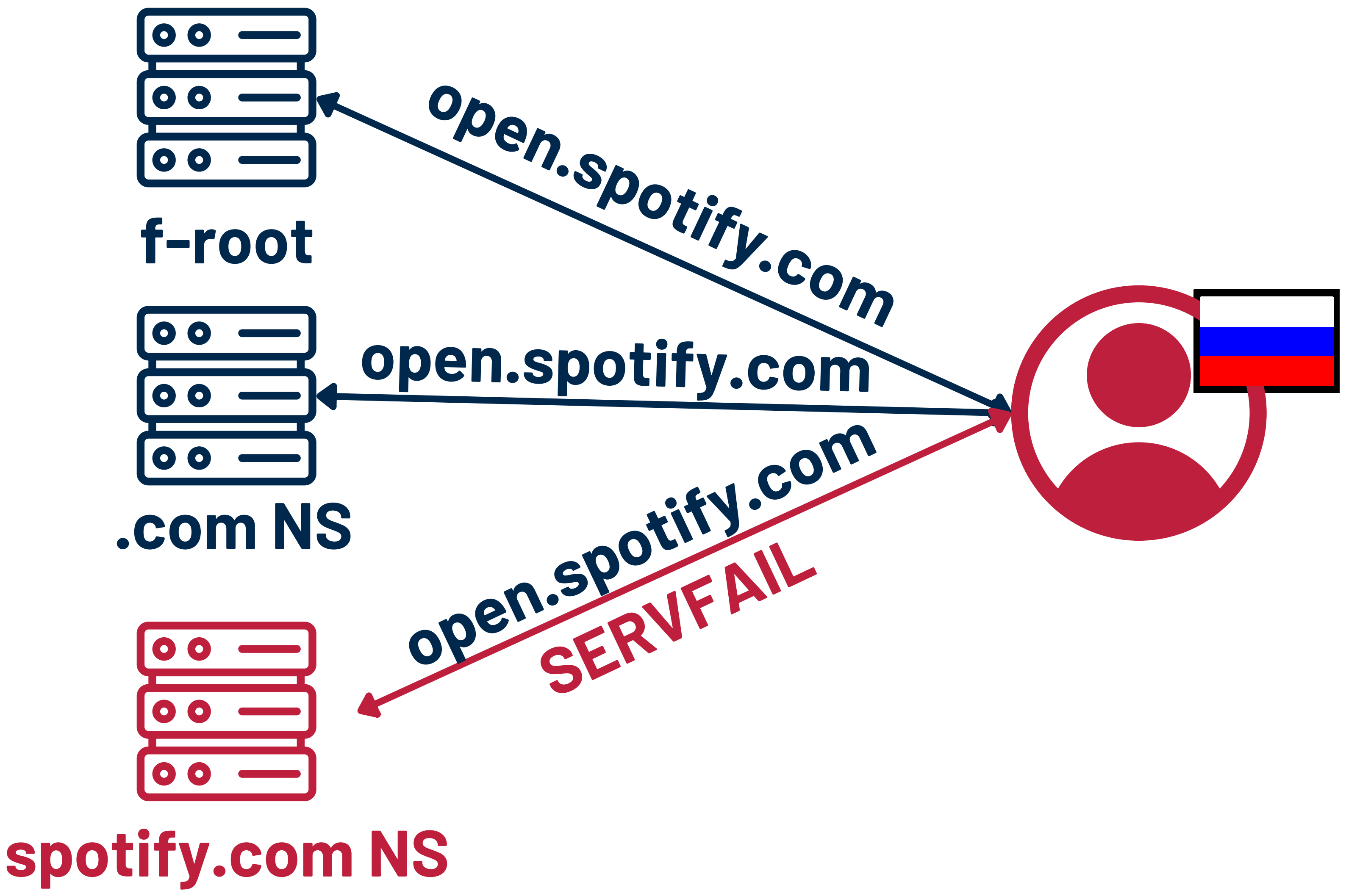
Measuring Geoblocking



GeoInspector

1. DNS Geoblocking
2. TCP & HTTP(S) Geoblocking

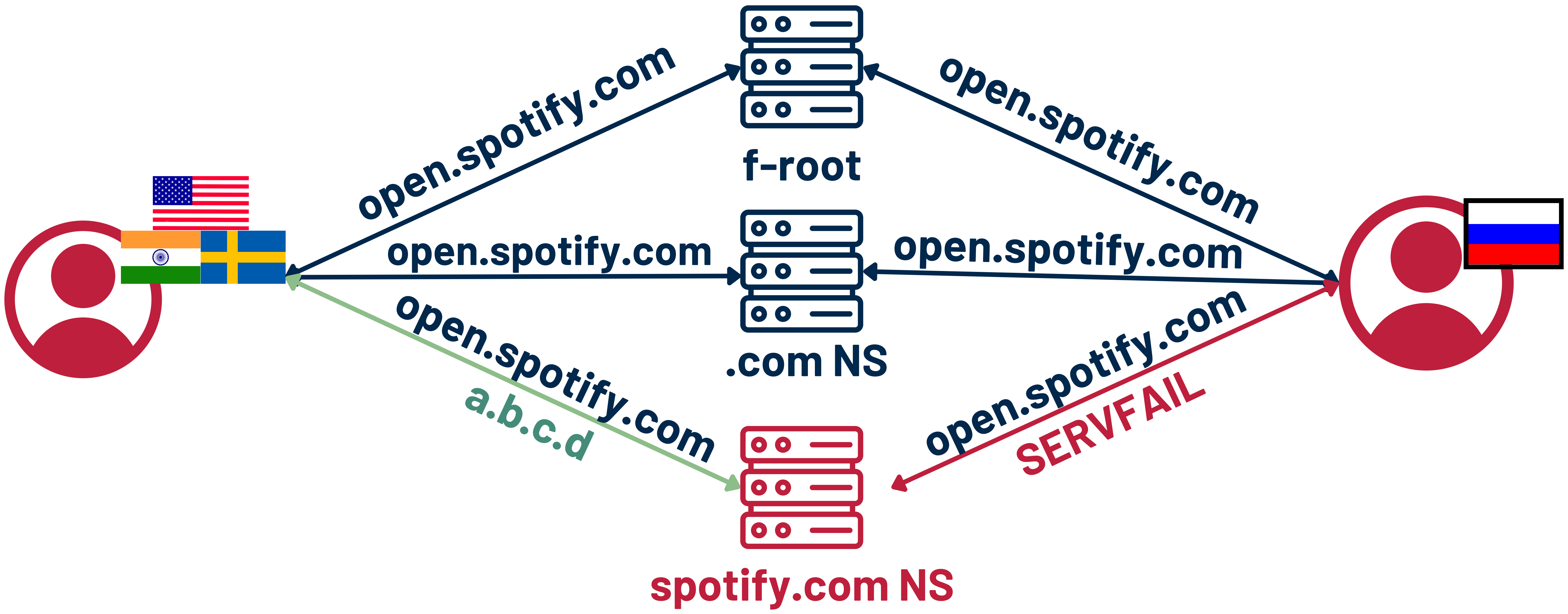
Measuring Geoblocking



GeoInspector

1. **DNS Geoblocking**
2. TCP & HTTP(S) Geoblocking

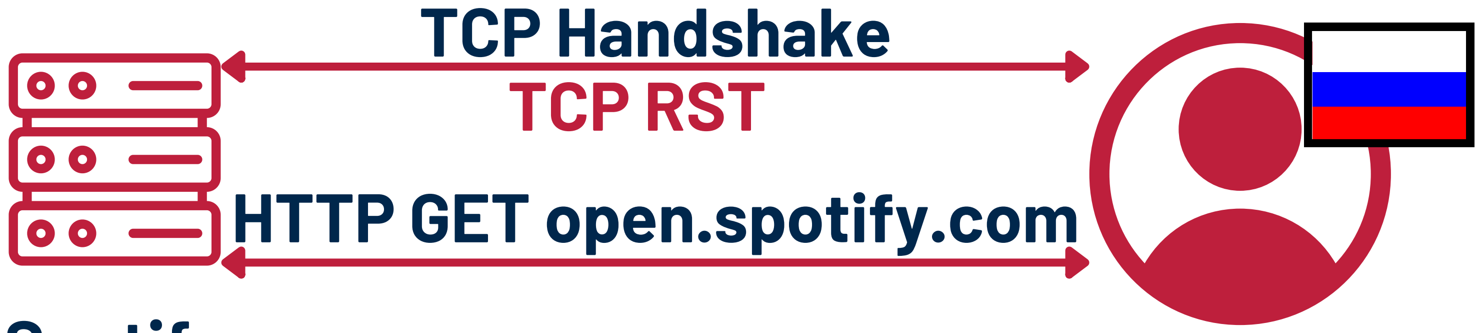
Measuring Geoblocking



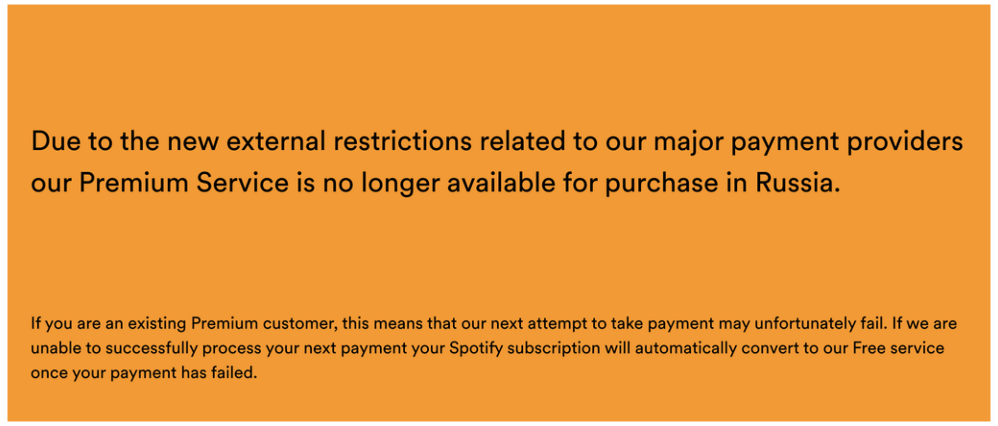
GeoInspector

1. DNS Geoblocking
2. **TCP & HTTP(S) Geoblocking**

Measuring Geoblocking



Spotify web server



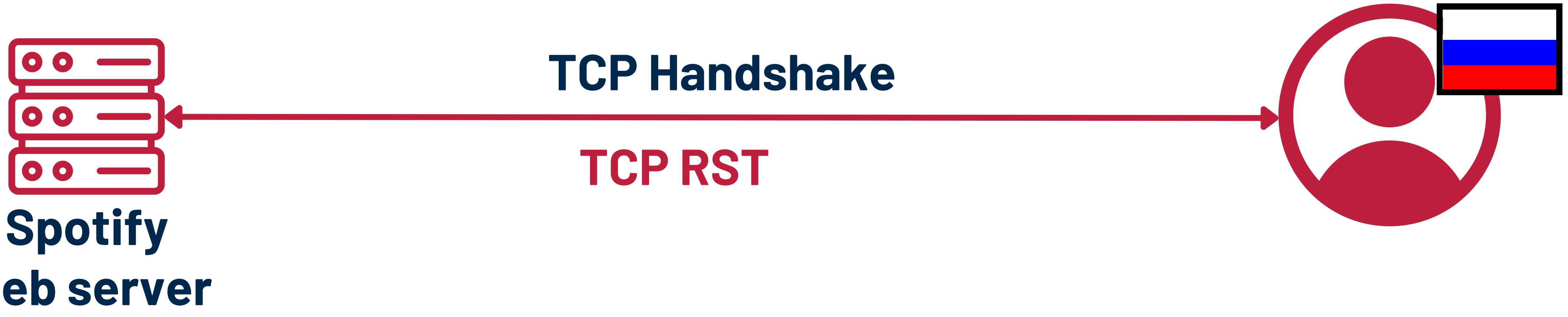
Due to the new external restrictions related to our major payment providers our Premium Service is no longer available for purchase in Russia.

