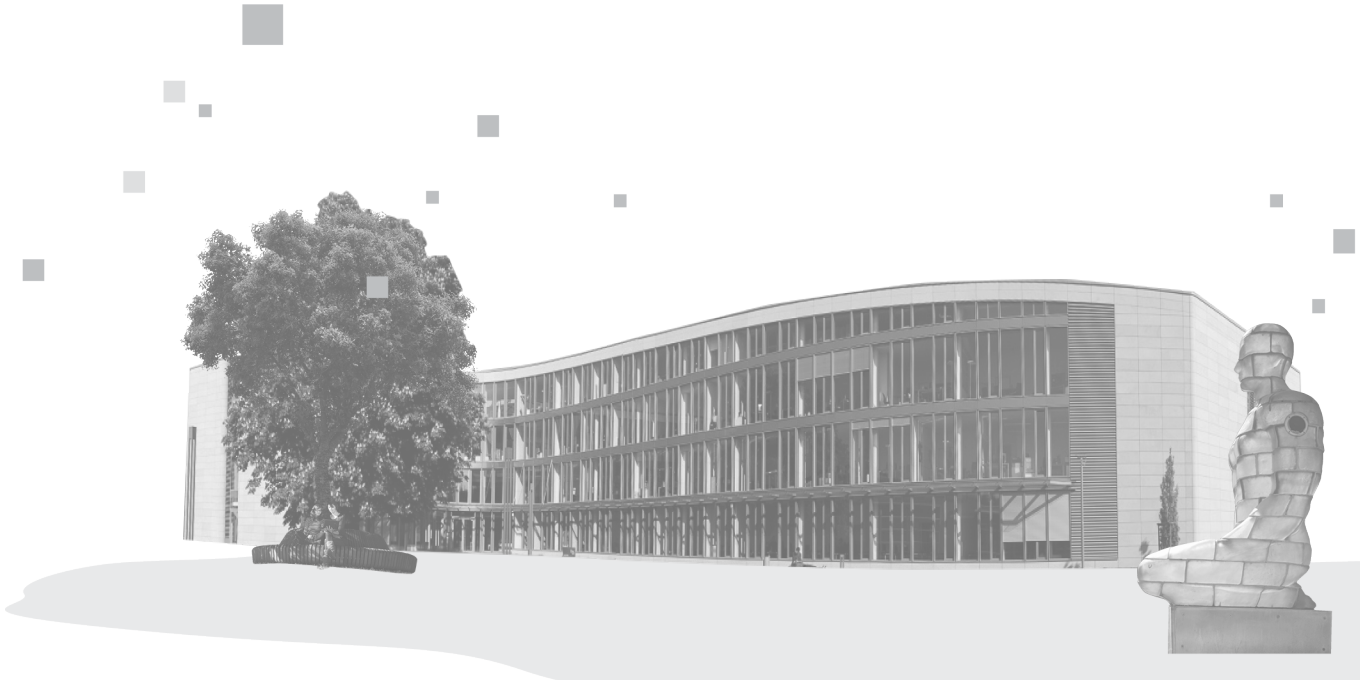
The WorldWideBlock Toolkit

Tracking Public Blocklists and Active Censorship Across 190 Countries

Jan Riedler

Vasilis Ververis

Vaibhav Bajpai



IFIP Networking 2026 | 26/05/2026

Motivation

Showcasing recent and ongoing censorship developments

Freedom on the Net Report 2025

Key Findings:

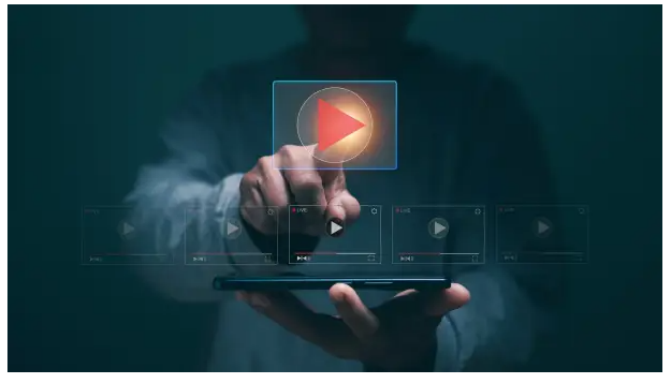
- Global Internet freedom declined for the 15th consecutive year
- Half of the 18 countries with an Internet freedom status of Free suffered score declines during the coverage period
- Control over online information has become an essential tool for authoritarian leaders seeking to entrench their regimes
- The immediate future of Internet freedom will depend on the ways in which governments deploy and regulate new technologies

https://freedomhouse.org/sites/default/files/2025-11/Freedom_on_the_Net_2025_Digital.pdf

Example | Italy's anti piracy shield

Cloudflare record fine: Italy's tough anti-piracy course hits DNS resolver

Due to refused network blocks, the Italian regulator Agcom is imposing a fine in the double-digit millions on the infrastructure giant Cloudflare.



(Image: krungchingpixs/Shutterstock)

Jan 10, 2026 at 9:18 pm CET 4 min. read

By Stefan Krempl

https://www.heise.de/en/news/Cloudflare-record-fine-Italy-s-tough-anti-piracy-course-hits-DNS-resolver-11136858.html

Research Questions

RQ 1: Which blocklists defined by network regulators are publicly accessible?

RQ 2: To what extent are domains blocked in practice?

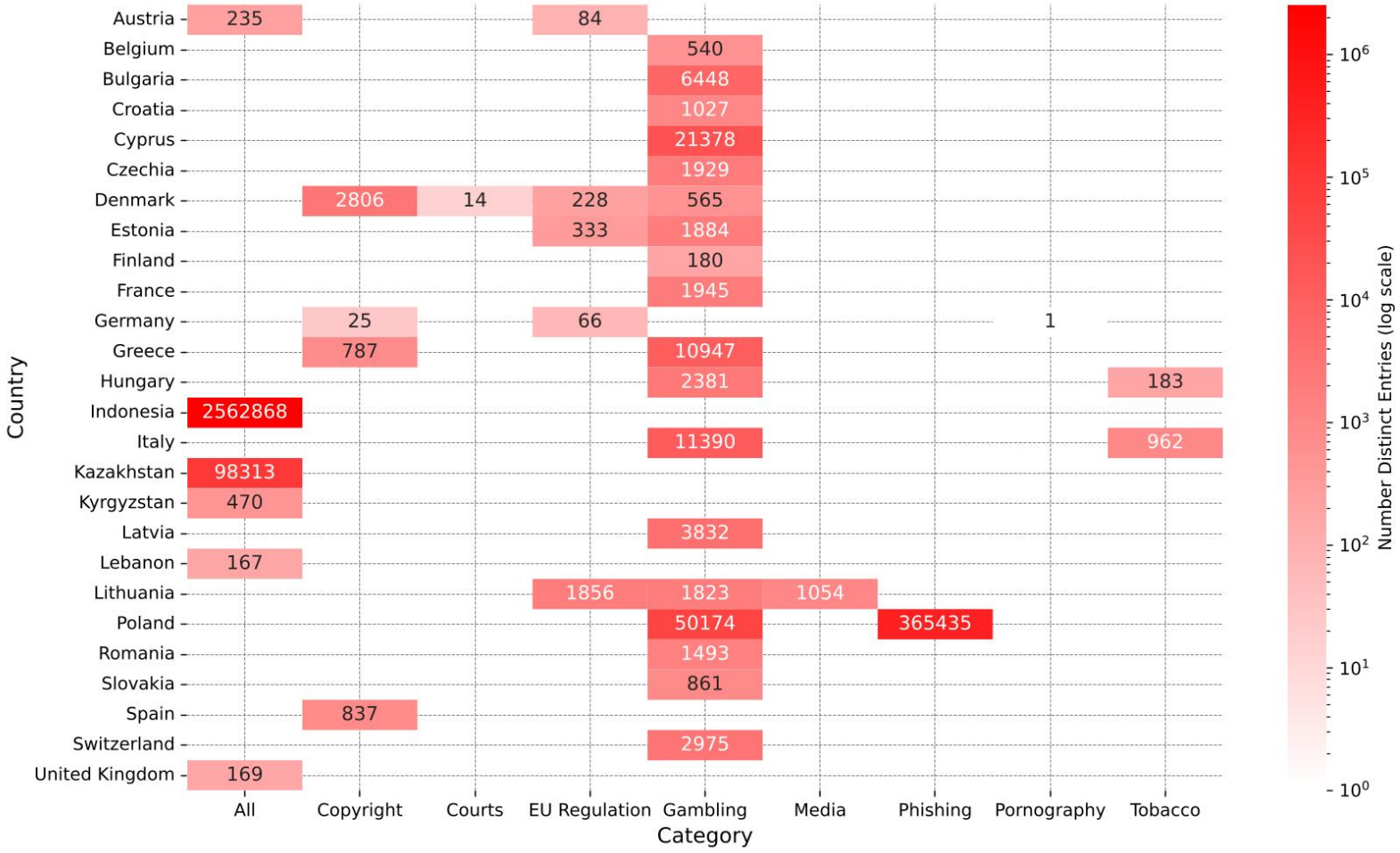
RQ 3: What techniques are currently implemented by network operators to enforce blocklists?

