DNS Maturity for National Cyber Resilience

Yasir Haq

ISOC Pulse Fellow 2024

University of Twente

Internet Society Pulse

Agenda

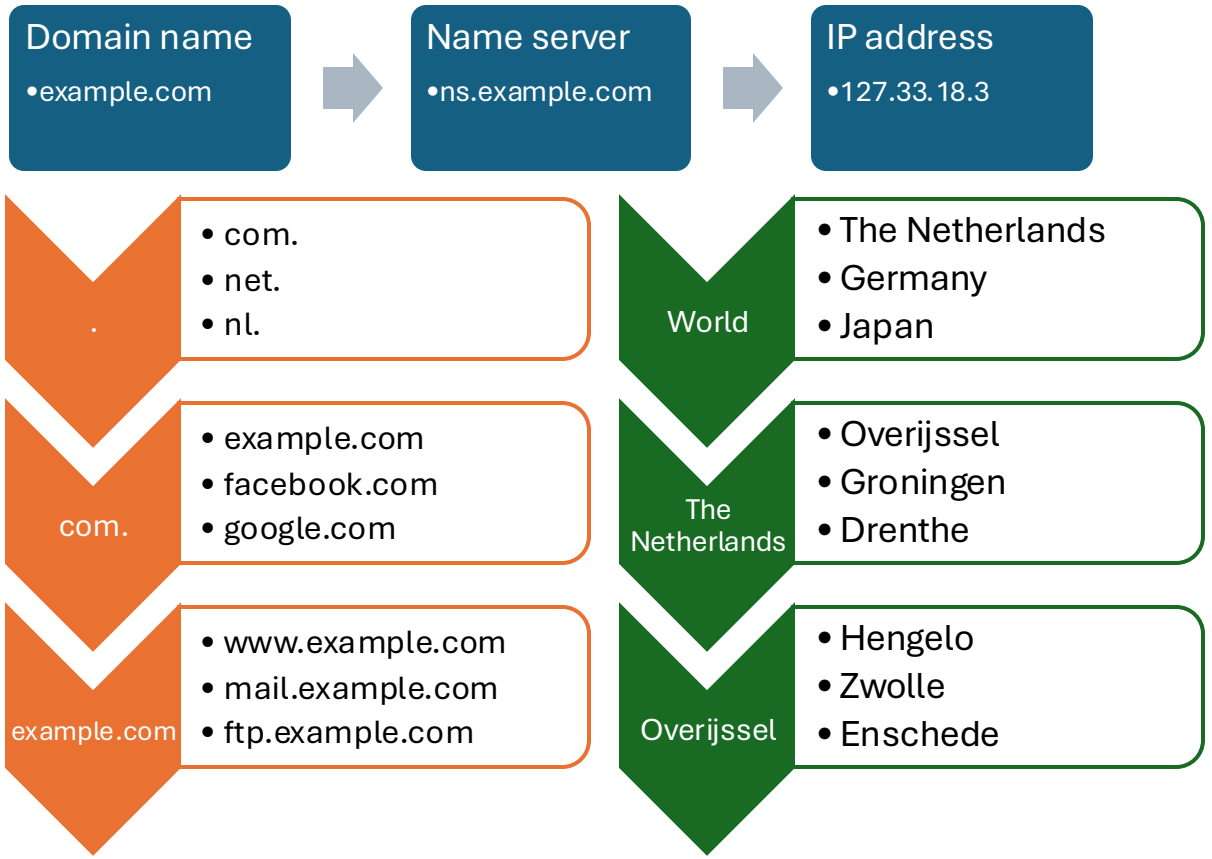
- Introduction
- Methodology
- Results
- Conclusions

Internet Society Pulse

Introduction

Domain Name System

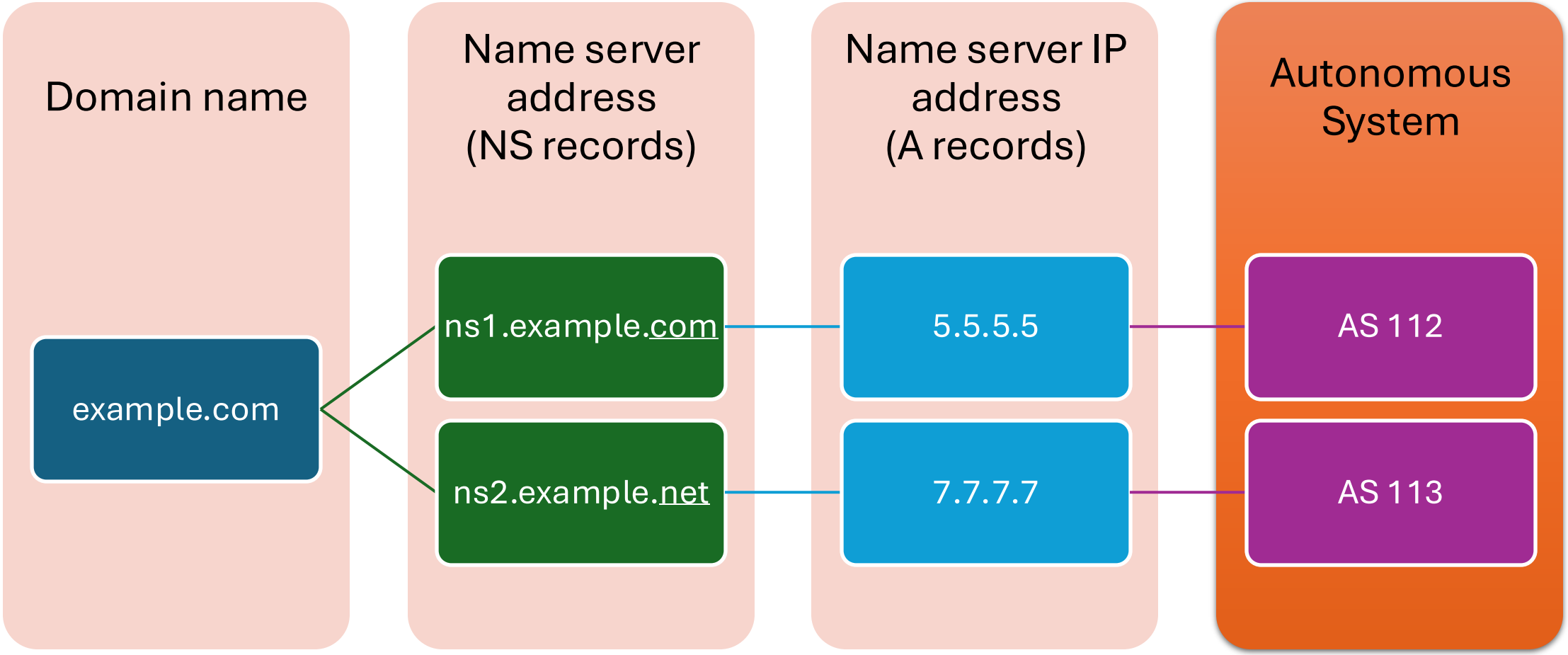
- DNS = Internet phone book
- A mission-critical infrastructure of the Internet
- Hierarchical structure ≈ mail address (from a country to a house)
- Attacks on DNS infrastructures: DDoS to take down the service
- It is crucial to promote security and resilience of DNS infrastructures