If you are an existing Premium customer, this means that our next attempt to take payment may unfortunately fail. If we are unable to successfully process your next payment your Spotify subscription will automatically convert to our Free service once your payment has failed.

GeoInspector

1. DNS Geoblocking
2. **TCP & HTTP(S) Geoblocking**

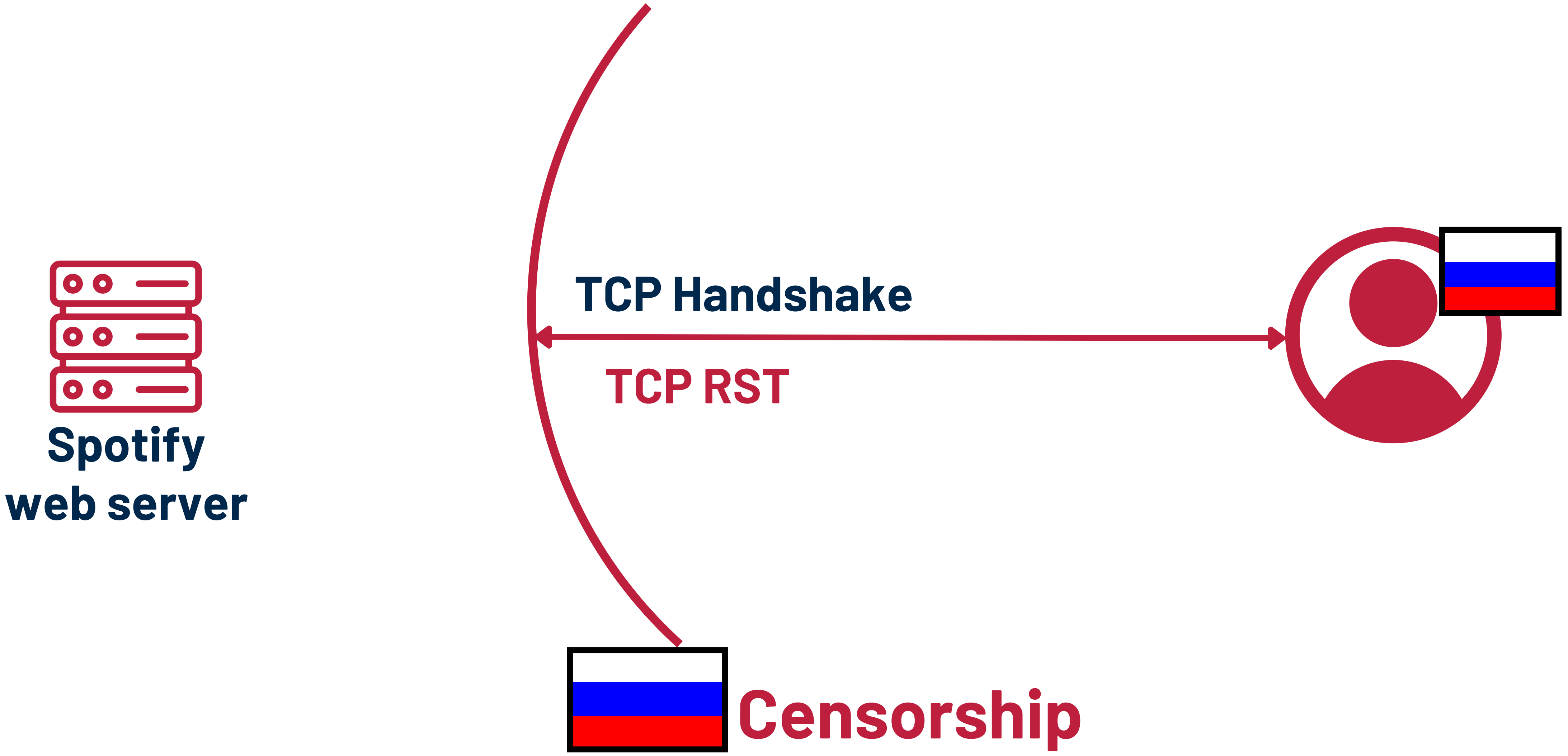
Measuring Geoblocking



GeoInspector

1. DNS Geoblocking
2. **TCP & HTTP(S) Geoblocking**

Measuring Geoblocking

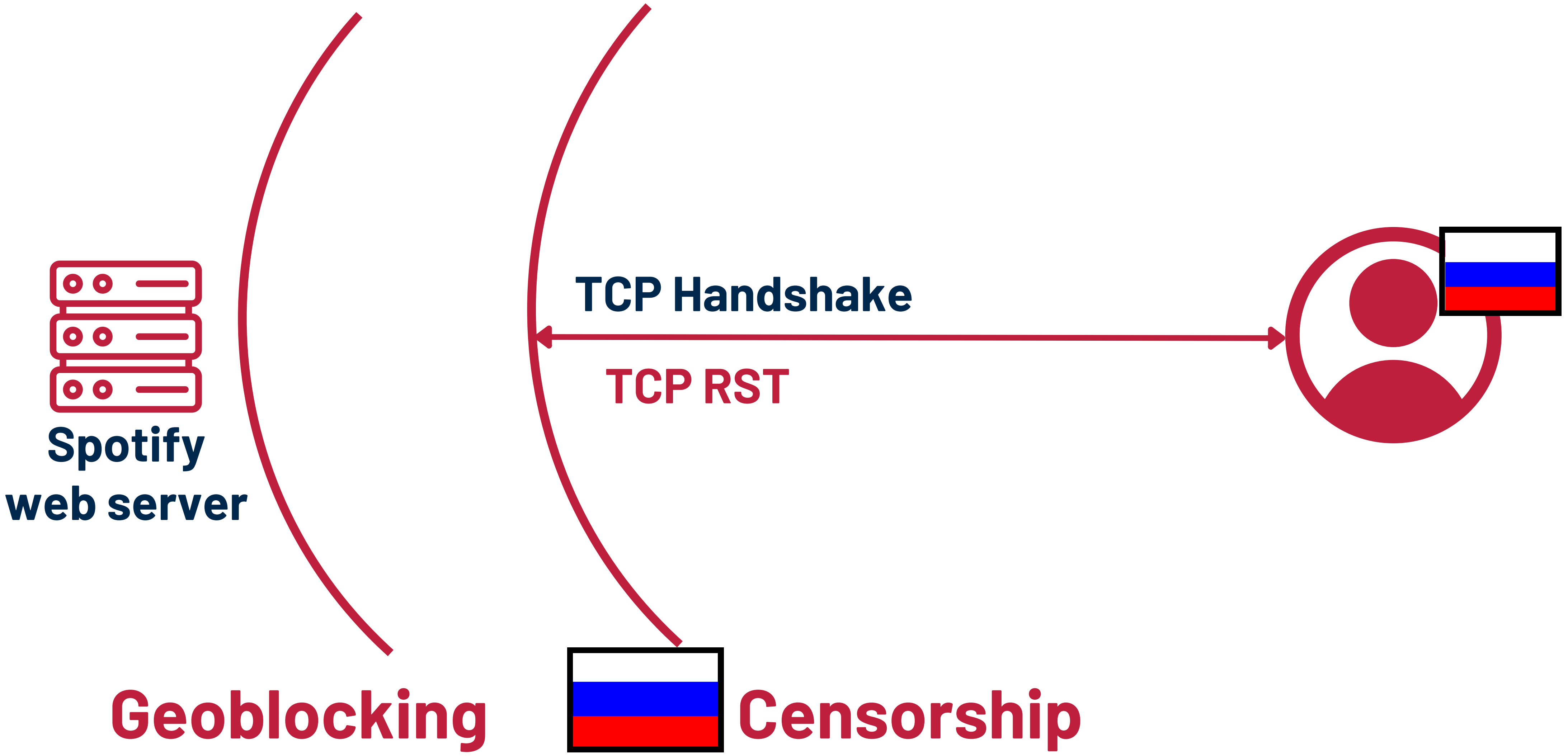


GeoInspector

1. DNS Geoblocking
2. **TCP & HTTP(S) Geoblocking**

Measuring Geoblocking

How to differentiate censorship & geoblocking?