Paper contributions

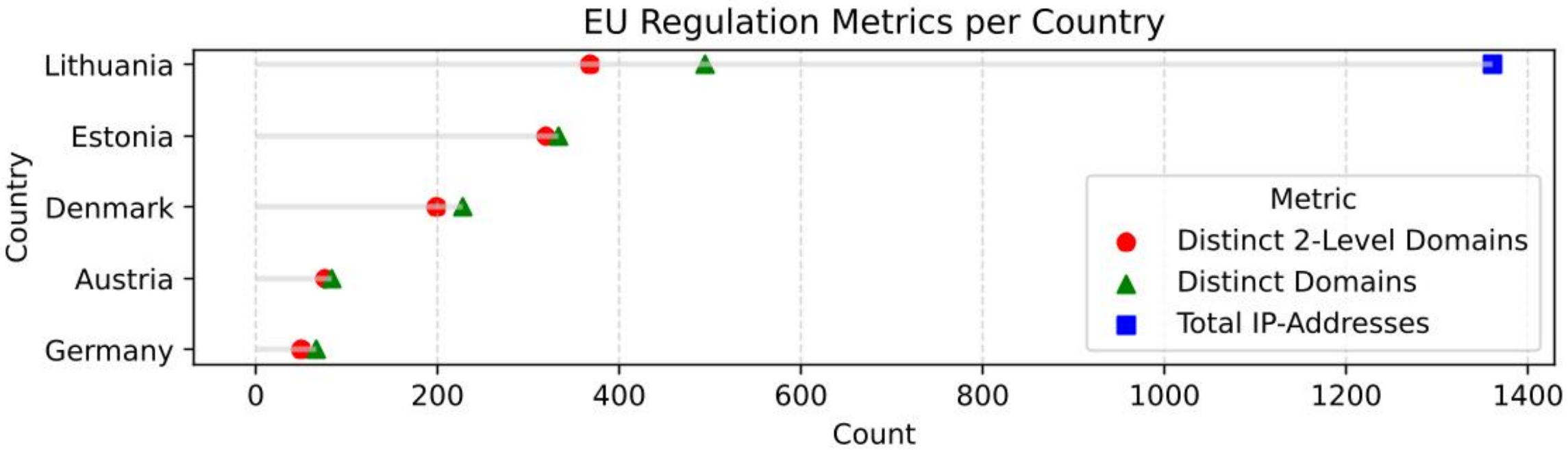
Presenting Core Contributions and Practical Implications

- **Global assessment of publicly available blocklists** covering 192 countries
- **Validate at Scale**:
  Perform >500 million measurements to verify over 20 million OONI anomalies, increasing reliability of detection
- **Introduce Novel Measurement Methods**:
  Design rVPmt and rDNSmt to improve censorship attribution and differentiate ISP-level blocking from measurement artefacts
- **Identify Blocking Techniques**:
  Show that DNS-based blocking is nearly universal, while advanced methods (e.g., SNI and HTTP Host header interception) are selectively applied
- **Map Global Censorship Practices**:
  Compile a comprehensive blocklist dataset across ~190 countries to systematically analyze enforcement strategies
- **Develop WorldWideBlock**:
  Build an automated, open-source platform that crawls 40 official government and ISP blocklists, enabling continuous monitoring and public visualization of global censorship

RQ 1: Which blocklists defined by network regulators are publicly accessible?



RQ 1: Which blocklists defined by network regulators are publicly accessible?



Internet Interference Measurement Platforms

- Open Observatory of Network Interference (**OONI**)
  - Based on volunteers running the measurements
  - 27,000 different domains

Internet Interference Measurement Platforms

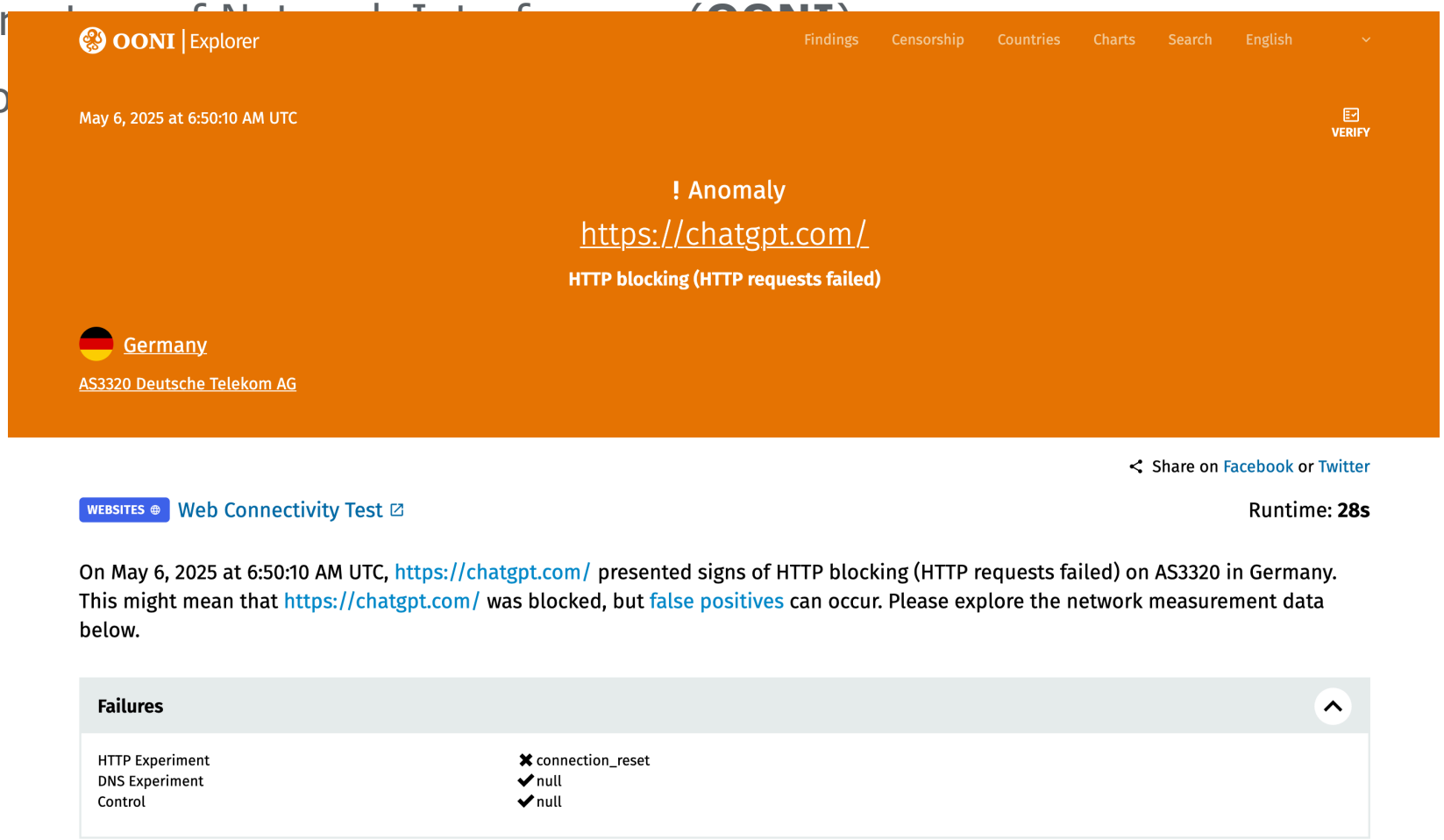
- Open Observatory of Network Interference (**OONI**)
  - Based on volunteers running the measurements
  - 27,000 different domains

Internet Interference Measurement Platforms

- Open Observatory of Network Interference (**OONI**)
  - Based on volunteers running the measurements
  - 27,000 different domains

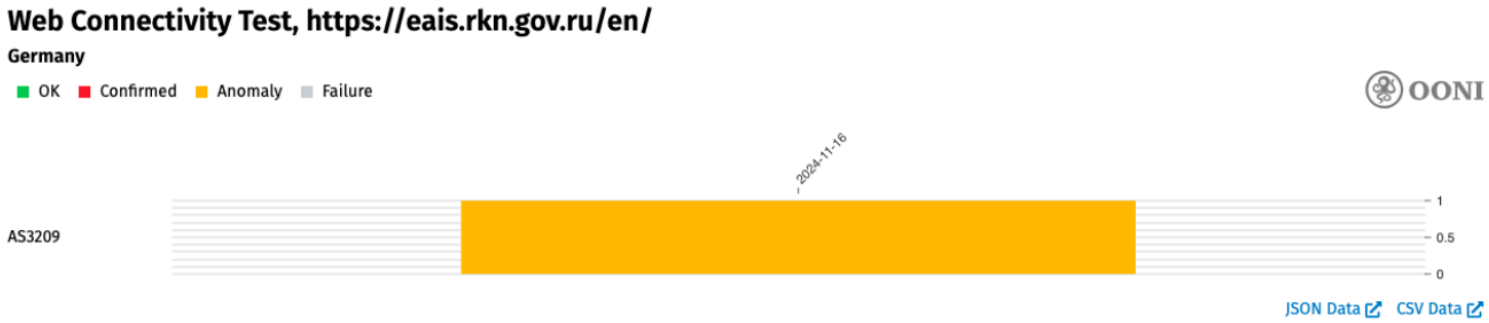
Internet Interference Measurement Platforms

- Open Obser
  - Based o
  - 27,000



Internet Interference Measurement Platforms

- Open Observatory of Network Interference (**OONI**)
  - Based on volunteers running the measurements
  - 27,000 different domains

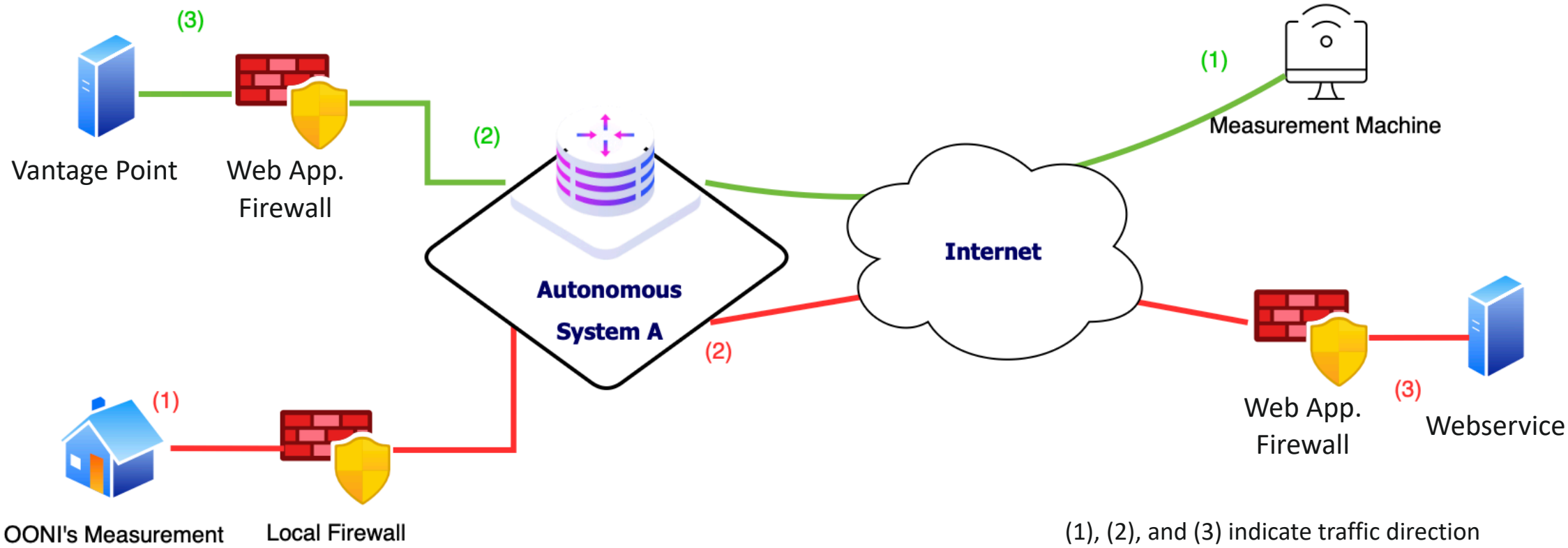


Internet Interference Measurement Platforms

- Open Observatory of Network Interference (**OONI**)
  - Based on volunteers running the measurements
  - 27,000 different domains
- Censored Planet
  - Remote measurement techniques
  - Closed source
  - 2,000 domains of Alexa’s Top List

