ICANN86 Policy Forum in Seville, Spain

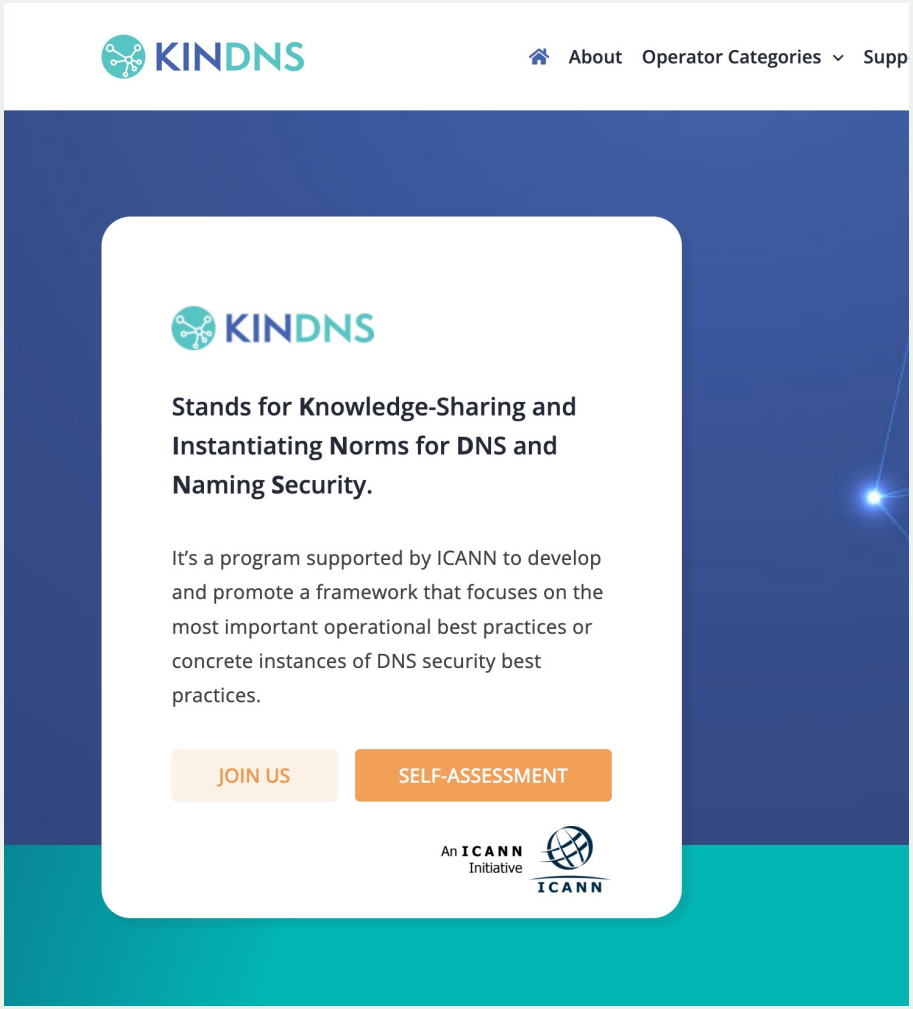
Evidence-based DNS Resilience

Amreesh Phokeer

Internet Society

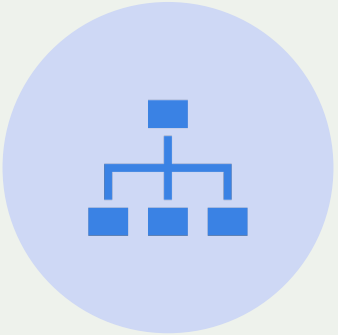
DNS Resilience

- Internet is increasingly hosting mission-critical applications and services
- Regulations such as NIS2 (EU) and CSF2 (US) to protect critical infrastructures
- We use the KINDNS framework to evaluate the measurable practices of DNS Resilience (both authorative and recursive)