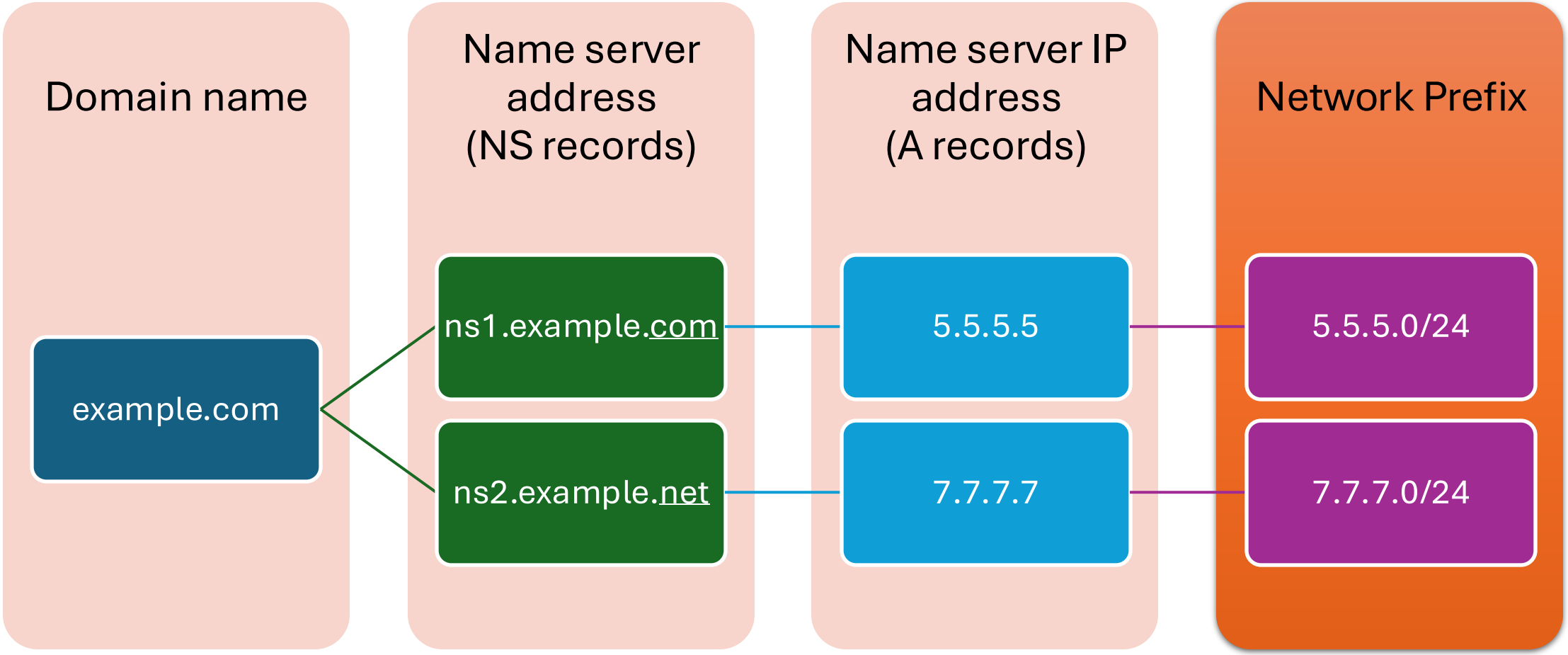
DNS Best Practice

- Resilience: maintain quality of service in non-ideal situations
  - Redundancy: duplicate critical components to prevent single points of failure
  - Distribution: spread resources across different physical locations and ensure logical separation to isolate problems
  - Diversity: mix of different technologies, providers, and geographic locations to reduce dependency on any single element
- Security: protect information confidentiality, integrity, and availability against cyber threat
  - Encryption: converting information into a ciphertext to prevent unauthorized access