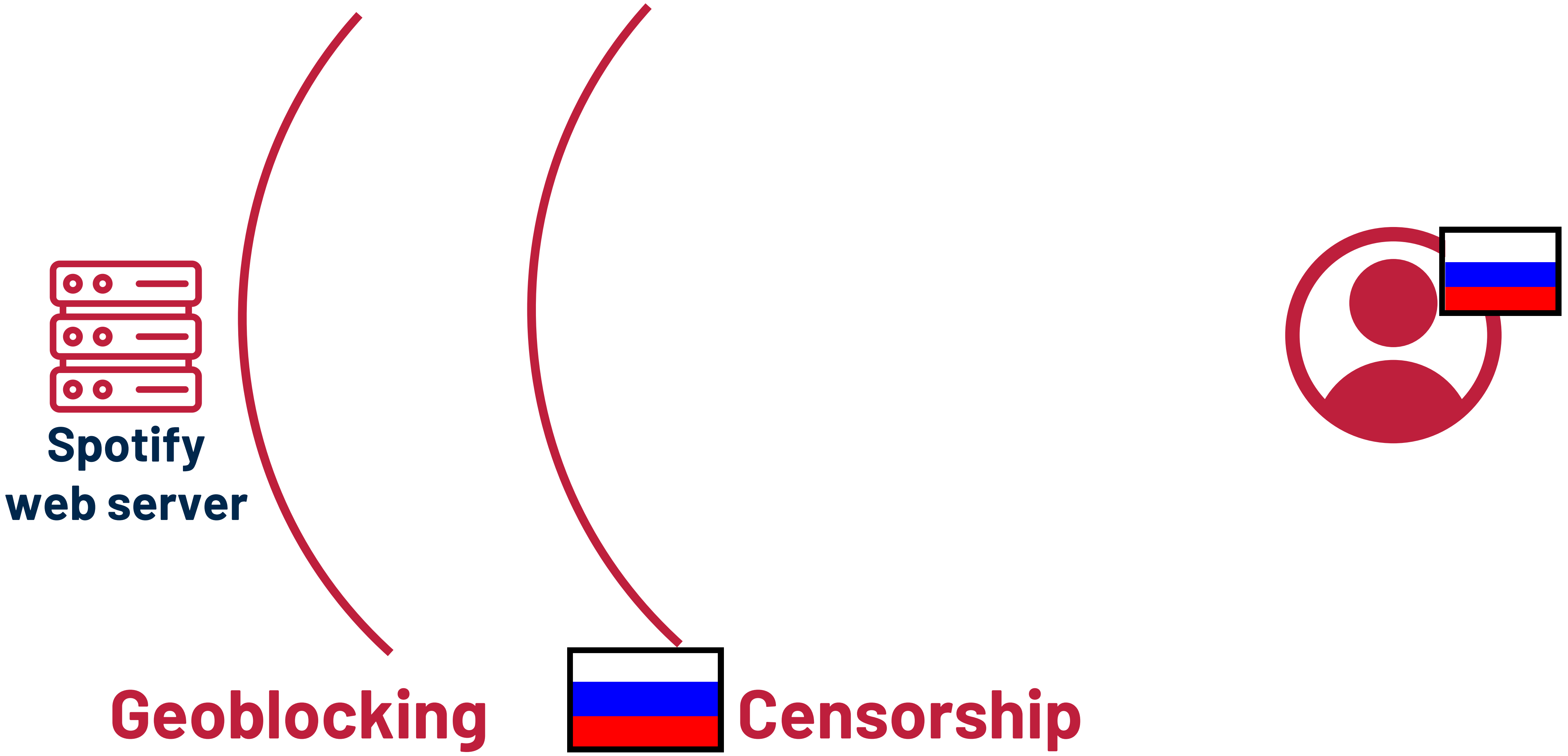
Measuring Geoblocking

GeoInspector

1. DNS Geoblocking
2. **TCP & HTTP(S) Geoblocking**

CenTrace

TCP and HTTP(S) traceroutes



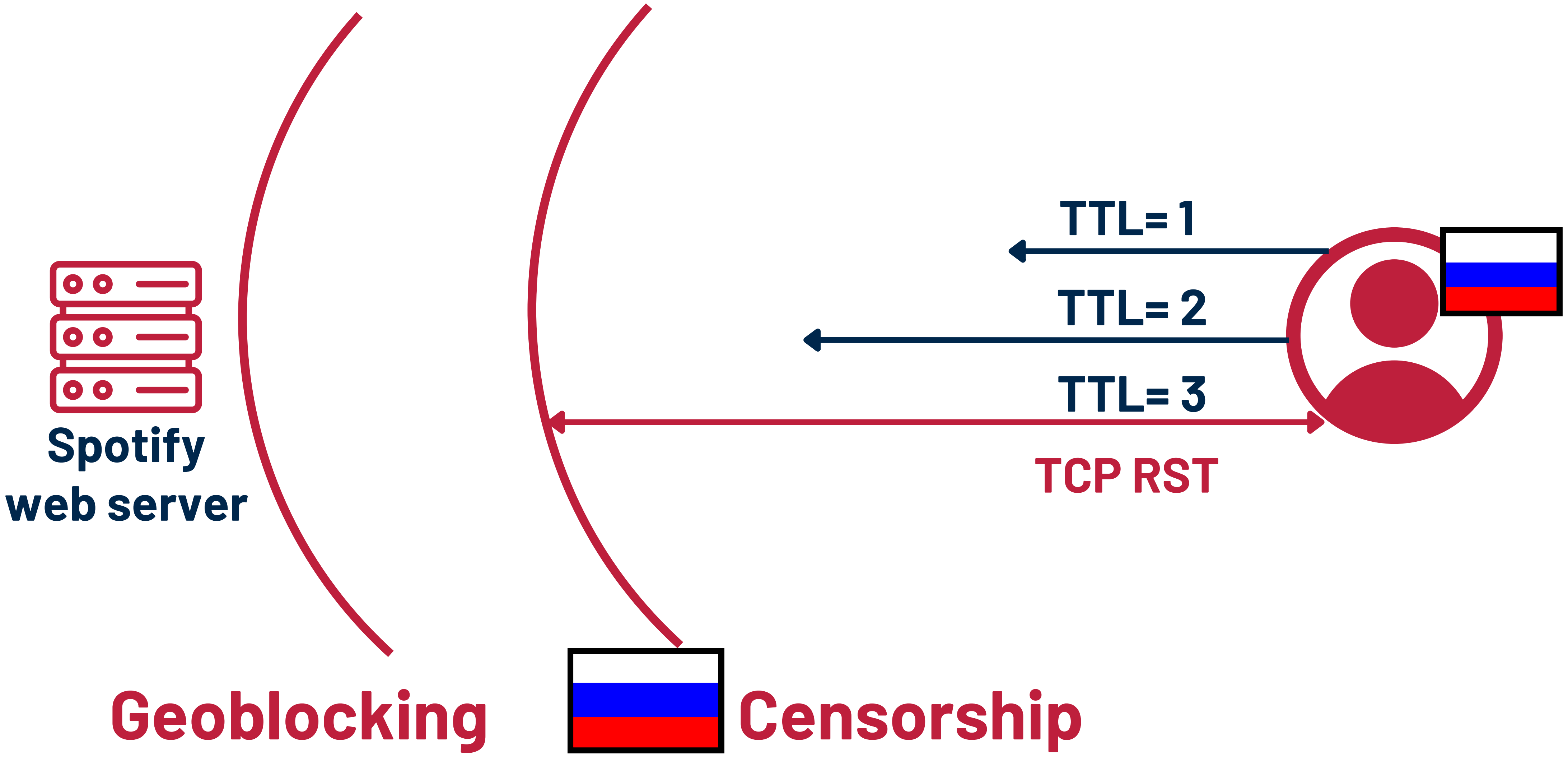
GeoInspector

1. DNS Geoblocking
2. **TCP & HTTP(S) Geoblocking**

Measuring Geoblocking

CenTrace

TCP and HTTP(S) traceroutes



GeoInspector

1. DNS Geoblocking
2. TCP & HTTP(S) Geoblocking

Measuring Geoblocking

CenTrace

TCP and HTTP(S) traceroutes

Measurements in May, 2022:

1. **623 Russian government domains** from 15 geodiverse VPs
2. **8,763 popular domains** from 4 Russian VPs

GeoInspector

1. DNS Geoblocking
2. TCP & HTTP(S) Geoblocking

Measuring Geoblocking

CenTrace

TCP and HTTP(S) traceroutes

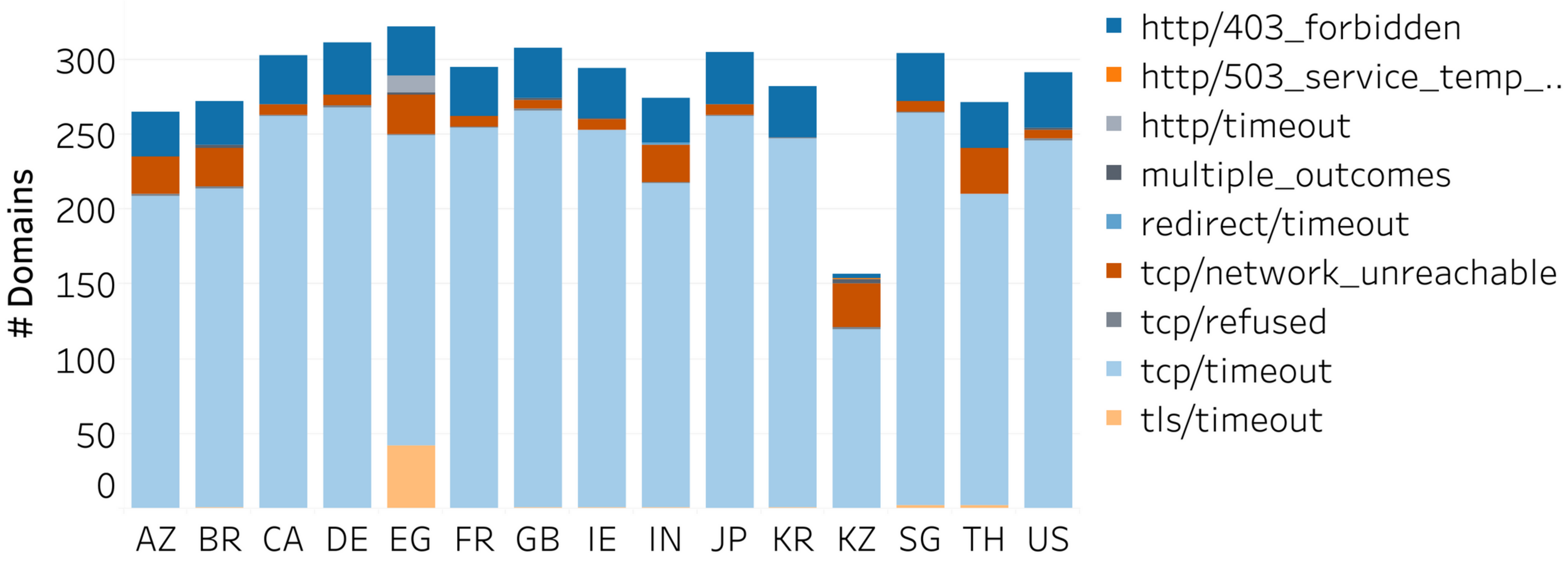
Measurements in May, 2022:

1. **623 Russian government domains** from 15 geodiverse VPs
2. **8,763 popular domains** from 4 Russian VPs

What did we find?