Resilience metrics

MEASURABLE VS NON-MEASURABLE PRACTICES



ORGANIZATIONAL PROCESSES ARE USUALLY NOT MEASURABLE

FOCUS ON OBSERVABLE CHARACTERISTICS

Authoritative DNS Resilience

KINDNS Measurable practices

Authoritative Server operators	TLDs, SLDs and Critical Zones
Practice 1 – DNSSEC and Key management	Covered
Practice 2 – Limited zone transfer	Covered
Practice 4 – Authoritative and recursive on different servers	Covered
Practice 5 – Two distinct name servers	Covered
Practice 6 – • Software diversity 🚫 • Network diversity ✅ • Geographic Diversity ✅	Partly

Different measures for different threats

Metric	Resilience against	Dataset
# auth. NSes	node failures	active scans [5]
# IP addr. of auth Nses	node failures	active scans [5]
# of ASes of NS IP addr.	routing issues	PFX2AS [6]
# of anycast addresses	site failures, DDoS	MAnycast2 [4], IPInfo [7]
# of TLDs of NS names	NS parent zone failures	active scans [5]
# of server locations	site failures, geofencing	IPInfo Location [7]

[4] Sommese et al., "MAnycast2: Using Anycast to Measure Anycast", IMC, *2020*

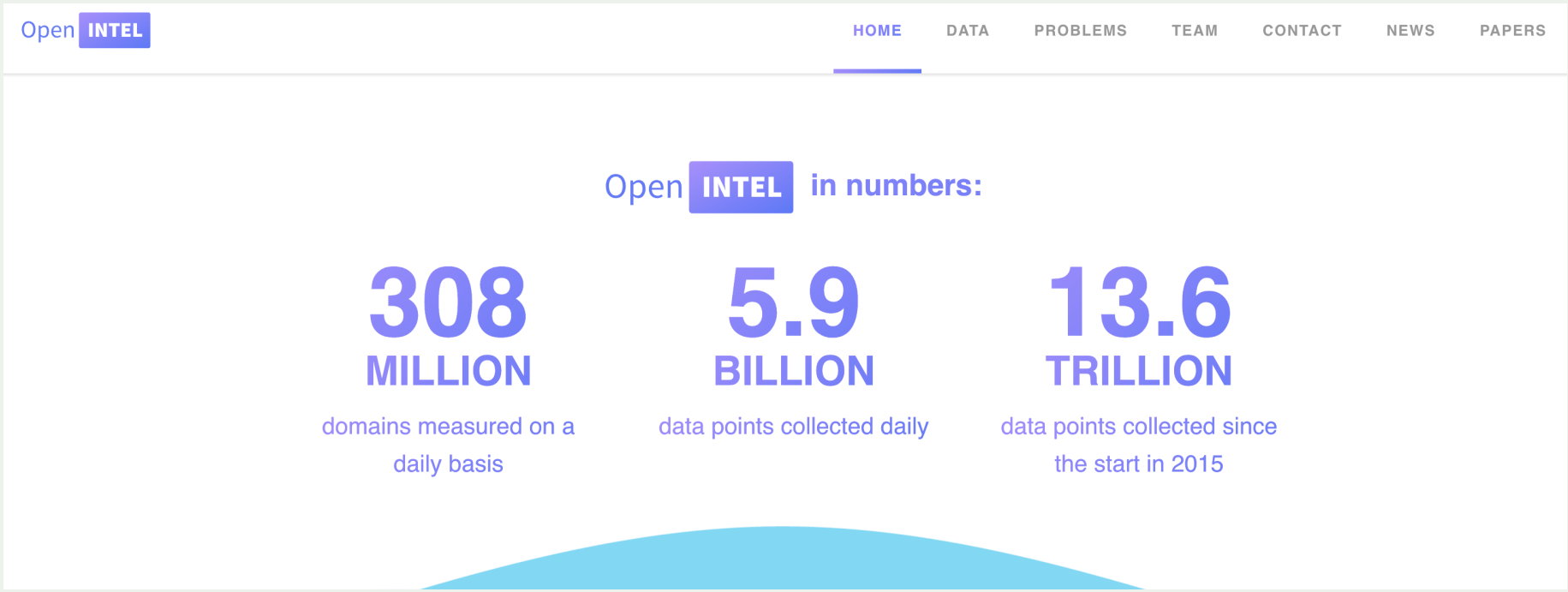
[5] Steurer et al., "A Tree in a Tree: Measuring Biases of Partial DNS Tree Exploration ", PAM, *2025*