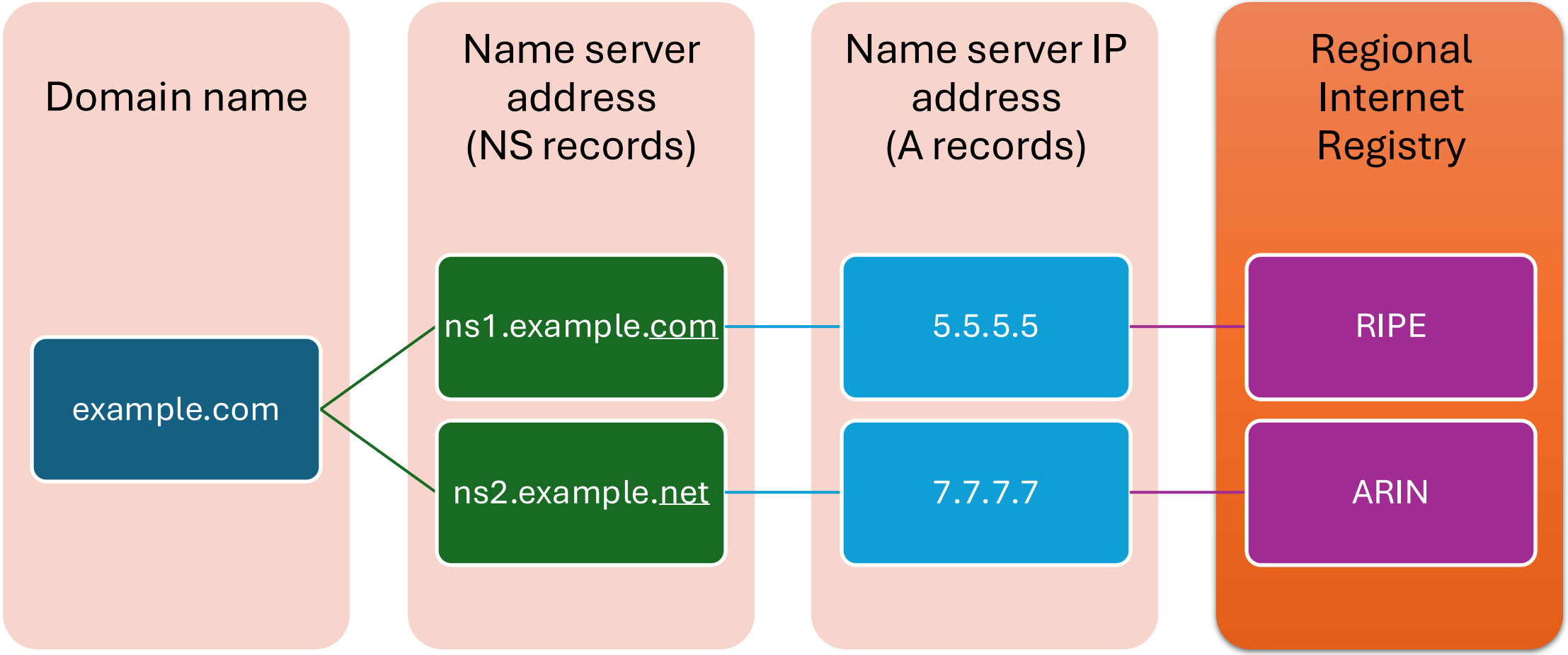
DNS Best Practice



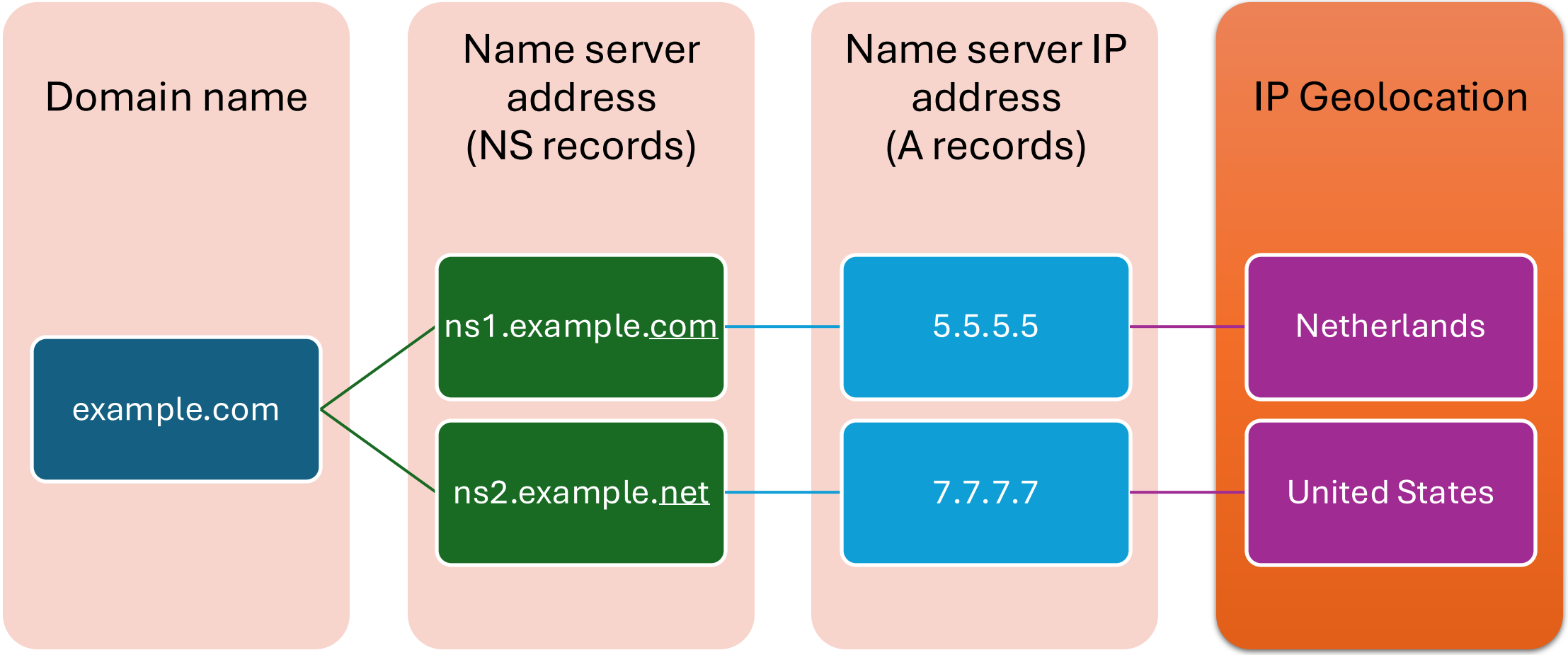
DNS Best Practice



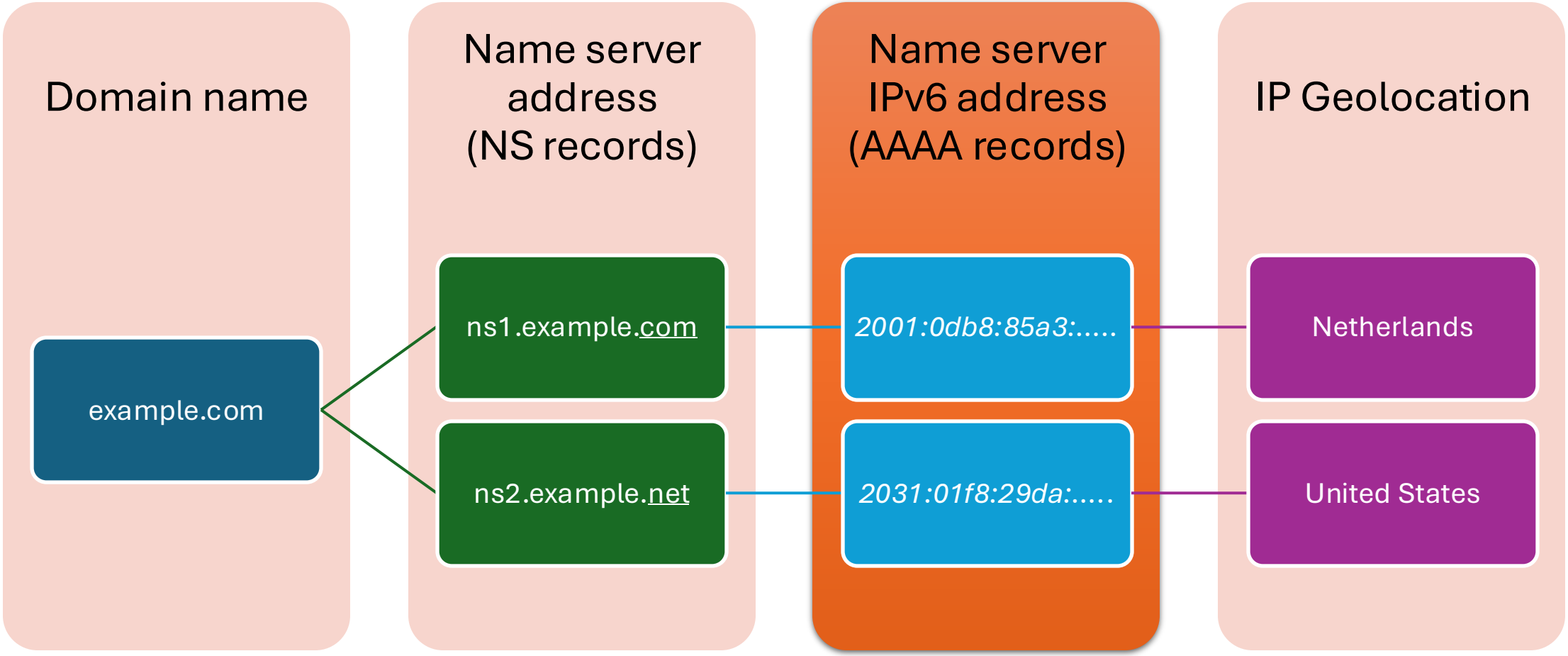
DNS Best Practice



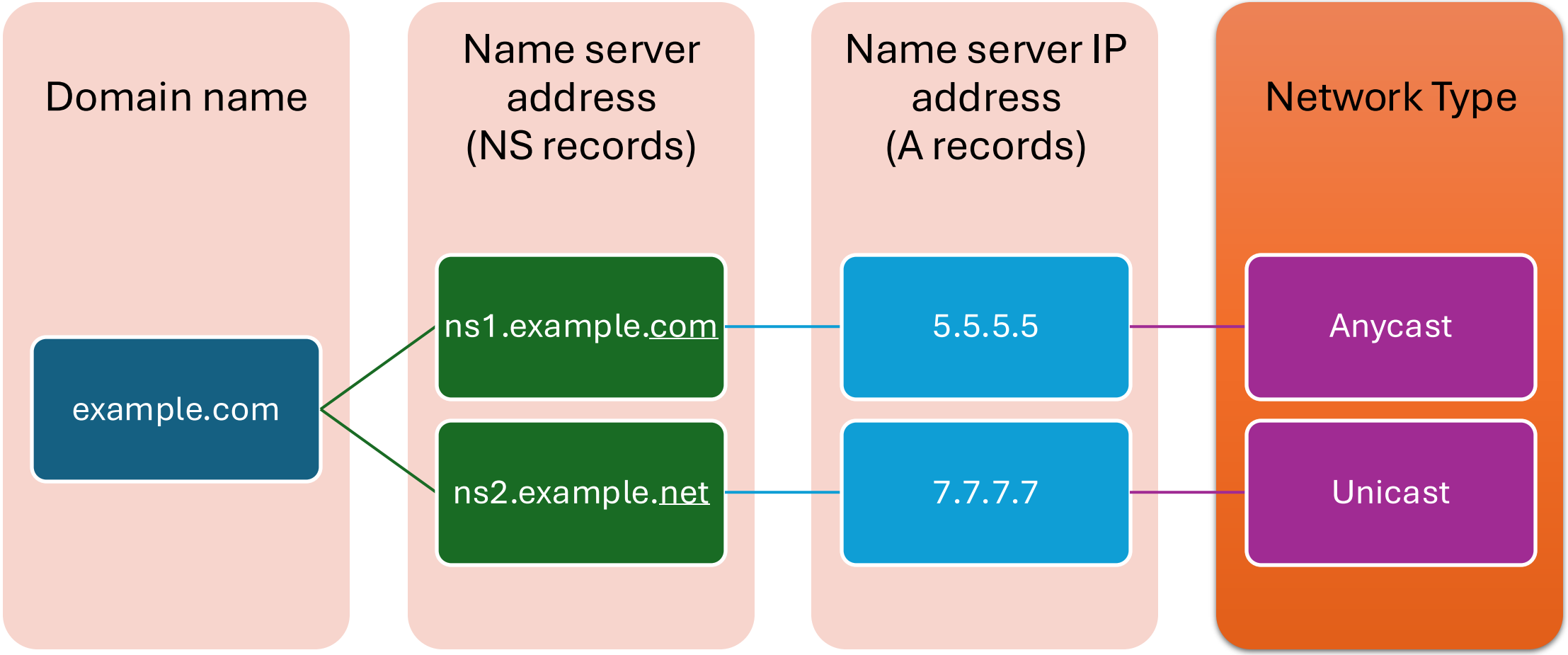
DNS Best Practice



DNS Best Practice

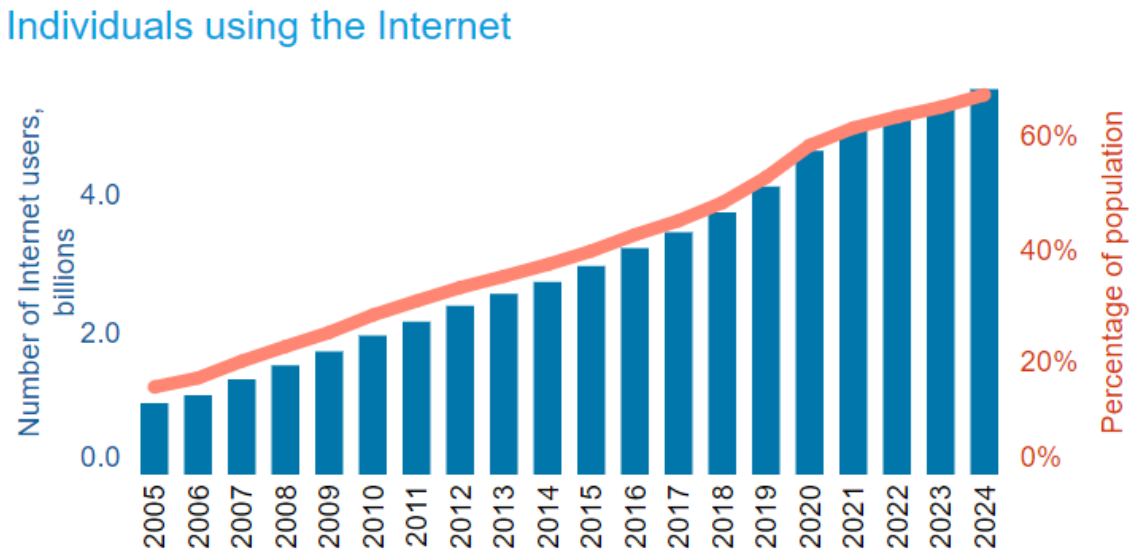


DNS Best Practice



National Cyber Resilience

- Increasing dependency on Internet for (critical) socio-economic activities
- Certain countries are more dependent than others
- Internet access → critical resource
- Internet disruptions → major socio-economic impact
- Resilient Internet → resilient nation



Source: ITU

COUNTRY	NUMBER OF INTERNET USERS 2024	DATA YEAR	% OF POPULATION USING INTERNET	INTERNET TRAFFIC 12/31/2020