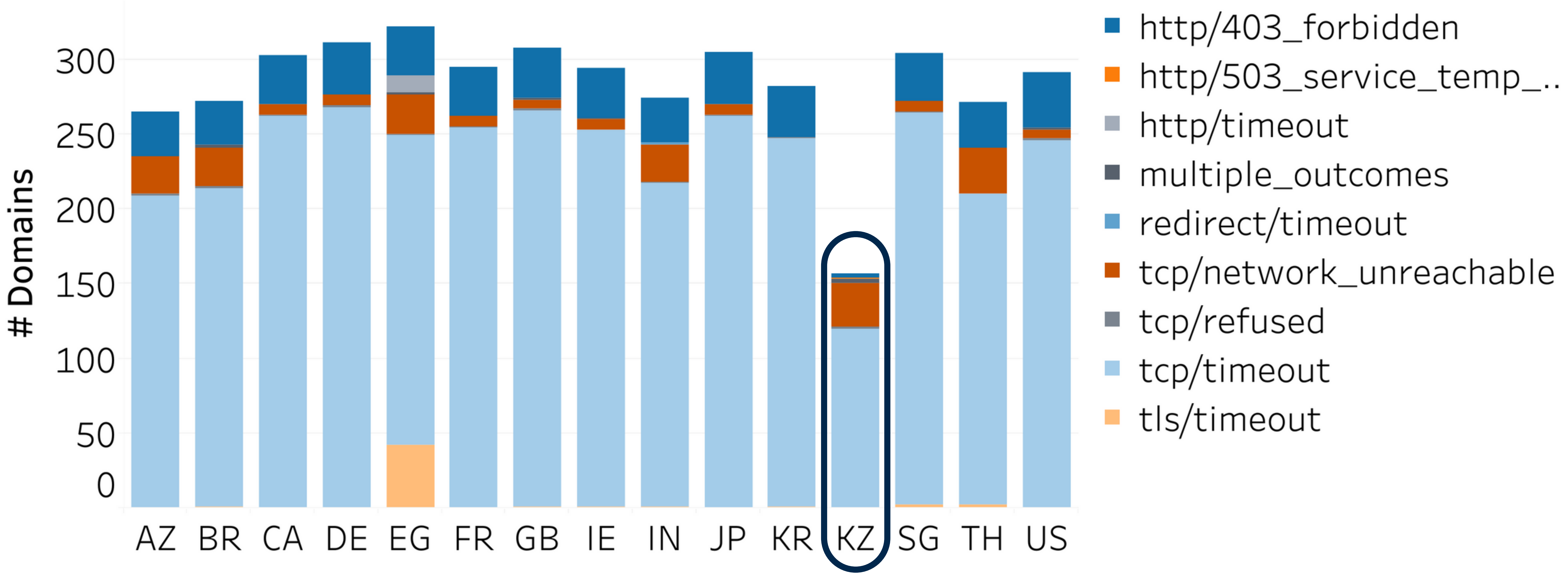
Significant geofencing by RU .gov domains

Significant geofencing by RU .gov domains



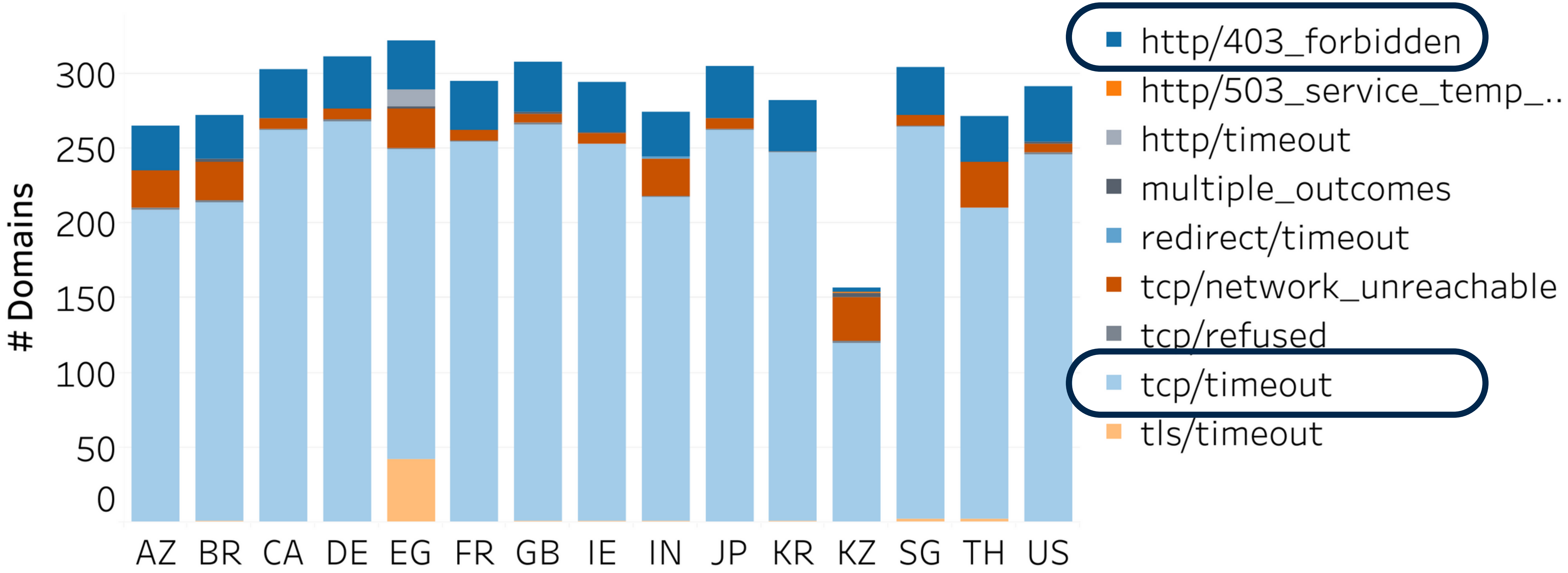
- **134 domains (>25%) not available outside RU**
- Interestingly, another 20% accessible from only RU and KZ
- TCP Timeouts and HTTP blockpages common

Significant geofencing by RU .gov domains



- 134 domains (>25%) not available outside RU
- **Interestingly, another 20% accessible from only RU and KZ**
- TCP Timeouts and HTTP blockpages common

Significant geofencing by RU .gov domains



- 134 domains (>25%) not available outside RU
- Interestingly, another 20% accessible from only RU and KZ
- **TCP Timeouts and HTTP blockpages common**

GeoInspector

1. DNS Geoblocking
2. TCP & HTTP(S) Geoblocking

Measuring Geoblocking

CenTrace

TCP and HTTP(S) traceroutes

Measurements in May, 2022:

1. **623 Russian government domains** from 15 geodiverse VPs
2. **8,763 popular domains** from 4 Russian VPs

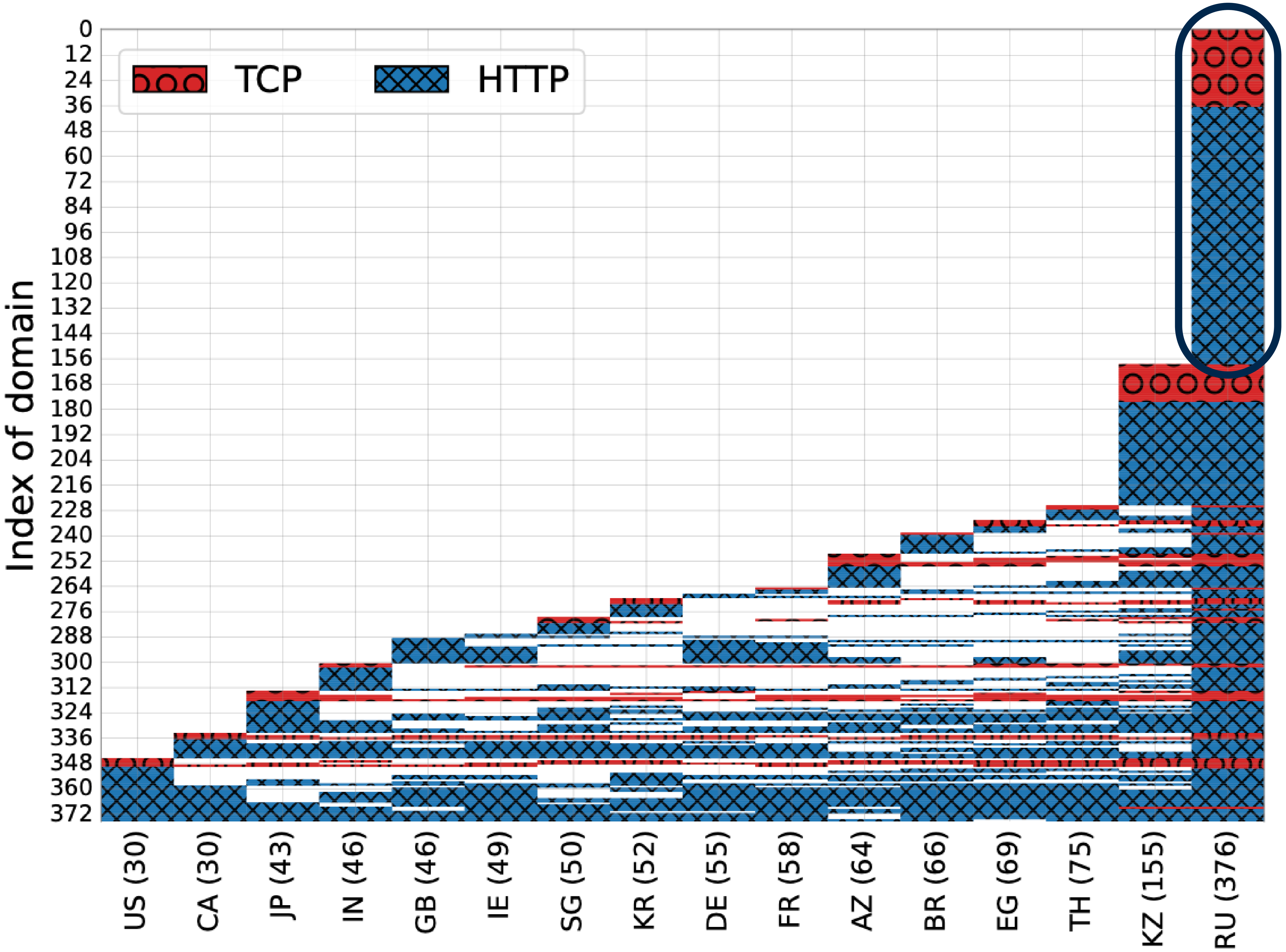
What did we find?