[6] CAIDA UCSD, RouteViews prefix2as dataset. https://www.caida.org/catalog/datasets/routeviews-prefix2as/, 2008

[7] IPInfo, *Trusted IP Data Provider from IPv6 to IPv4. https://ipinfo.io, 2025*

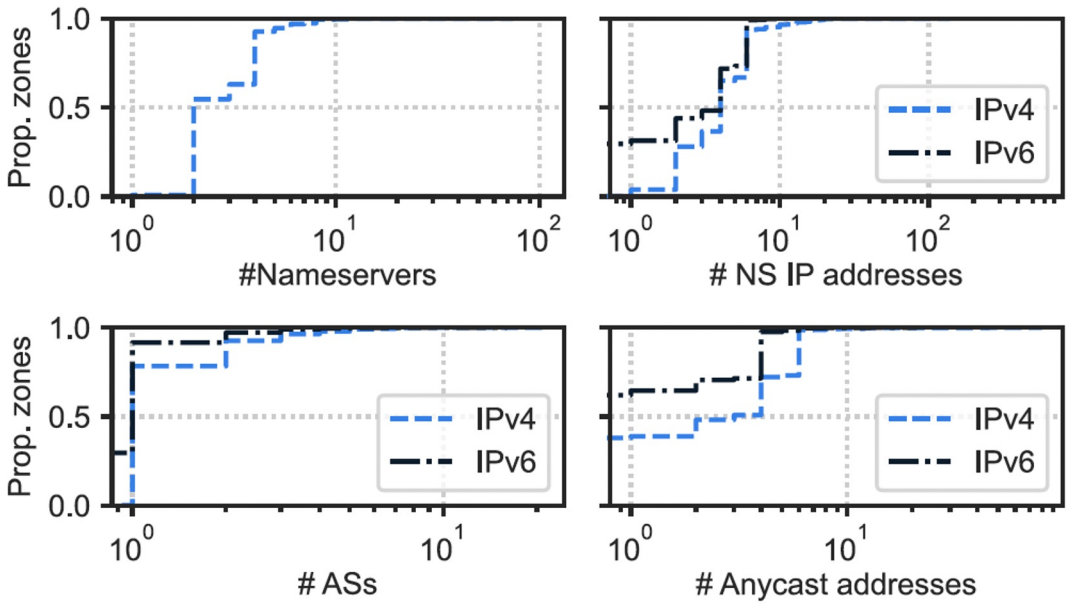
Data Collection

- ct: Names from unexpired certificates from Certificate Transparency logs: Argon, Xenon, Oak, Sectico Sabre, CloudFlare Nimbus, DigiCert Nessie, DigiCert Yeti, and TrustAsia.
- zf: Zone files from ICANN's Centralized Zone Data Service (CZDS) and available TLDs (.se, .nu, .ee, .ch, and .li).
- opendata: Names from the open-data efforts of AFNIC [2] and SK-NIC.
- Top-lists: Names from the corresponding domain top-list such as tranco, majestic, radar, umbrella:

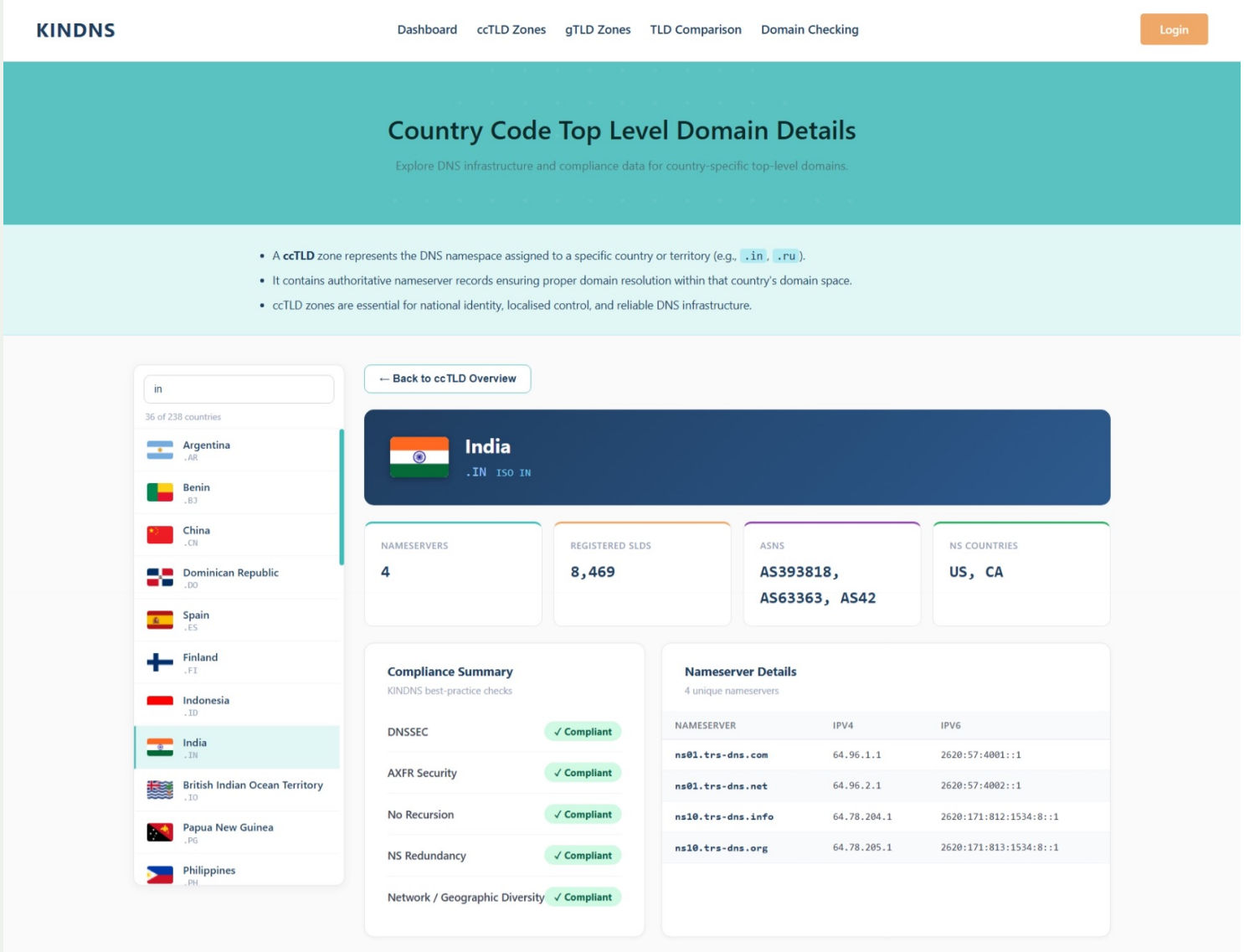

Open INTEL
HOME
DATA
PROBLEMS
TEAM
CONTACT
NEWS
PAPERS
Open INTEL in numbers:
308
MILLION
domains measured on a daily basis
5.9
BILLION
data points collected daily
13.6
TRILLION
data points collected since the start in 2015

Direct metrics

- Resilience metrics for the Tranco Top 1M domains [2]
- IPv6 deployments include fewer addresses, ASes, and rely less on anycast



Dashboard (Work in Progress)



Recursive Resolver Resilience

DNS Resilience Evaluation System Features

Feature	Implementation	Requirements	Related Work
BCP38 compliant	fetch public data	Fetching public data	
QMIN	resolver scans with zmap or cusom go tool	Nameserver, scan server, wild-card queries, list of resolver for testing	A Second Look at DNS QNAME Minimization
MANRS compliant	Is network part of route leaks/hijacks? ROV? RPKI?	(note: distance to affected networks)	Measuring MANRS ecosystem GRIP (georgia tech) ROVISTA, geoff huston
Software diversity	SNMP, dig, fpdns2		
Allow DNS traffic only	port scan of selected ports/services	Scan server (22,23,25,80,110,143,...) → use a list of 10-20 ports (have proxying in mind)	
DNSSEC validation		Setup DNSSEC signed domain + NS with “tampered” records	Geoff Huston’s DNSSEC measurements