Methodology

Validating blocked OONI Measurements (non-DNS)



(1), (2), and (3) indicate traffic direction
Green: rVPmt measurement architecture
Red: OONI anomaly measurement architecture

rDNSmt

1. DNS query for control domain (reachable test)

Measurement Machine

Test Resolver

Control Resolver

rDNSmt

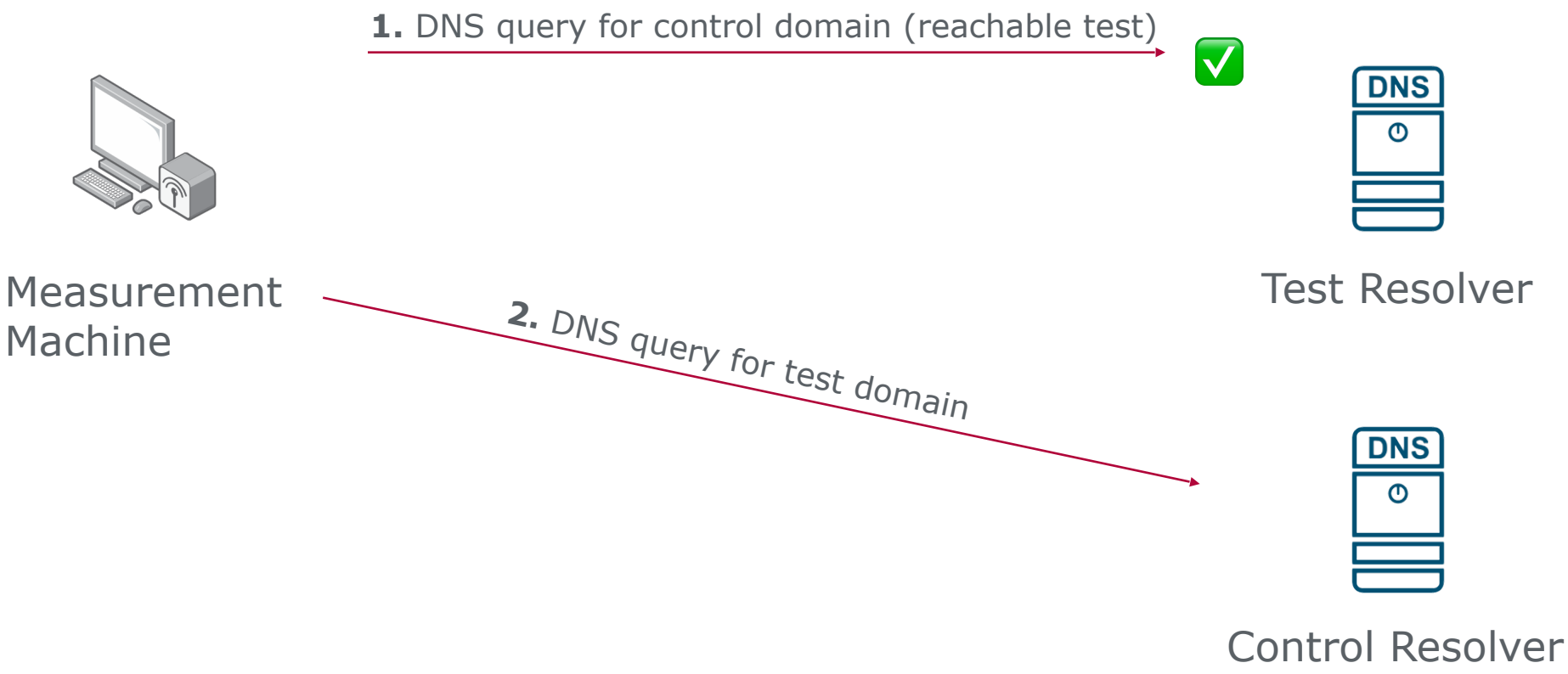
1. DNS query for control domain (reachable test)

Measurement Machine

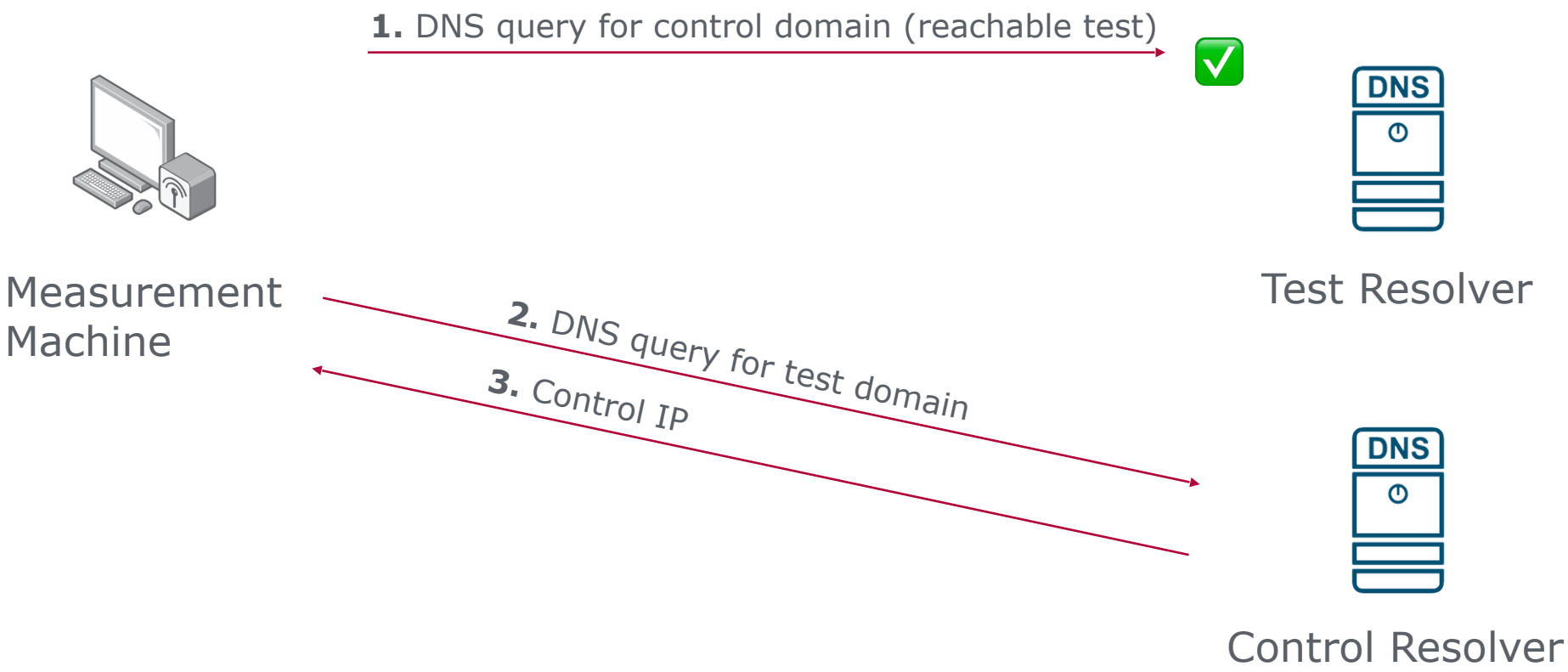
Test Resolver

Control Resolver

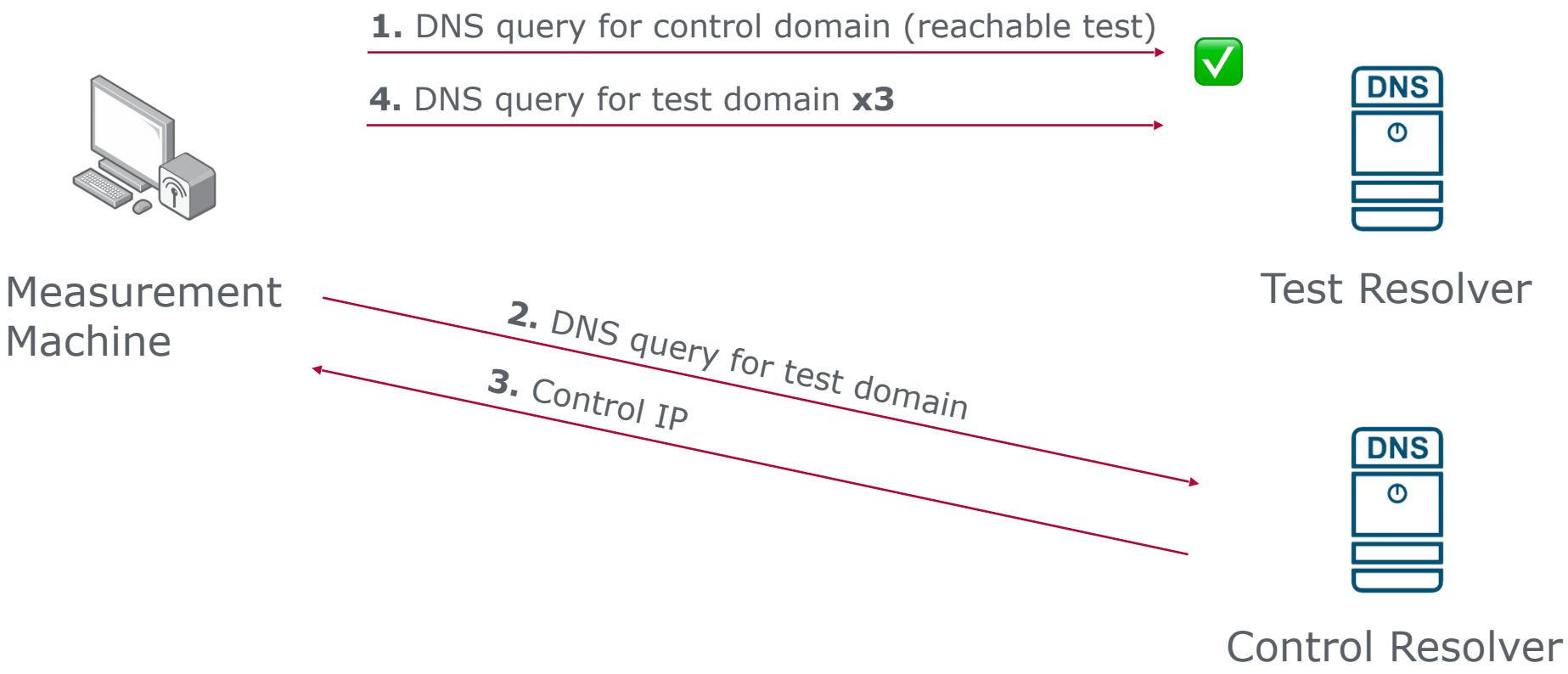
rDNSmt


1. DNS query for control domain (reachable test)
DNS
Test Resolver
Measurement Machine
2. DNS query for test domain
DNS
Control Resolver