Significant geofencing by RU .gov domains

Significant geoblocking of RU and KZ users by popular domains

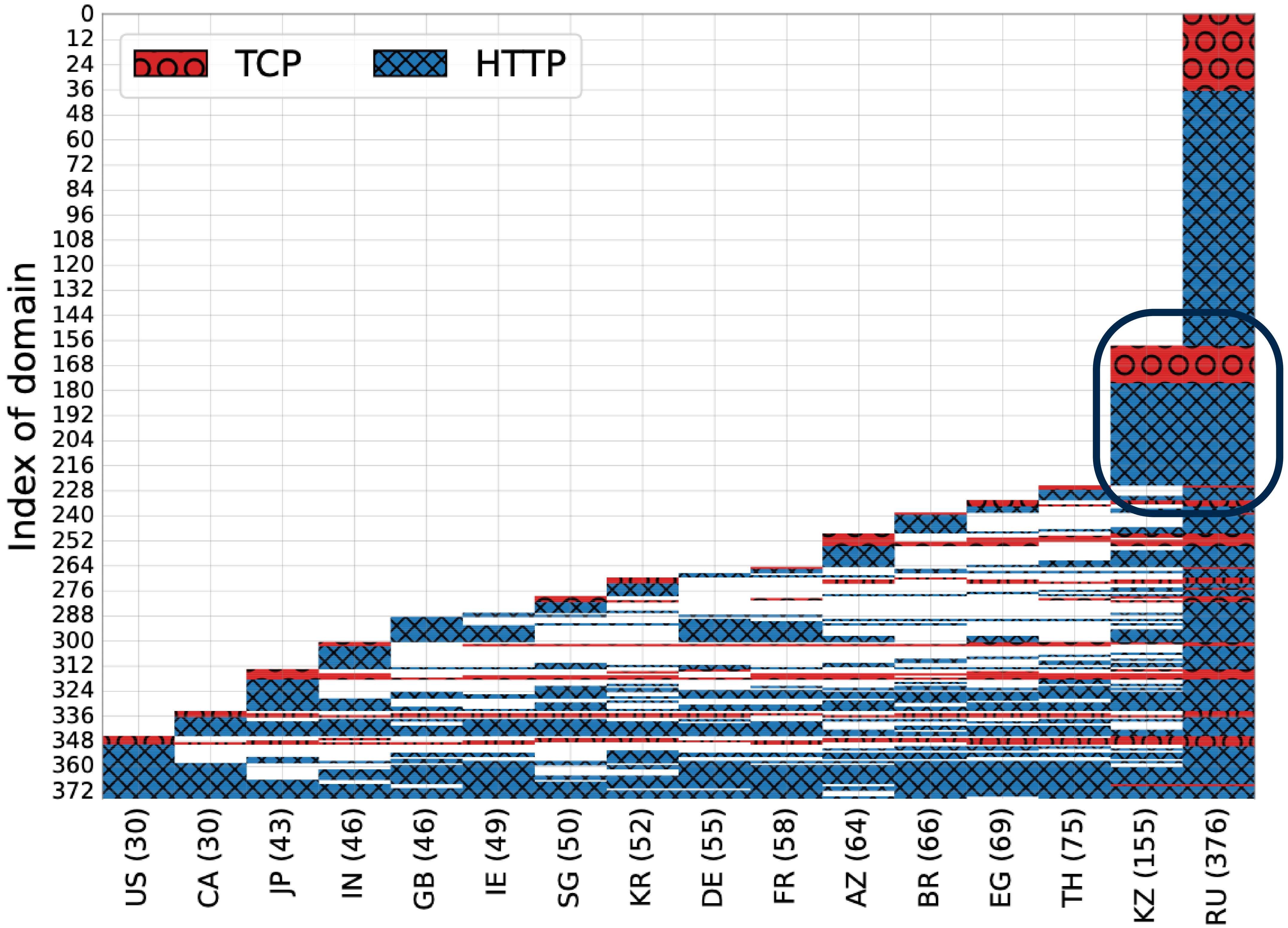
Significant geoblocking of RU and KZ users by popular domains

- **159 domains not available only in RU**
- Another 67 are unavailable in RU and KZ
- A majority of domains served HTTP blockpages (including CDN pages)
- Government, Education, Shopping, News (e.g. *pbs.org*)



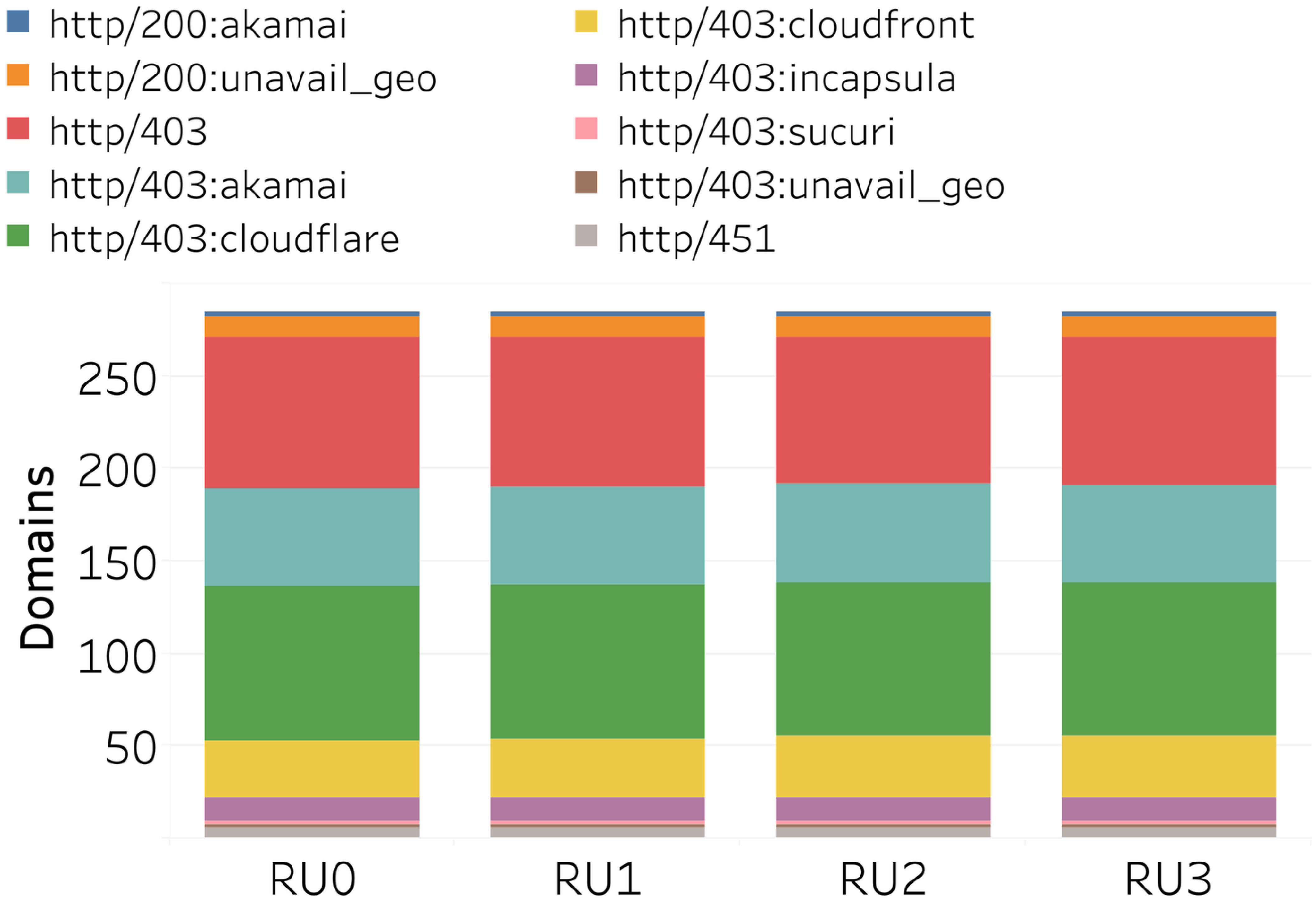
Significant geoblocking of RU and KZ users by popular domains

- 159 domains not available only in RU
- **Another 67 are unavailable in RU and KZ**
- A majority of domains served HTTP blockpages (including CDN pages)
- Government, Education, Shopping, News (e.g. *pbs.org*)



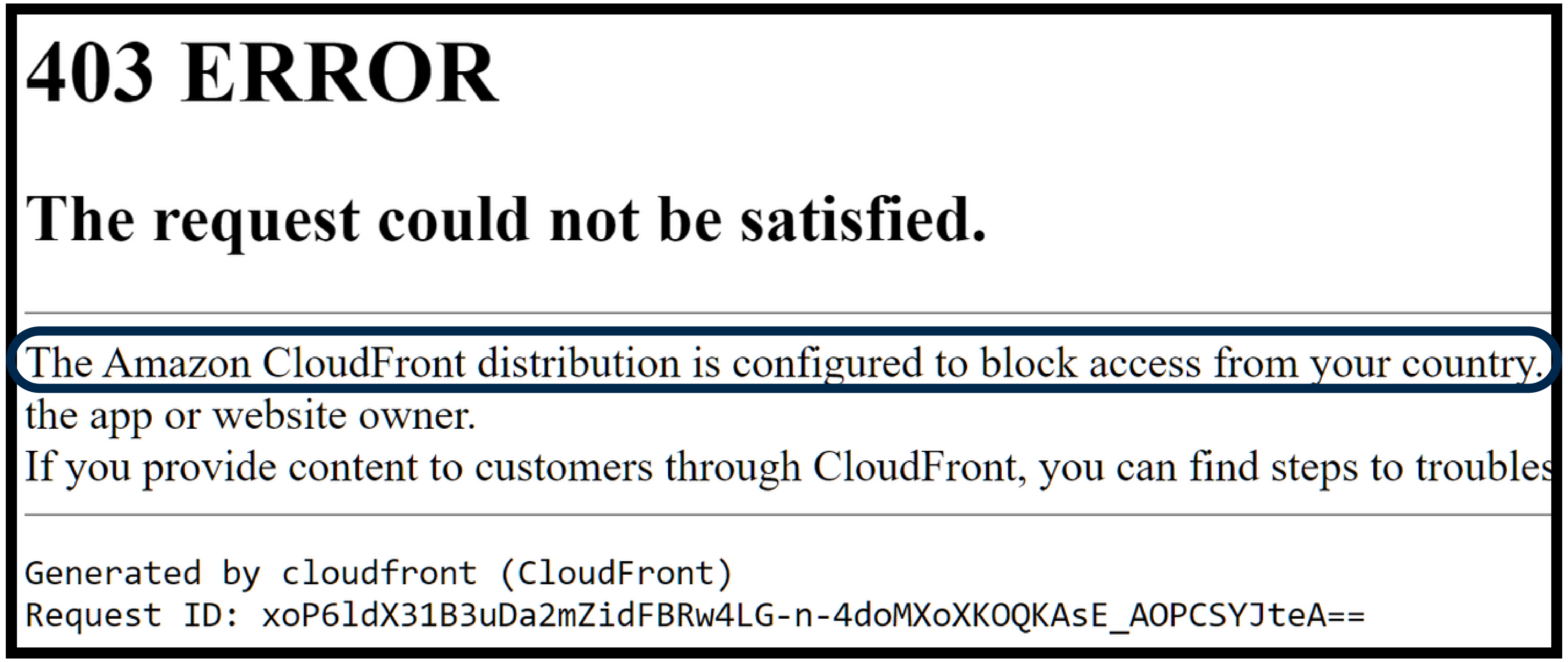
Significant geoblocking of RU and KZ users by popular domains

- 159 domains not available only in RU
- Another 67 are unavailable in RU and KZ
- **A majority of domains served HTTP blockpages (including CDN pages)**
- Government, Education, Shopping, News (e.g. *pbs.org*)



Significant geoblocking of RU and KZ users by popular domains

- 159 domains not available only in RU
- Another 67 are unavailable in RU and KZ
- A majority of domains served HTTP blockpages (including CDN pages)
- **Government, Education, Shopping, News (e.g. *pbs.org*)**



403 ERROR

The request could not be satisfied.