China	1.1B	2022	77.3%	989.1M
India	881.3M	2023	62.6%	749.3M
United States	311.3M	2023	92.4%	312.3M
Indonesia	215.6M	2023	78.8%	196.4M
Pakistan	170M	2022	70.8%	76.4M
Brazil	165.3M	2022	77.1%	149.1M
Nigeria	136.2M	2020	63.8%	154.3M
Russia	129.8M	2022	89.5%	116.4M
Bangladesh	126.2M	2022	75.9%	111.9M
Japan	117.4M	2021	94.2%	118.6M
Mexico	96.8M	2023	75.1%	85M

Questions

How can we measure national cyber resilience based on maturity of the DNS infrastructures supporting the country?

- We evaluated DNS maturity of ccTLDs and top sites per country
- We estimated countries with the highest level of risk based on the maturity and the potential impact of downtime

Internet Society Pulse

Methodology

Data Sources and Analysis

- We use data from multiple sources to measure the DNS maturity of:
  1. ccTLDs
  2. Top 1K sites per country under the designated ccTLD (e.g. Germany: .de)
- We excluded IDN* ccTLDs (e.g., .pϕ)
- We implement a heuristic to filter our top lists

IANA Root Zone DB
- List of ccTLDs

IANA WHOIS
- Auth. NS records

NRO Delegation
- IP-to-prefix
- IP-to-RIR

CAIDA IP-to-AS

bgp.tools Anycatch
- Anycast prefix

getdns
- NS records
- A/AAAA records
- DS records

ipinfo Geolocation
- IP country geolocation

DomainTools
- Domain count per ccTLD

Mozilla PSL
- FQDN to PLD

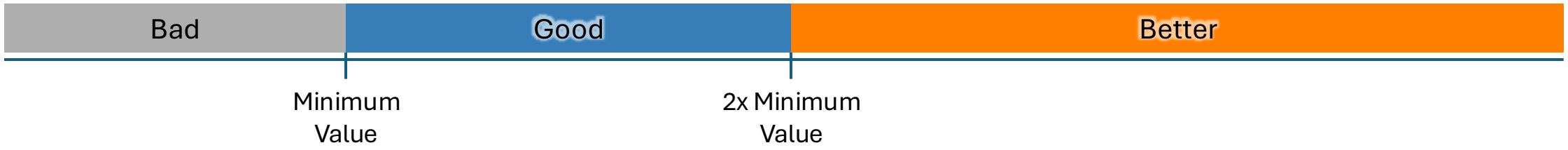
Google CrUX Country Report
- Top sites by country