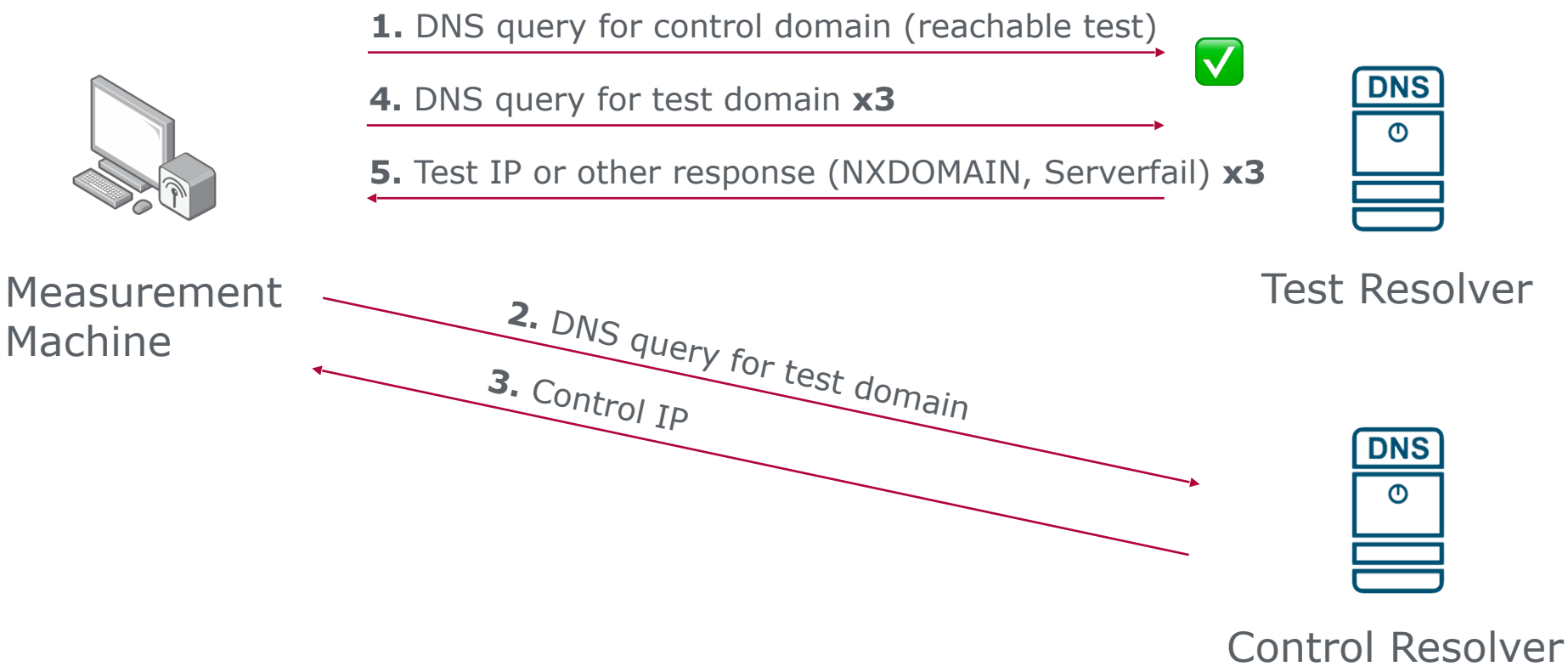
rDNSmt


1. DNS query for control domain (reachable test)
DNS
Test Resolver
Measurement Machine
2. DNS query for test domain
3. Control IP
DNS
Control Resolver

rDNSmt


1. DNS query for control domain (reachable test)
4. DNS query for test domain x3
DNS
Test Resolver
Measurement Machine
2. DNS query for test domain
3. Control IP
DNS
Control Resolver

rDNSmt


1. DNS query for control domain (reachable test)
4. DNS query for test domain x3
5. Test IP or other response (NXDOMAIN, Serverfail) x3
DNS
Test Resolver
Measurement Machine
2. DNS query for test domain
3. Control IP
DNS
Control Resolver