The Amazon CloudFront distribution is configured to block access from your country.
the app or website owner.
If you provide content to customers through CloudFront, you can find steps to troubles

```
Generated by cloudfront (CloudFront)
Request ID: xoP6ldX31B3uDa2mZidFBRw4LG-n-4doMXoXKOQKAsE_AOPCSYJteA==
```

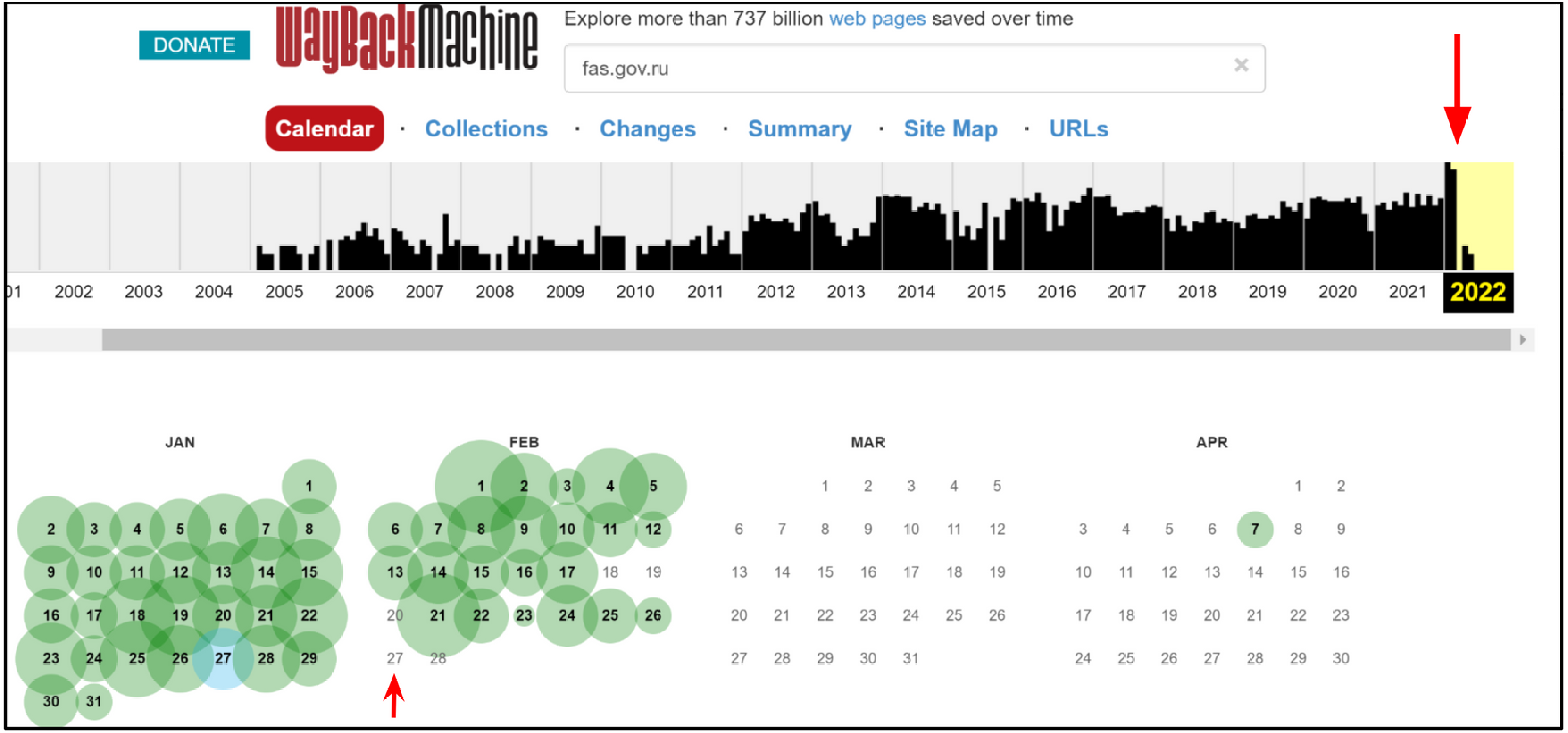
GeoInspector

CenTrace

Is there a connection between the invasion and the geoblocking?

Significant geoblocking of RU and KZ users by popular domains

Is there a connection between the invasion and the geoblocking?



Explore more than 737 billion web pages saved over time

fas.gov.ru

JAN

						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

FEB

		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28					

MAR

		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

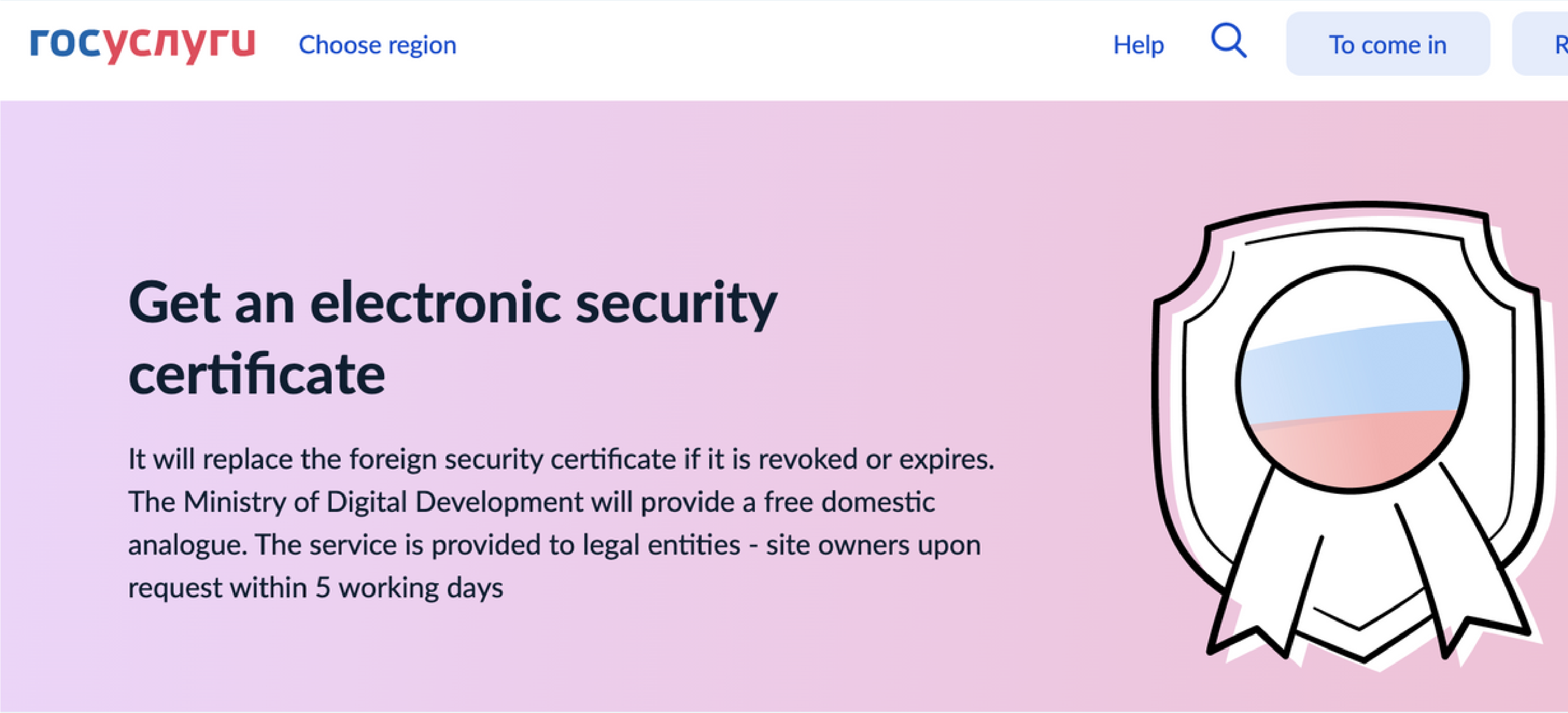
APR

					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

Russia’s Domestic Certificate Authority

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

- **Reaction:** Ministry of Digital Development provided a **free domestic certificate (CN=Russian Trusted Root CA)** to replace foreign expired or revoked certificates



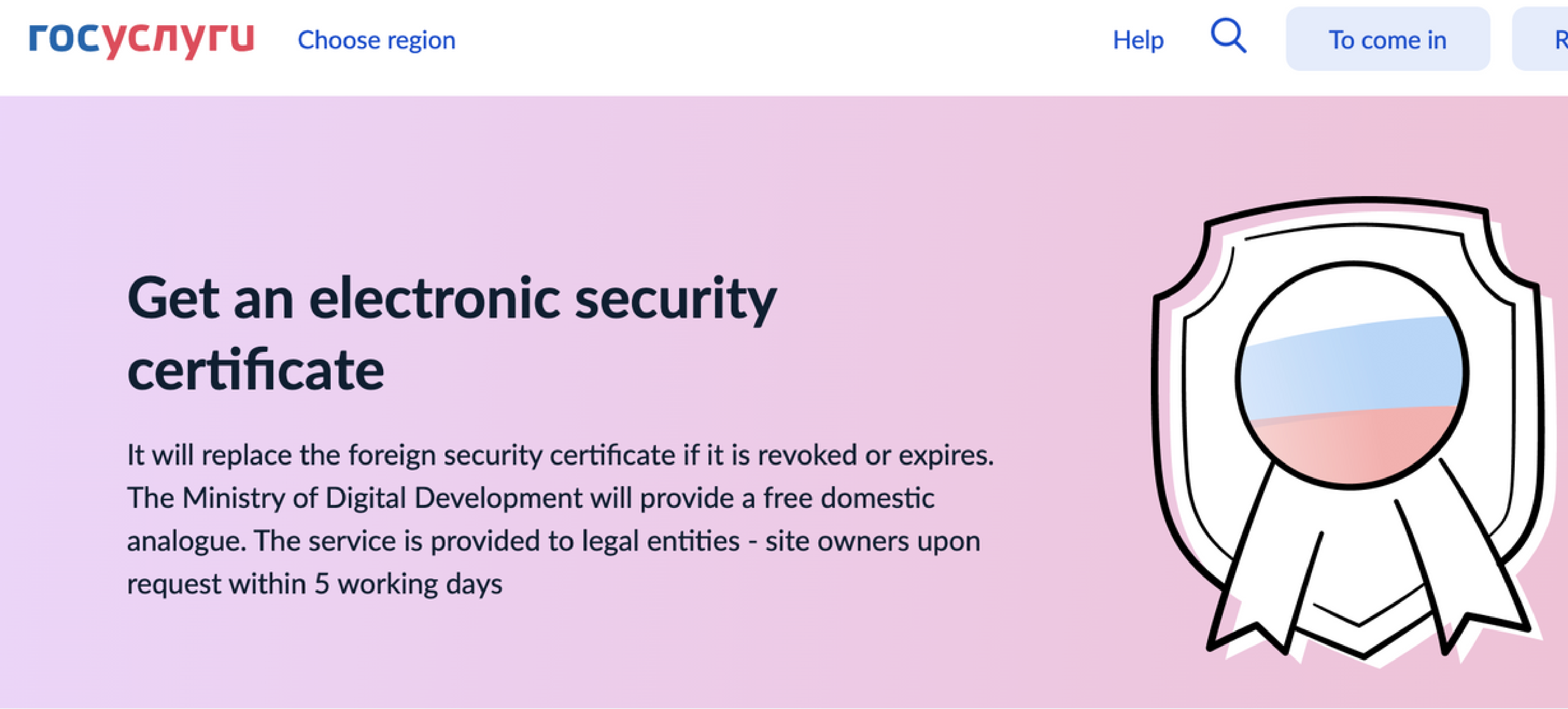
Get an electronic security certificate

It will replace the foreign security certificate if it is revoked or expires. The Ministry of Digital Development will provide a free domestic analogue. The service is provided to legal entities - site owners upon request within 5 working days