DNS Resilience Evaluation System Features

Feature	Implementation	Requirements	Related Work
Geographical diversity			
Topological diversity	Measuring inside networks? Hard to measure	what are good patterns for running reliable rec. DNS server that are also measurable (probably out of scope for this work)	
Caching best practices	Query popular domain names → TTL values Instrument max. caching time?		Open Intel data
Anycast	https://github.com/ut-dacs/anycast-census and manycast.net		LACeS: An Open, Fast, Responsible, and Efficient Longitudinal Anycast Census System
Consolidation effect	Open DNS API data		

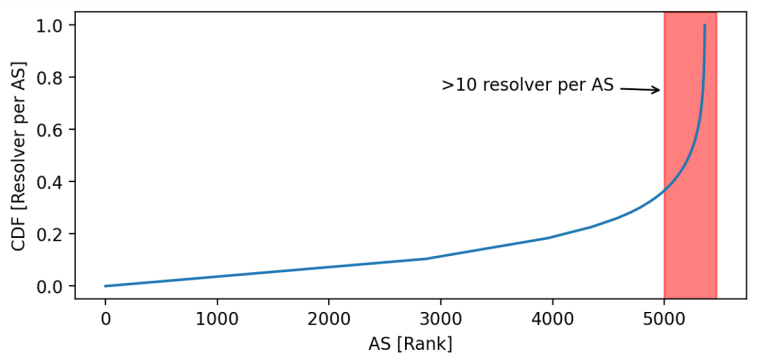
DNS Resilience Evaluation System
Data sources

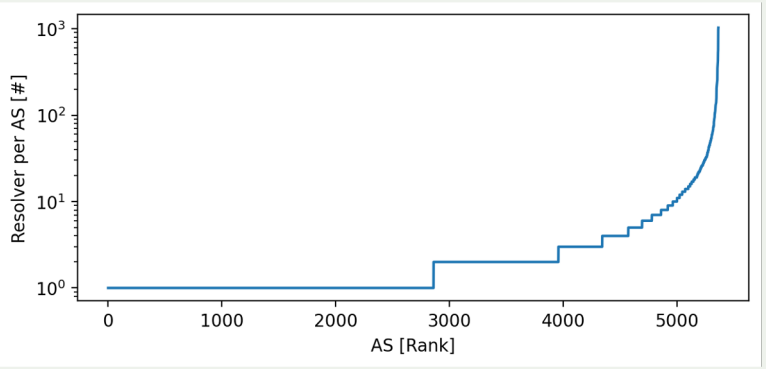
Data source	Public?	Update interval	Content	Link
Open DNS API	✓	Weekly updates	Open resolver and forwarder	https://odns-data.netd.cs.tu-dresden.de
CAIDA Spoofer	✓	Daily updates	AS and prefix list that allow for spoofing	https://api.spoofer.caida.org/
Open Intel data	✓	Daily updates	Domain names, real time zone feeds	https://openintel.nl/data/
DNSSEC validation	✓	Daily updates	Network level overview of DNSSEC validation (there is a parser available) (How to get access to that?)	https://stats.labs.apnic.net/dnssec

Measurement vantage points Infrastructure

Vantage point	Probes	Costs	Country	Limitations	Measurements
TU Dresden	1	–	DE	No	Internet-wide
HAW Hamburg	1	–	DE	No	Internet-wide
BCIX	1	–	DE	No	Internet-wide
RIPE Atlas	>1k	Credits	World-wide		Enrich set of resolvers
Proxies	?	Varying	World-wide	Ethics	Proxy measurements already running Maybe for cross validation
VPNs	?	Varying	World-wide	Keep in mind that they might lie about their location	First test from TUD vantage point, then run over VPN