DNS Best Practice Metrics and Classification

(based on Sommese (2023)[1])

Internet Society Pulse

	Metric	Description	Minimum Value
Critical	nNSes	Number of unique NS records	2
	nIPv4	Number of unique IPv4 addresses for NSes	2
	nIPv6	Number of unique IPv6 addresses for NSes	2
	nPrefixes4	Number of unique IPv4 BGP prefixes for NSes	2
	nPrefixes6	Number of unique IPv6 BGP prefixes for NSes	2
	nASv4	Number of unique IPv4 ASes for NSes	2
	nASv6	Number of unique IPv6 ASes for NSes	2
	nGeoDiverseNSes	Number of unique NS geolocations	2
Recommended	nTLDs	Number of unique TLDs for NS addresses	2
	nRIRv4	Number of unique IPv4 RIR for NSes	2
	nRIRv6	Number of unique IPv6 RIR for NSes	2
	nAnycast4	Number of IPv4 Anycast server	1
	nAnycast6	Number of IPv6 Anycast server	1

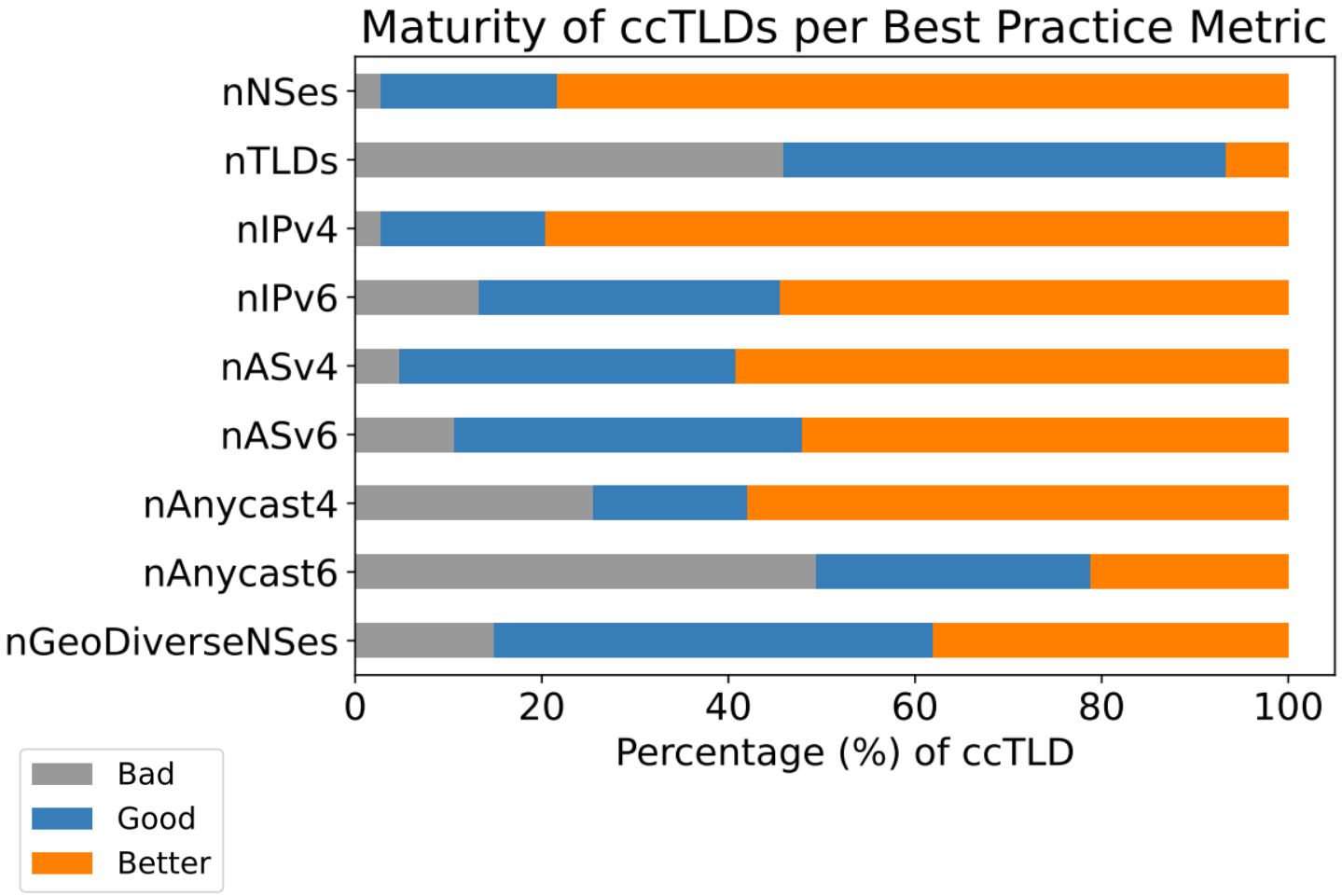


[1]Sommese, R. (2023). *Everything in Its Right Place: Improving DNS resilience*. https://research.utwente.nl/en/publications/everything-in-its-right-place-improving-dns-resilience