Russia's Domestic Certificate Authority

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

- **Reaction:** Ministry of Digital Development provided a **free domestic certificate (CN=Russian Trusted Root CA)** to replace foreign expired or revoked certificates



Get an electronic security certificate

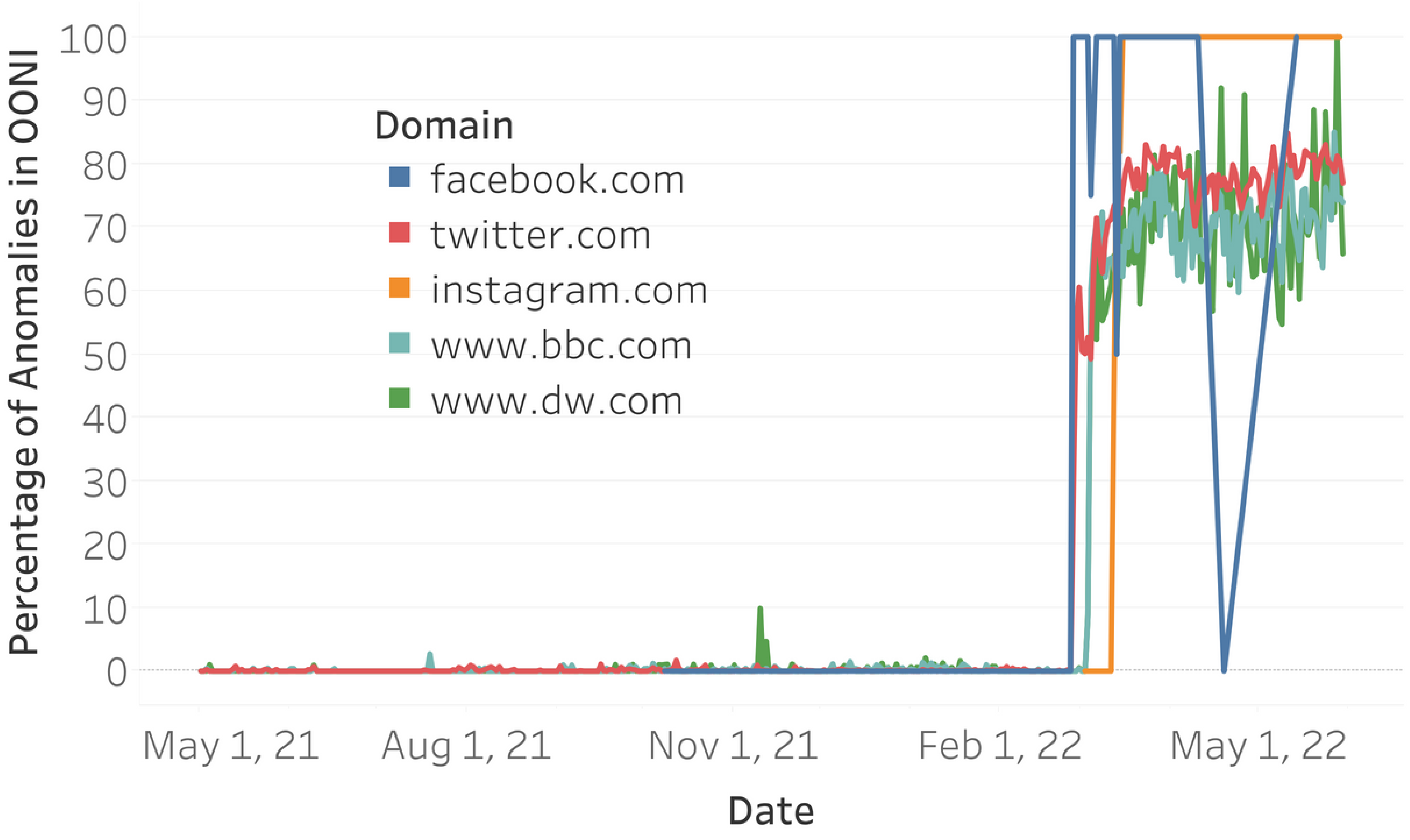
It will replace the foreign security certificate if it is revoked or expires. The Ministry of Digital Development will provide a free domestic analogue. The service is provided to legal entities - site owners upon request within 5 working days

- 3,722 domains signed in May '22, crawled using Yandex and Chrome browsers

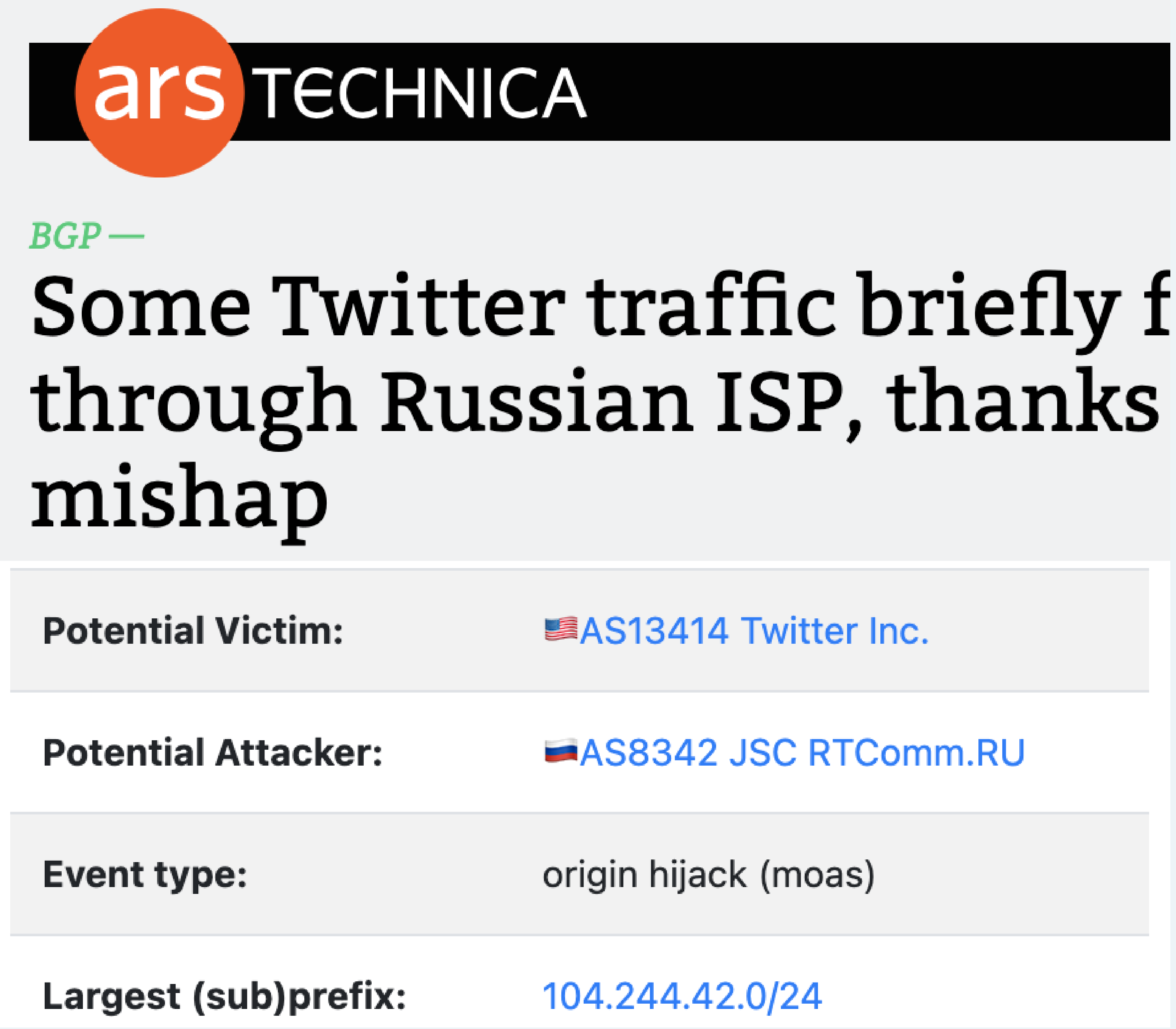
- 114 (3%) domains presented the new Russian certificate in Yandex

- 46 domains had a recently expired certificate originally issued by a trusted CA