rDNSmt

Measurement Machine

1. DNS query for control domain (reachable test) ✅

4. DNS query for test domain **x3**

5. Test IP or other response (NXDOMAIN, Serverfail) **x3**

Test Resolver

2. DNS query for test domain

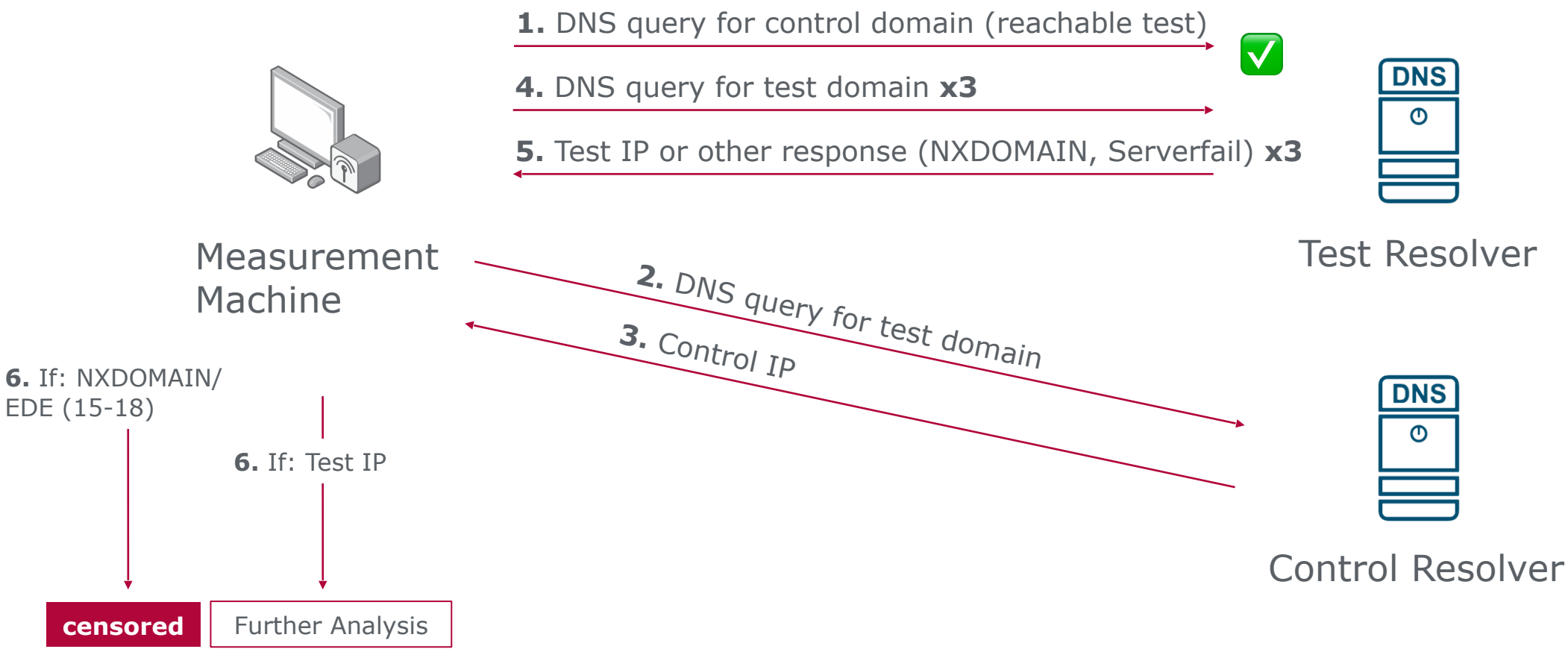
3. Control IP

Control Resolver

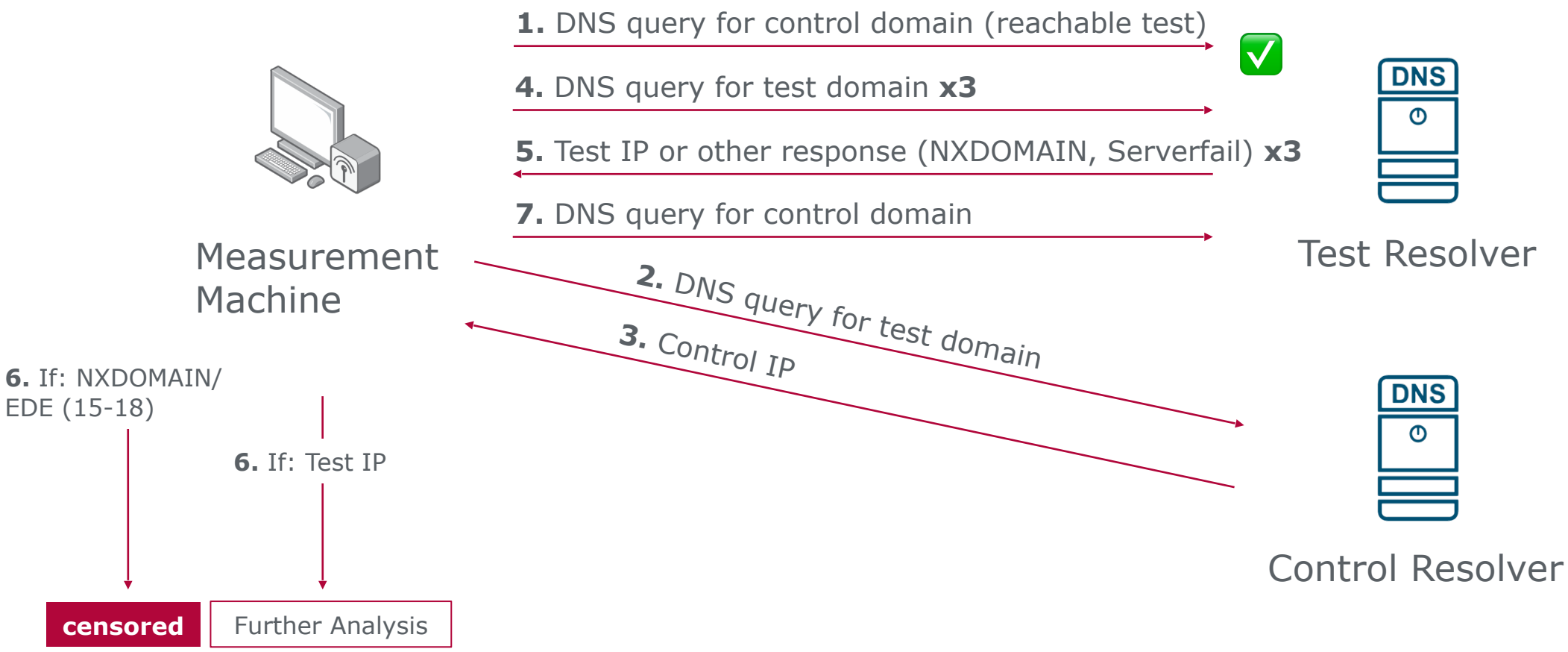
6. If: NXDOMAIN/ EDE (15-18)

censored

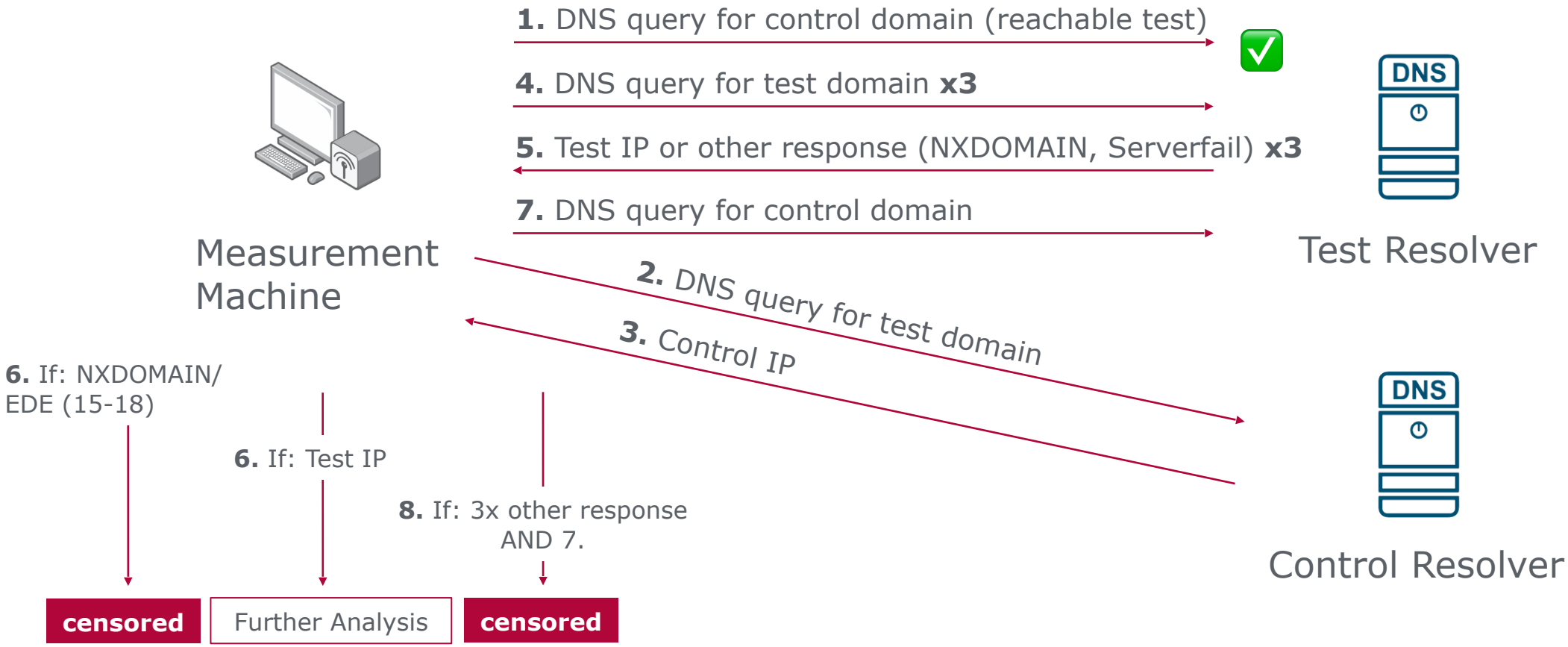
rDNSmt


1. DNS query for control domain (reachable test)
4. DNS query for test domain x3
5. Test IP or other response (NXDOMAIN, Serverfail) x3
Measurement Machine
Test Resolver
2. DNS query for test domain
3. Control IP
Control Resolver
6. If: NXDOMAIN/ EDE (15-18)
6. If: Test IP
censored
Further Analysis

rDNSmt


1. DNS query for control domain (reachable test)
4. DNS query for test domain x3
5. Test IP or other response (NXDOMAIN, Serverfail) x3
7. DNS query for control domain
2. DNS query for test domain
3. Control IP
Measurement Machine
Test Resolver
Control Resolver
DNS
DNS
6. If: NXDOMAIN/ EDE (15-18)
6. If: Test IP
censored
Further Analysis

rDNSmt


1. DNS query for control domain (reachable test)
4. DNS query for test domain x3
5. Test IP or other response (NXDOMAIN, Serverfail) x3
7. DNS query for control domain
Measurement Machine
Test Resolver
2. DNS query for test domain
3. Control IP
Control Resolver
6. If: NXDOMAIN/ EDE (15-18)
6. If: Test IP
8. If: 3x other response AND 7.
censored
Further Analysis
censored

rDNSmt - Further Analysis

rDNSmt - Further Analysis

- Control IPs and Test IPs share at least one common address **not censored**

rDNSmt - Further Analysis

- Control IPs and Test IPs share at least one common address
- Test IPs are non-public

not censored

censored

rDNSmt - Further Analysis

- Control IPs and Test IPs share at least one common address
- Test IPs are non-public

not censored

censored

IP Range	Version	Purpose
10.0.0.0/8	IPv4	Private network
172.16.0.0/12	IPv4	Private network
192.168.0.0/16	IPv4	Private network
127.0.0.0/8	IPv4	Loopback addresses
0.0.0.0	IPv4	Unspecified address
169.254.0.0/16	IPv4	Link-local addresses
100.64.0.0/10	IPv4	Carrier-grade NAT (CGNAT)
fc00::/7	IPv6	Unique Local Address (ULA)

rDNSmt - Further Analysis

- Control IPs and Test IPs share at least one common address
- Test IPs are non-public
- Invalid TLS certificates of the Test-IPs and different compared to the certificates of the Control-IPs

not censored

censored

Blockpage

rDNSmt - Further Analysis

- Control IPs and Test IPs share at least one common address — **not censored**
- Test IPs are non-public — **censored**
- Invalid TLS certificates of the Test-IPs and different compared to the certificates of the Control-IPs — **Blockpage**
- No TLS certificates of the Test-IPs but IPs are reachable (Port 80) — **Blockpage**

rDNSmt - Further Analysis

- Control IPs and Test IPs share at least one common address — **not censored**
- Test IPs are non-public — **censored**
- Invalid TLS certificates of the Test-IPs and different compared to the certificates of the Control-IPs — **Blockpage**
- No TLS certificates of the Test-IPs but IPs are reachable (Port 80) — **Blockpage**

Validation using CensoredPlanets Blockpage Patterns

rDNSmt - Further Analysis

- Control IPs and Test IPs share at least one common address — **not censored**
- Test IPs are non-public — **censored**
- Invalid TLS certificates of the Test-IPs and different compared to the certificates of the Control-IPs — **Blockpage**
- No TLS certificates of the Test-IPs but IPs are reachable (Port 80) — **Blockpage**

Validation using CensoredPlanets Blockpage Patterns

rDNSmt - Further Analysis

- Control IPs and Test IPs share at least one common address — **not censored**
- Test IPs are non-public — **censored**
- Invalid TLS certificates of the Test-IPs and different compared to the certificates of the Control-IPs — **Blockpage**
- No TLS certificates of the Test-IPs but IPs are reachable (Port 80) — **Blockpage**