Internet Society Pulse

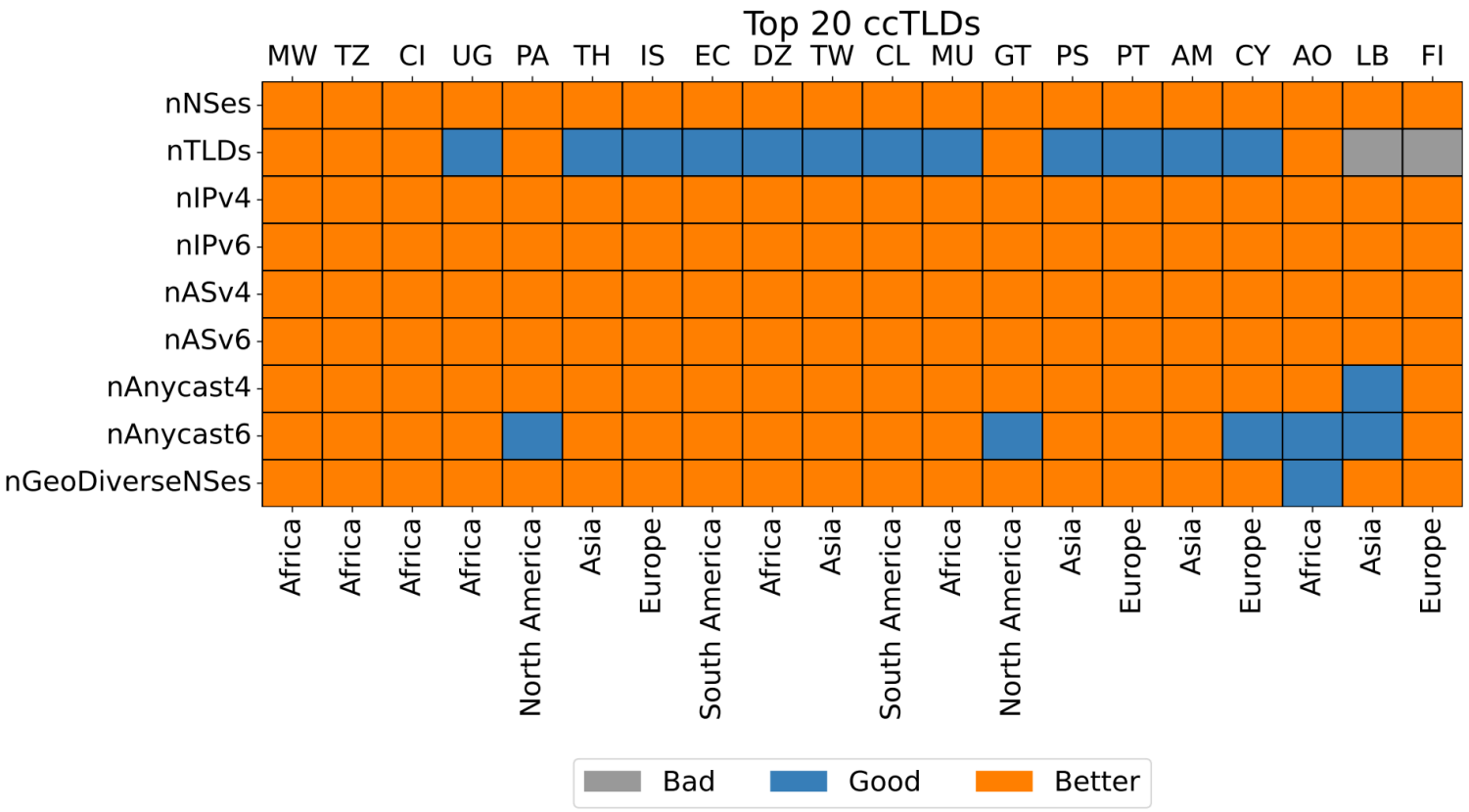
Results

DNS maturity of ccTLDs



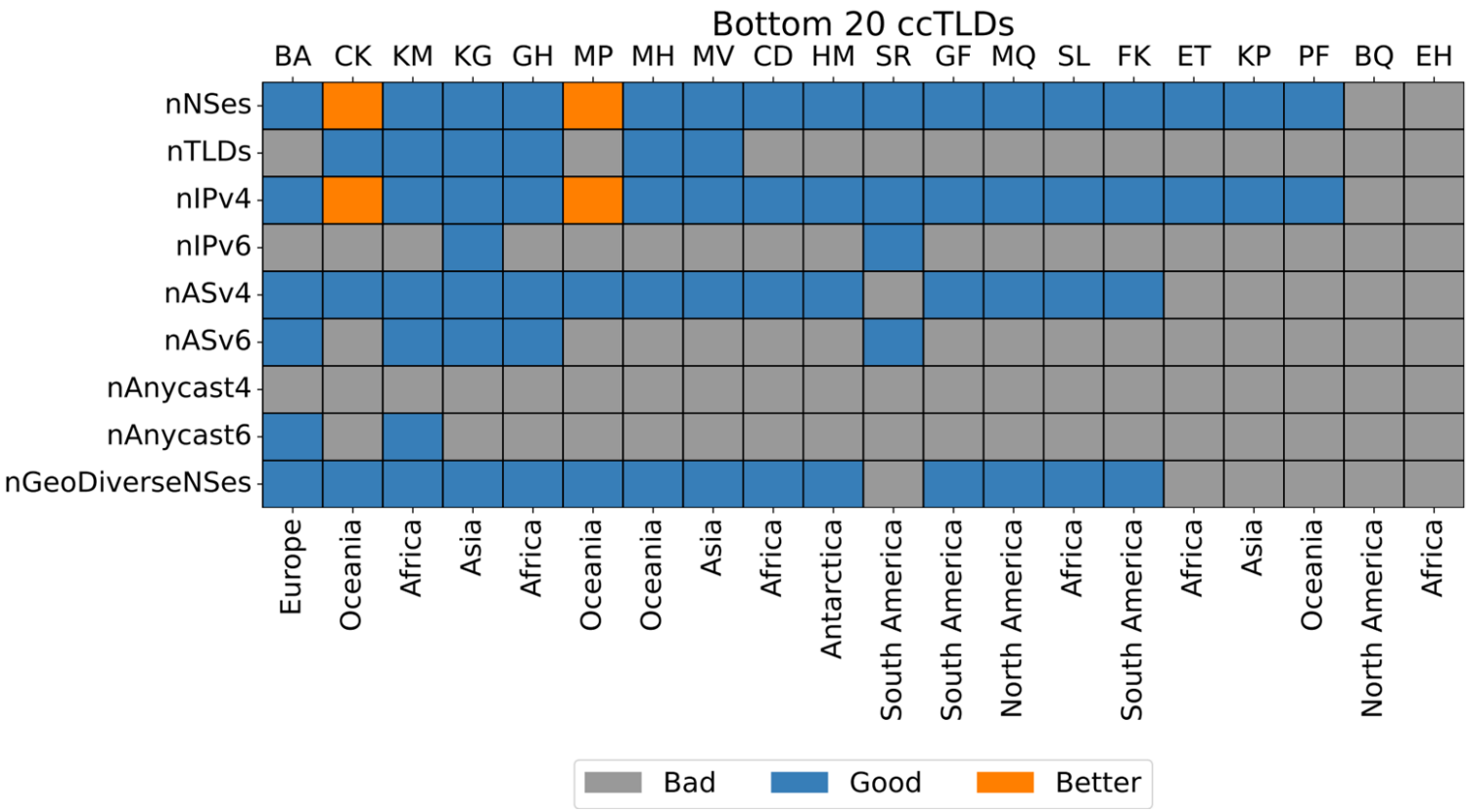
- Most ccTLDs have implemented redundancy strategy (see nNSes, nIPv4&6, nASv4&6)
- Regarding diversity strategy, only in the IP geolocations (nGeoDiverseNSes) but not in the name server TLD (nTLDs), i.e., they use name server addresses from the same TLD (e.g., ns1.abc.com, ns2.def.com)
- Adoption of Anycast for name servers remains limited, i.e., <80% (see nAnycast4&6)