Website Censorship



BGP Withdrawals



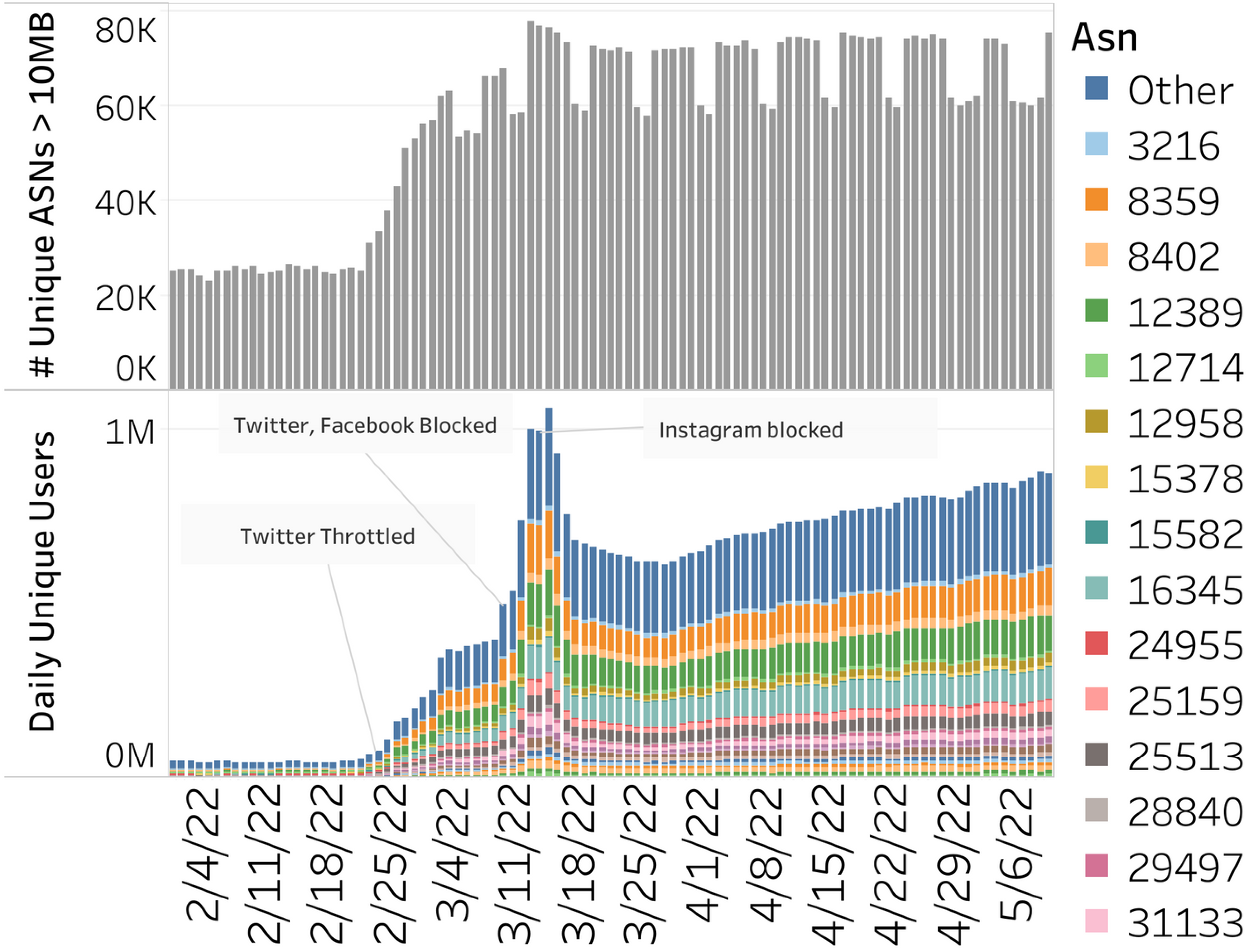
ars TECHNICA

BGP —

Some Twitter traffic briefly f
through Russian ISP, thanks
mishap

Potential Victim:	🇺🇸AS13414 Twitter Inc.
Potential Attacker:	🇷🇺AS8342 JSC RTComm.RU
Event type:	origin hijack (moas)
Largest (sub)prefix:	104.244.42.0/24

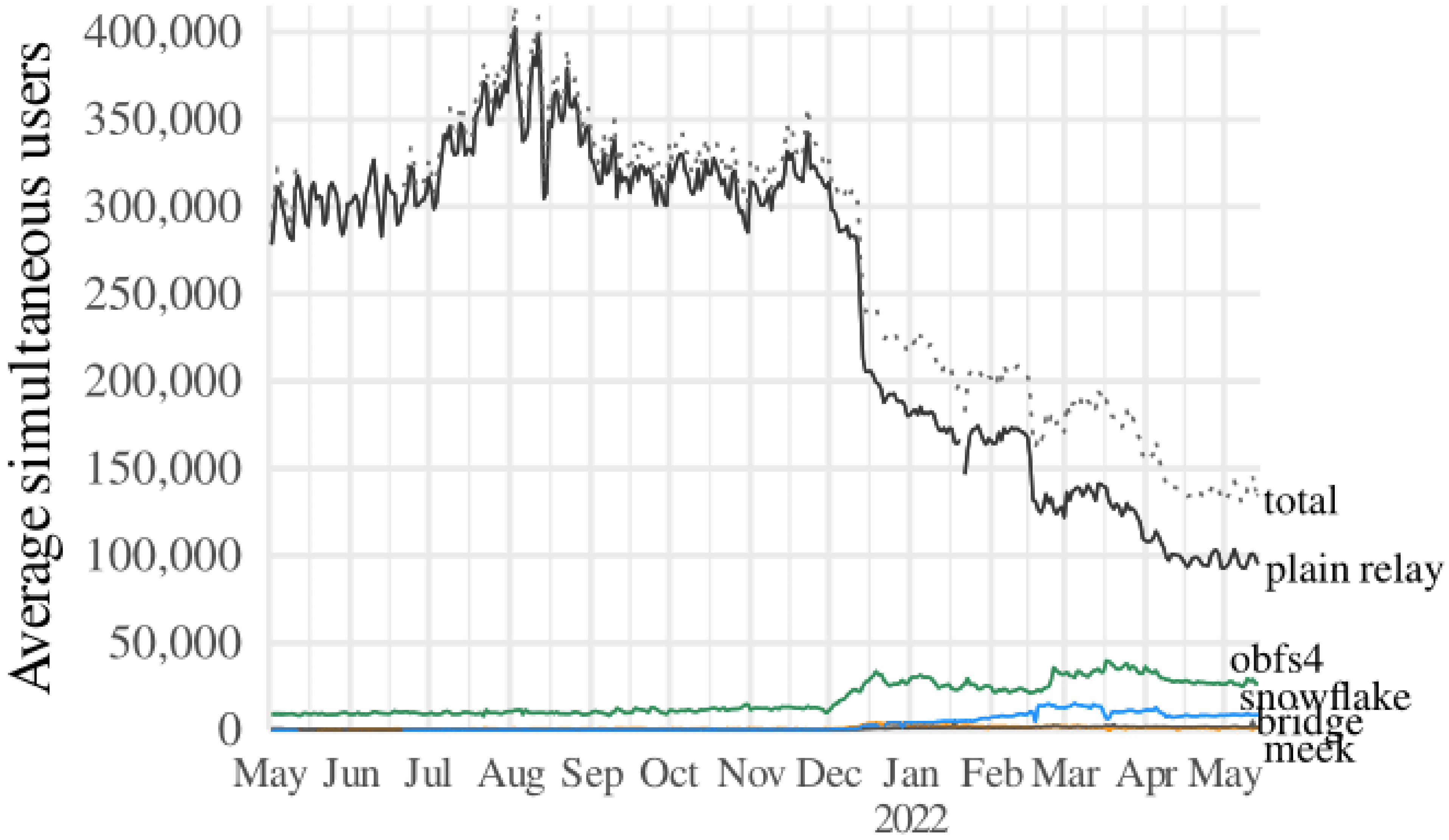
Russia and the Circumvention Community



Psiphon

- **Throttled Twitter ->** Psiphon use **rapidly escalated** as Russia began throttling access to Twitter
- **Blocked Instagram** -> **Psiphon usage peaked** at over 1.1M daily unique users
- Increase was observed in all major ASNs
- Observed changes in Psiphon protocols used at **the same time across many ASNs -> centralized censorship of circumvention**

Russia and the Circumvention Community



Tor

- In Dec 2021, **Tor network was blocked** in many ISPs in Russia

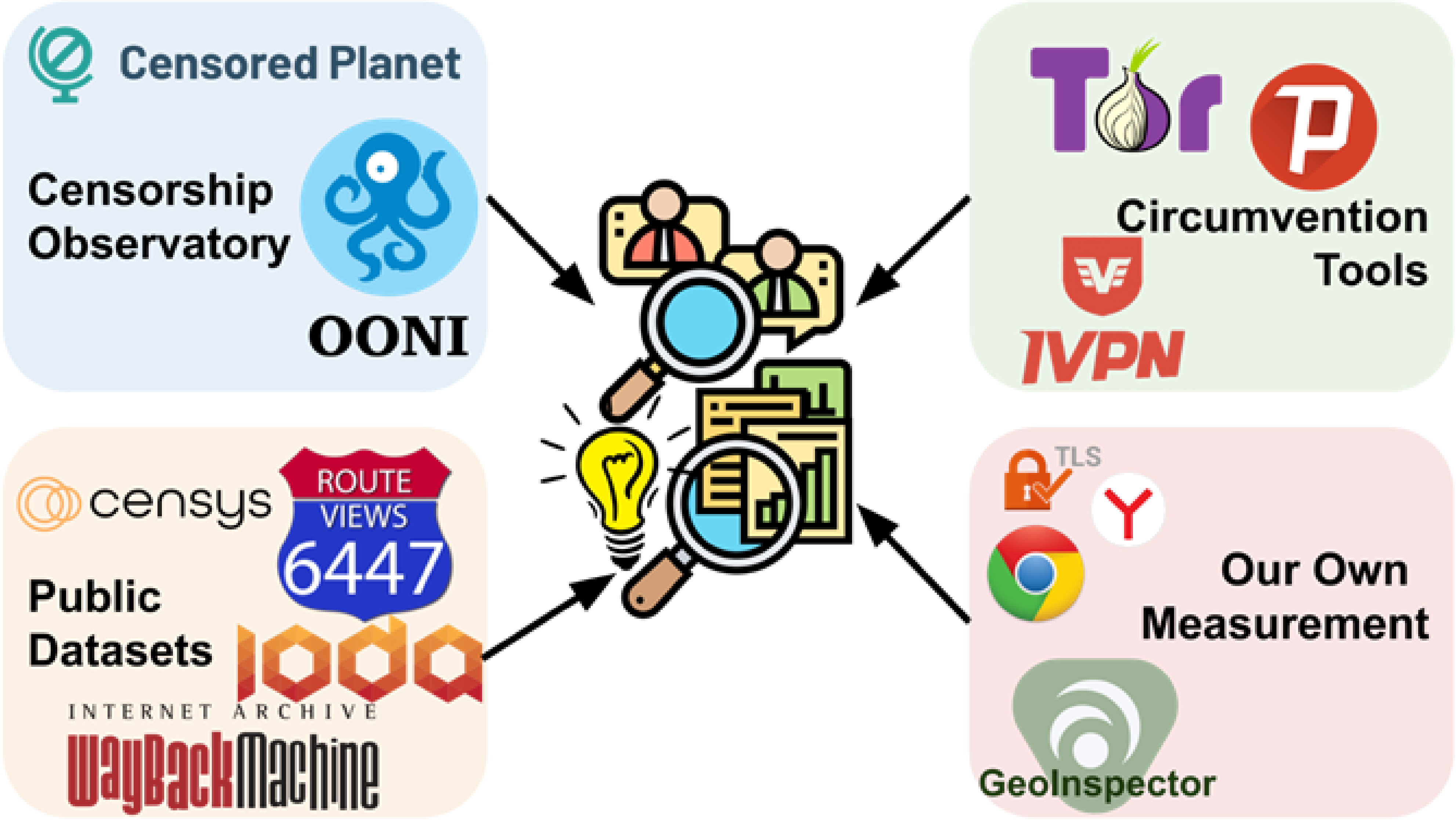
- Comprehensive blocking of Tor caused users to use obfuscation protocols. 15 “default” **obfs4 bridges were blocked**.

- Non-default obsf4 bridges progressively discovered and IP address blocked

- **meek and snowflake bridges** briefly blocked

- The **torproject.org website** was blocked from Dec 2021, until July 2022

Our Study



New measurement tools for:

- Measuring geoblocking (GeoInspector)
- Crawling domestic TLS certificates

Distributed measurements from:

- 4 VPs in Russia (residential and datacenter)
- 15 VPs in other countries

Data from 9 data sources:

- Censorship Data (Censored Planet, OONI)
- BGP withdrawals (Routeviews, IODA)
- Historical data (Censys, Internet Archive)
- Circumvention Tools (Tor, Psiphon, IVPN)

Our Study

A cautionary tale for Internet freedom:

- Highlights how nation-state censors *and* private Internet services may **isolate specific regions** from the support of the rest of the world.

- Encourages **multi-perspective study** on Internet freedom **beyond nation-state censorship** - private actors increasingly contribute to Internet splintering