Validation using CensoredPlanets Blockpage Patterns

rDNSmt

1. DNS query for control domain (reachable test)

Measurement Machine

Test Resolver

rDNSmt

Measurement Machine

1. DNS query for control domain (reachable test)

Test Resolver

rDNSmt

Measurement Machine

1. DNS query for control domain (reachable test)

2. DNS query for test domain (DNS Poisoning)

X

Test Resolver

rDNSmt

Measurement Machine

1. DNS query for control domain (reachable test)

2. DNS query for test domain (DNS Poisoning)

3. Response that differs from **1.**?

X

Test Resolver

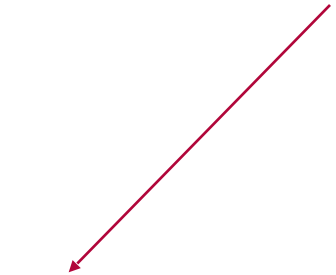
rDNSmt

Measurement Machine

1. DNS query for control domain (reachable test)

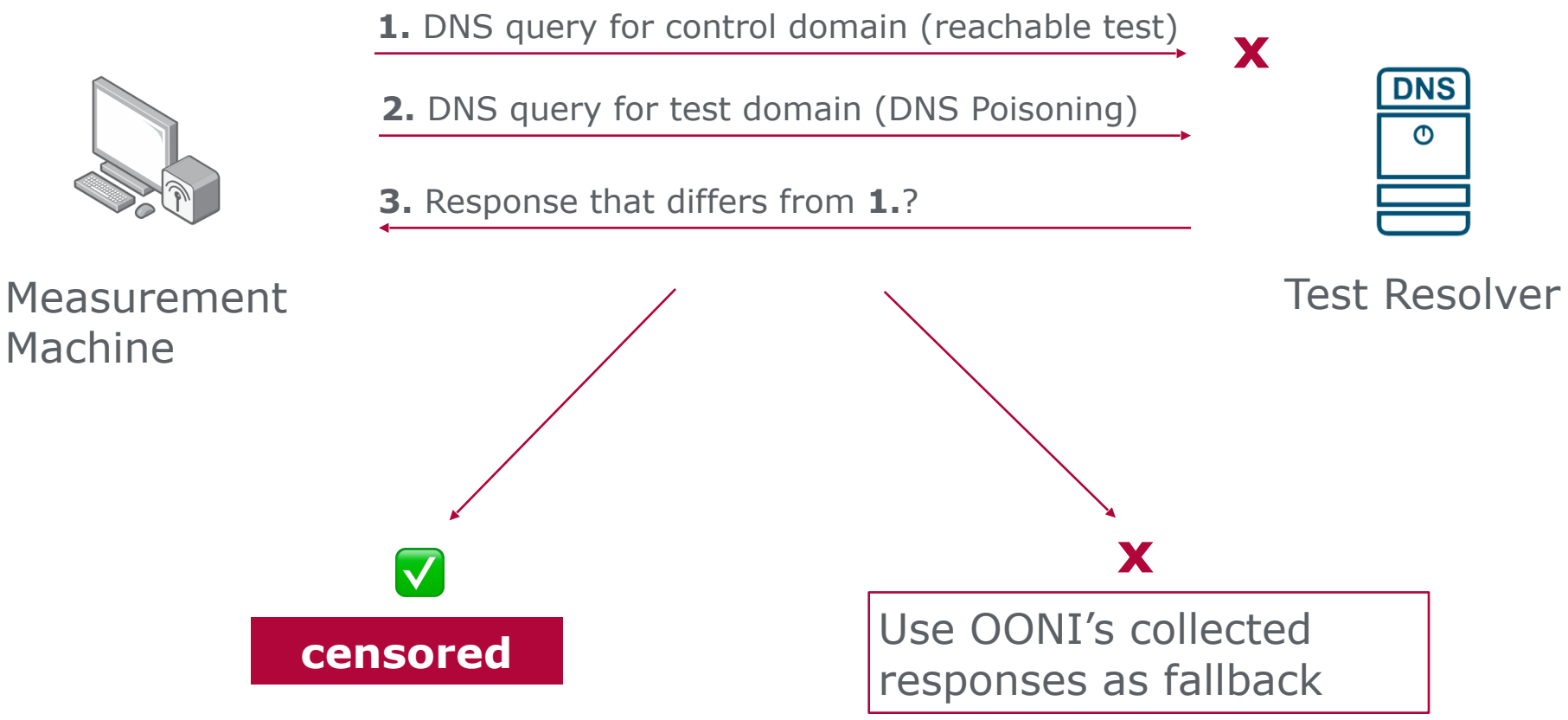
2. DNS query for test domain (DNS Poisoning)

3. Response that differs from **1.**?

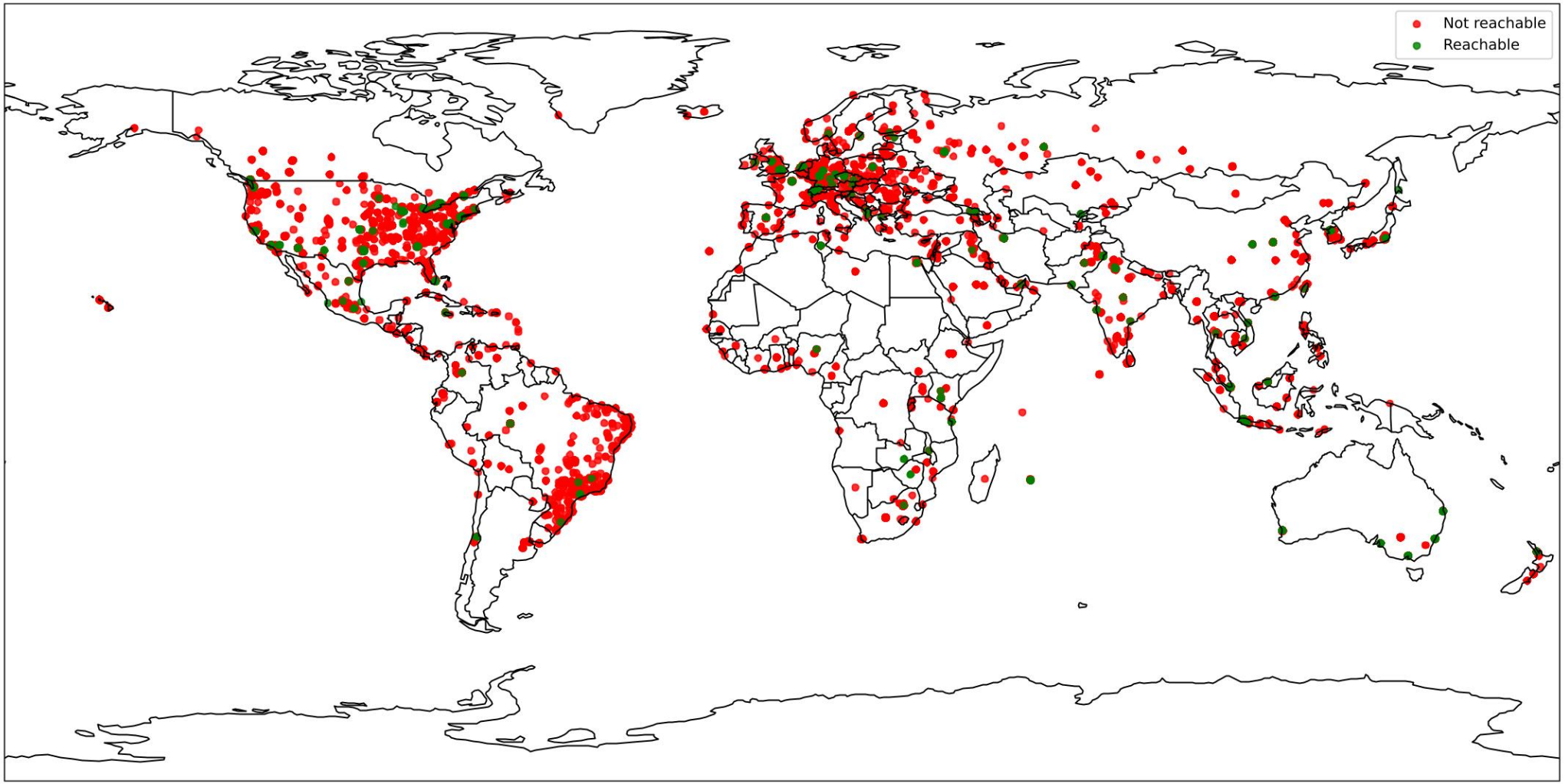


Test Resolver

rDNSmt


1. DNS query for control domain (reachable test)
2. DNS query for test domain (DNS Poisoning)
3. Response that differs from 1.?
DNS
Measurement Machine
Test Resolver
censored
Use OONI's collected responses as fallback

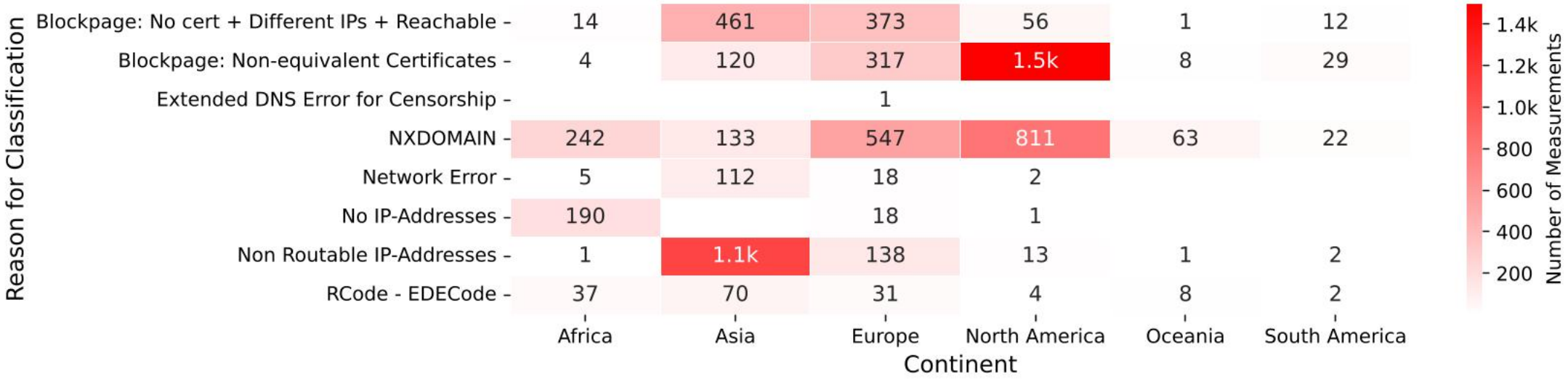
rDNSmt – Geographic Distribution of DNS Resolvers



rDNSmt – Classification Reasons for Censored Measurements

RQ 2: To what extent are domains blocked in practice?