Open resolver report



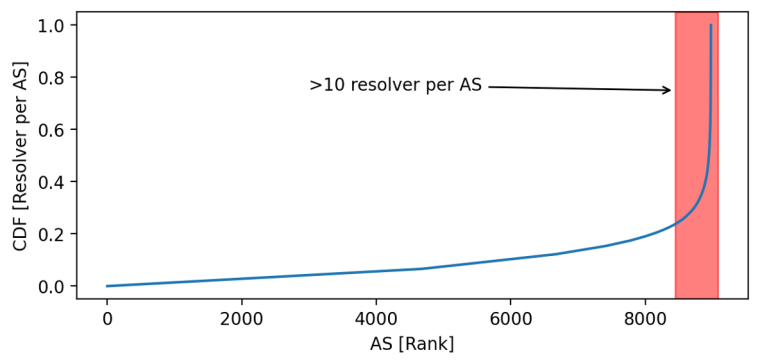


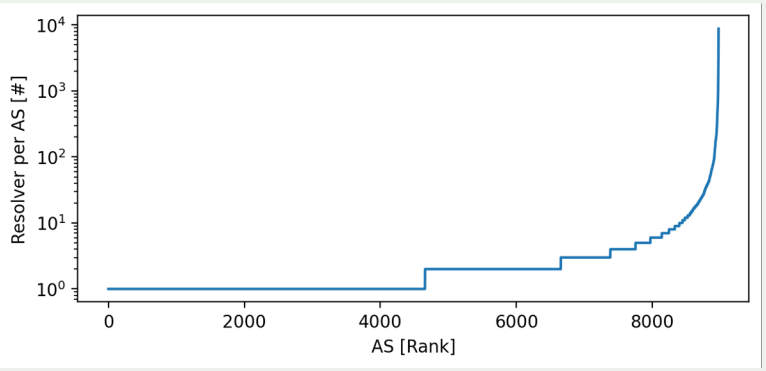
93% of ASes with open resolvers host less than 10 open resolvers.

We observe only a single open resolver per AS for 46% of the ASes.

We observe **28k** open resolvers in **5.4k** ASes and **183** countries.

Closed resolver report





We observe in 94% of ASes with closed resolvers host less than 10 instances.

We observe only a single closed resolver per AS for 48% of the ASes.

We observe **72k** closed resolvers in **9k** ASes and **212** countries*.

*unique country codes, not necessarily independent nations

Overview of spoofing networks

Open DNS API (Transparent forwarders):

ASes that allow spoofing: **2280**

Distributed in **98** countries, affecting **5.6k** BGP announced prefixes.

CAIDA Spoofer:

ASes that allow spoofing: **672**

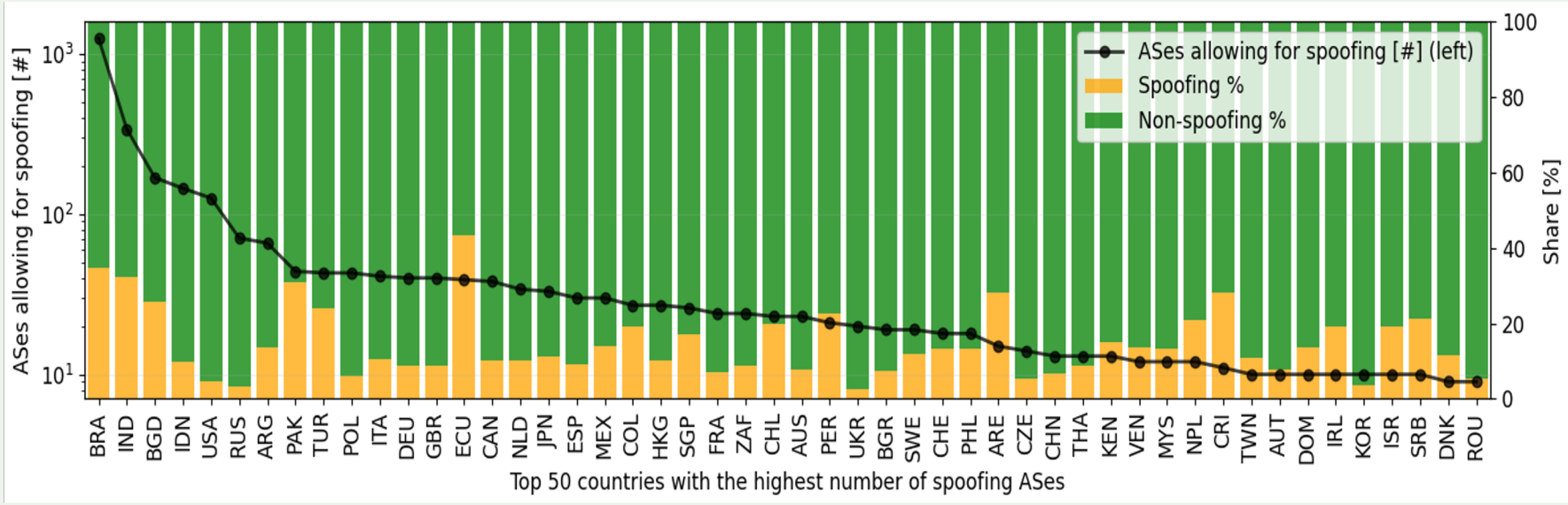
Distributed in **98** countries, affecting **2k** networks prefixes.