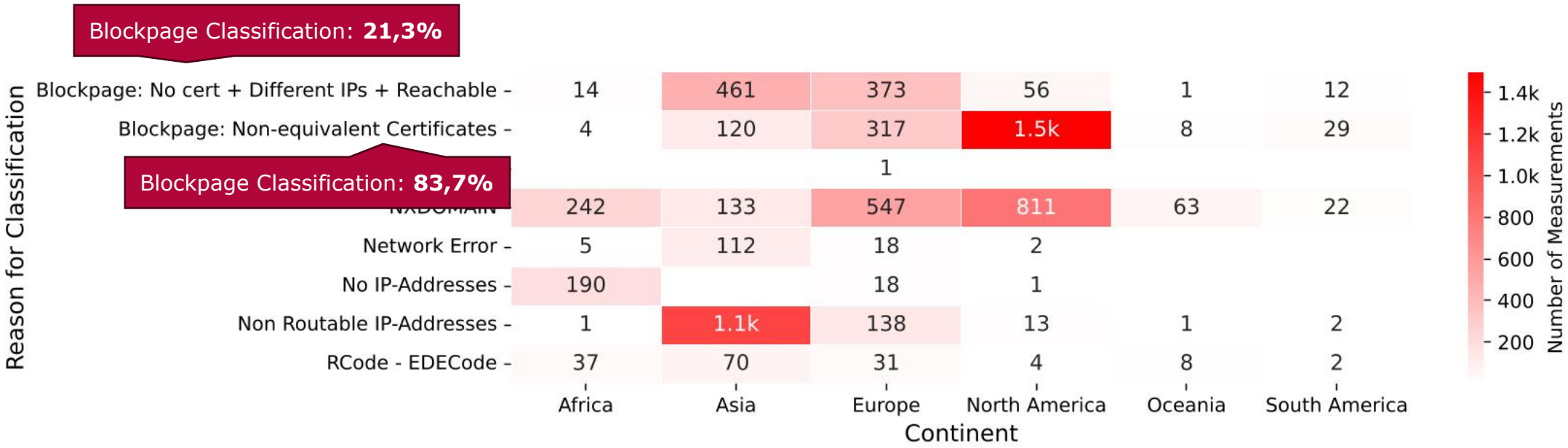
RQ 3: What techniques are currently implemented … to enforce blocklists?



rDNSmt – Classification Reasons for Censored Measurements

RQ 2: To what extent are domains blocked in practice?

RQ 3: What techniques are currently implemented … to enforce blocklists?



DNS Poisoned Requests to Unreachable DNS Resolvers

RQ 2: To what extent are domains blocked in practice?

RQ 3: What techniques are currently implemented … to enforce blocklists?

Country	Number of Blocked Domains
China	1,452
Iran	4,337

OONI Errors Resulting in DNS Anomalies

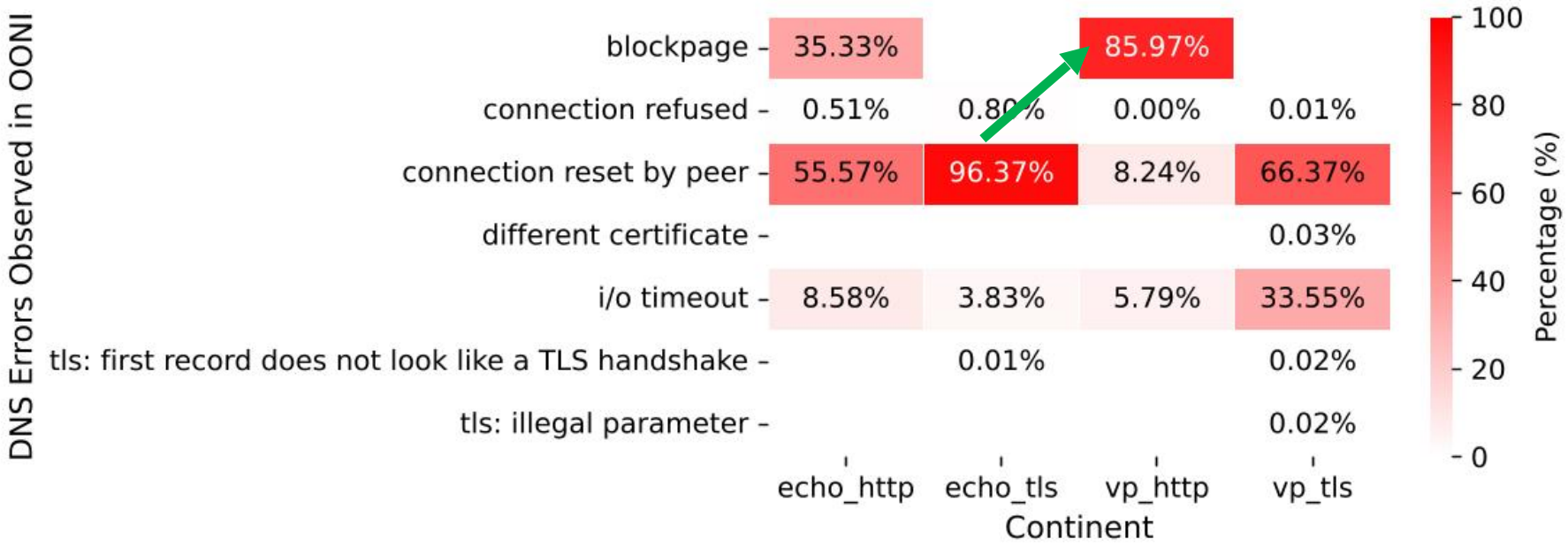
RQ 2: To what extent are domains blocked in practice?

RQ 3: What techniques are currently implemented … to enforce blocklists?

rVPmt – Vantage Point Overview

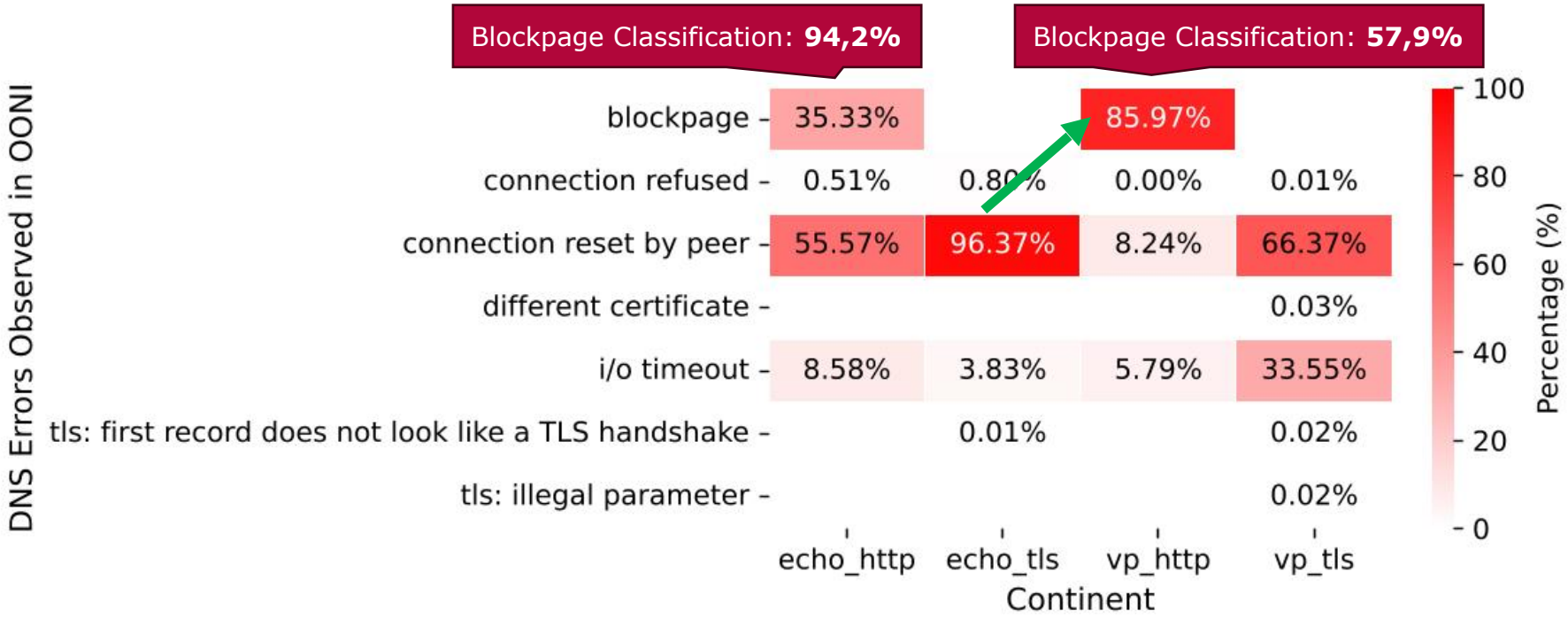
rVPmt – Classification Reasons for Censored Measurements

RQ 3: What techniques are currently implemented … to enforce blocklists?



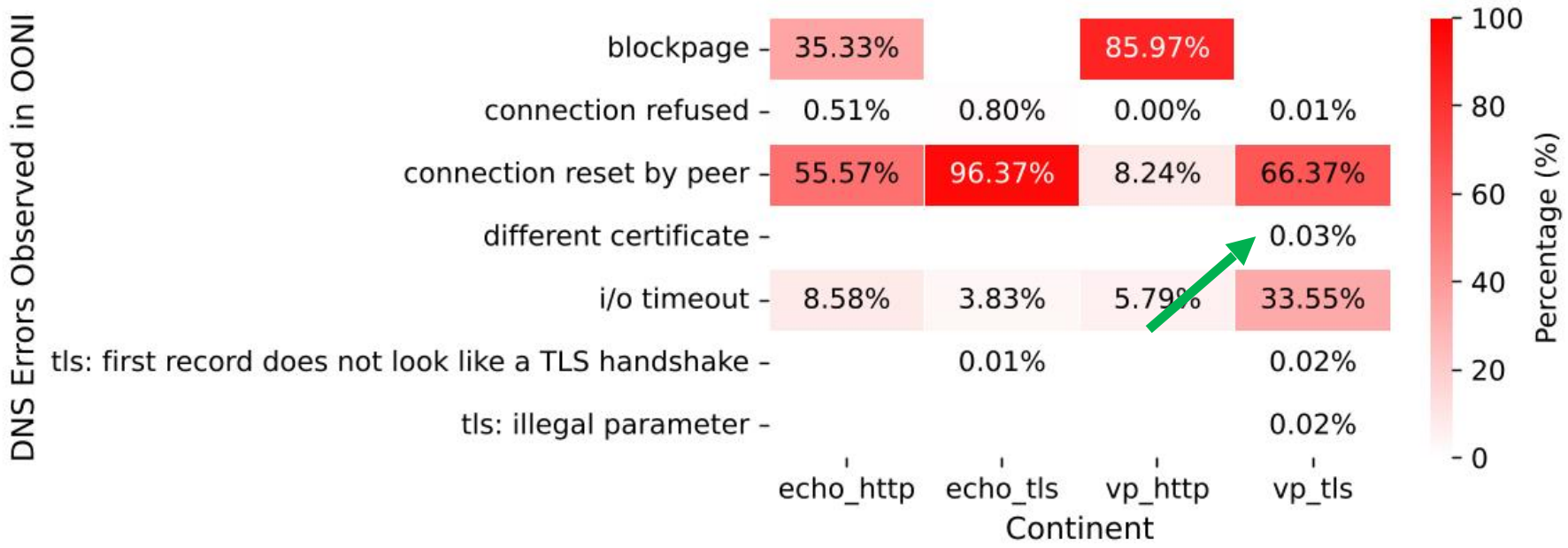
rVPmt – Classification Reasons for Censored Measurements

RQ 3: What techniques are currently implemented … to enforce blocklists?



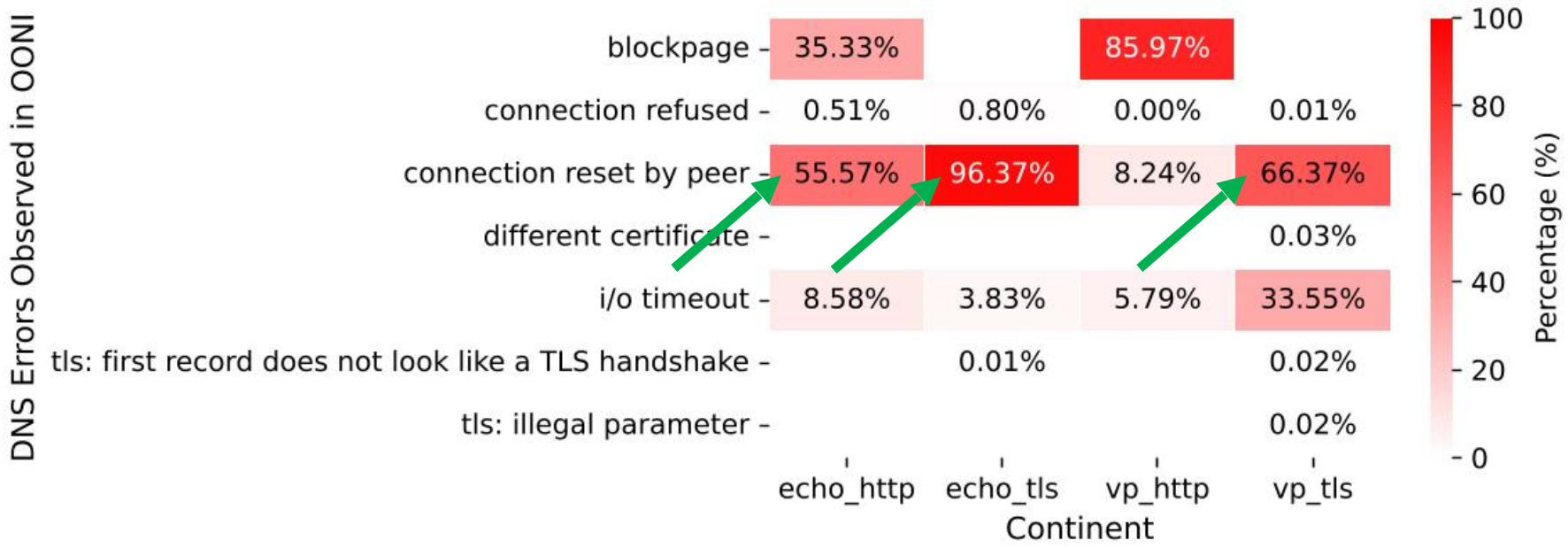
rVPmt – Classification Reasons for Censored Measurements

RQ 3: What techniques are currently implemented … to enforce blocklists?



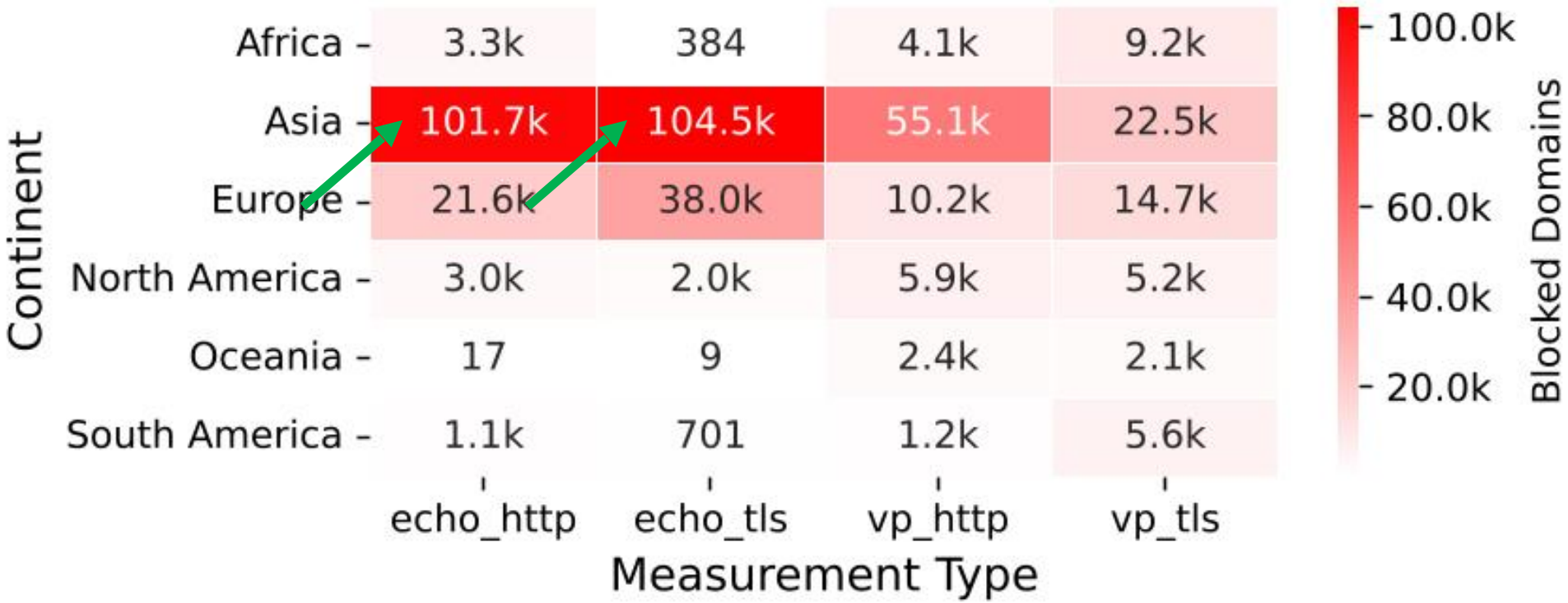
rVPmt – Classification Reasons for Censored Measurements

RQ 3: What techniques are currently implemented … to enforce blocklists?



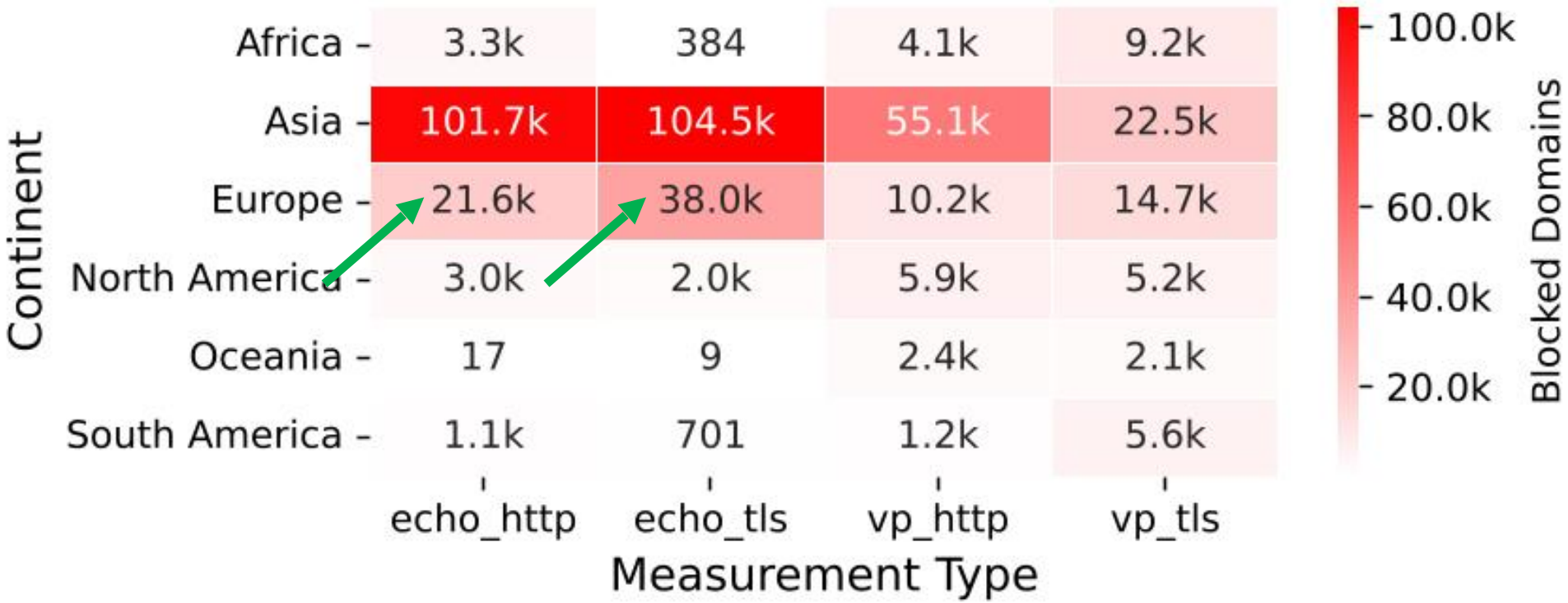
rVPmt – Distinct Blocked Domains per Continent

RQ 2: To what extent are domains blocked in practice?



rVPmt – Distinct Blocked Domains per Continent

RQ 2: To what extent are domains blocked in practice?



The WorldWideBlock Toolkit: Tracking Public Blocklists and Active Censorship Across 190 Countries

Key Takeaways:

- First global study of domain blocklists across 190 countries
- Confirms that many countries lack transparency in publicly disclosing blocklists
- New remote measurement methods, rVPmt and rDNSmt, were introduced to improve the accuracy of censorship attribution
- DNS-based techniques were the primary blocking method, using NXDOMAIN responses, unroutable IP addresses, or redirects to block pages
- Active DNS poisoning could only be confirmed in China and Iran
- Many countries block traffic based on the HTTP Host header or SNI, typically by injecting TCP RST packets or redirecting users to block pages

Interested in a PhD position?

Have a look at our website or come and chat with us!

https://hpi.de/bajpai

janriedler/worldwideblock