Overlap with CAIDA Spoofer:

98 ASes (4.3%)

66 countries (67%)

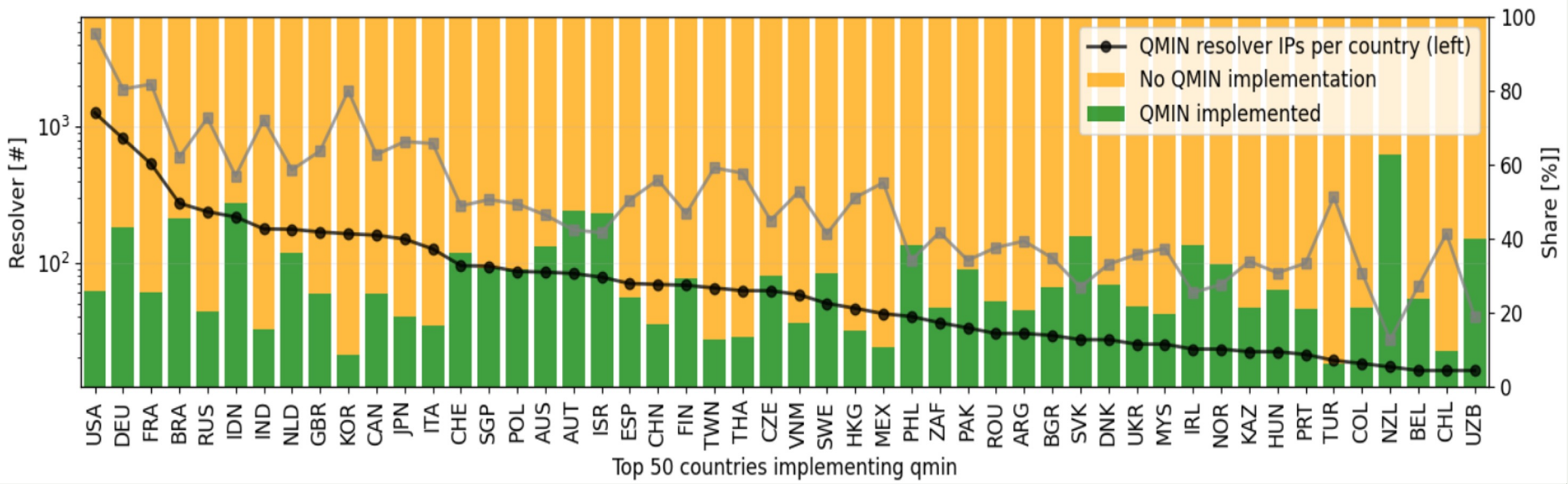
Spoofing networks
Overview



index	queried_ip_country	spoofing_asn_count	spoofing_asn_relative_amount
0	BRA	1,250	36.55
1	IND	340	9.94
2	BGD	169	4.94
3	IDN	145	4.24
4	USA	126	3.68

QMIN measurements
First results

~26k open resolvers tested
→ 6.4k (25%) implement qmin
→ 13.6k (52%) do not implement qmin
→ ambiguous for remaining 6k



Thank you

phokeer@isoc.org