Top 20 ccTLDs by DNS Maturity



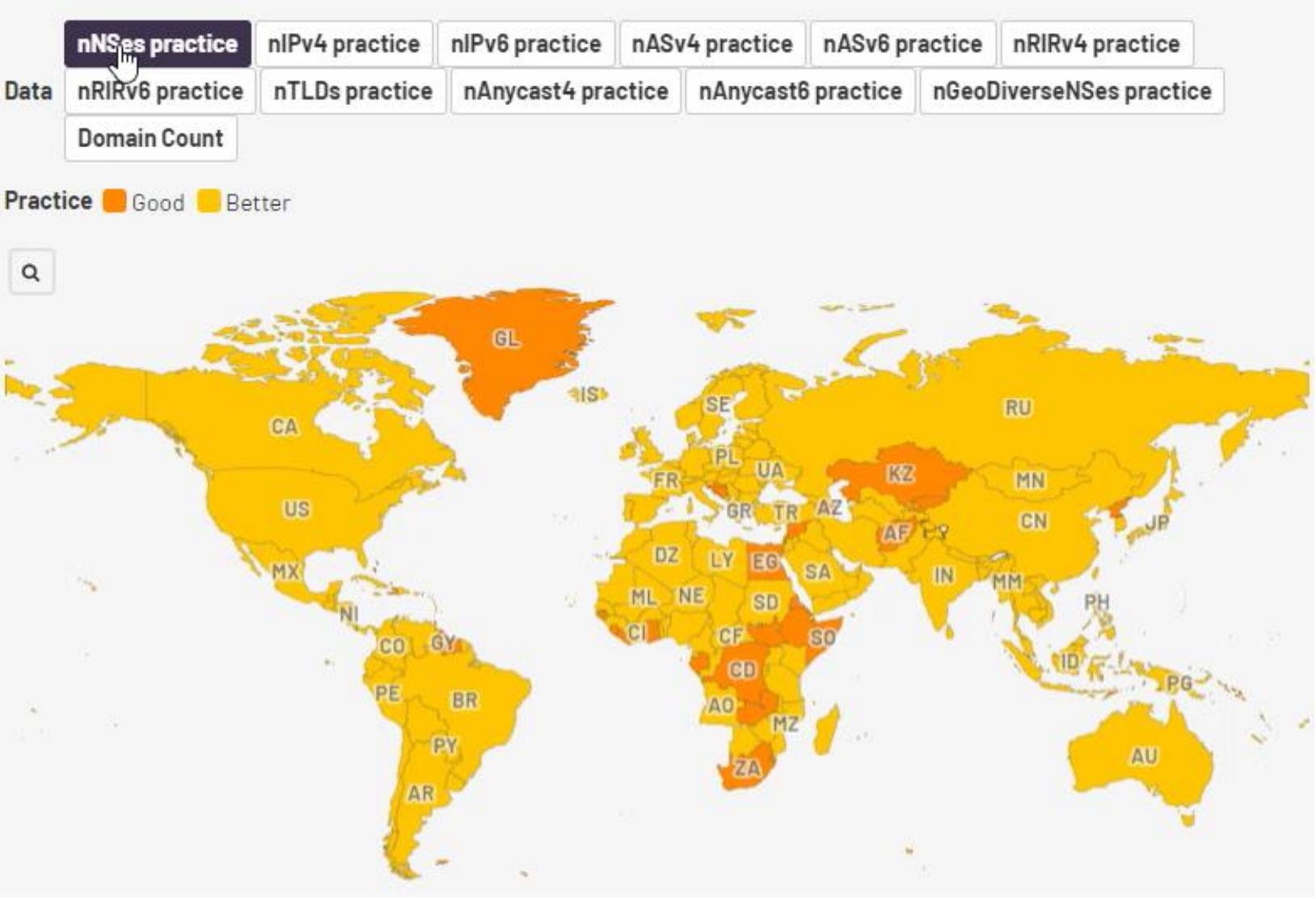
- Only a few ccTLDs from countries in Europe (IS, PT, CY, FI) and North America (PA, GT) despite the advanced economic development of these regions.
- In contrast, African (MW, TZ, CI, UG, DZ, MU) and Asian (TH, TW, PS, AM, LB) ccTLDs show a stronger presence.

Bottom 20 ccTLDs by DNS Maturity



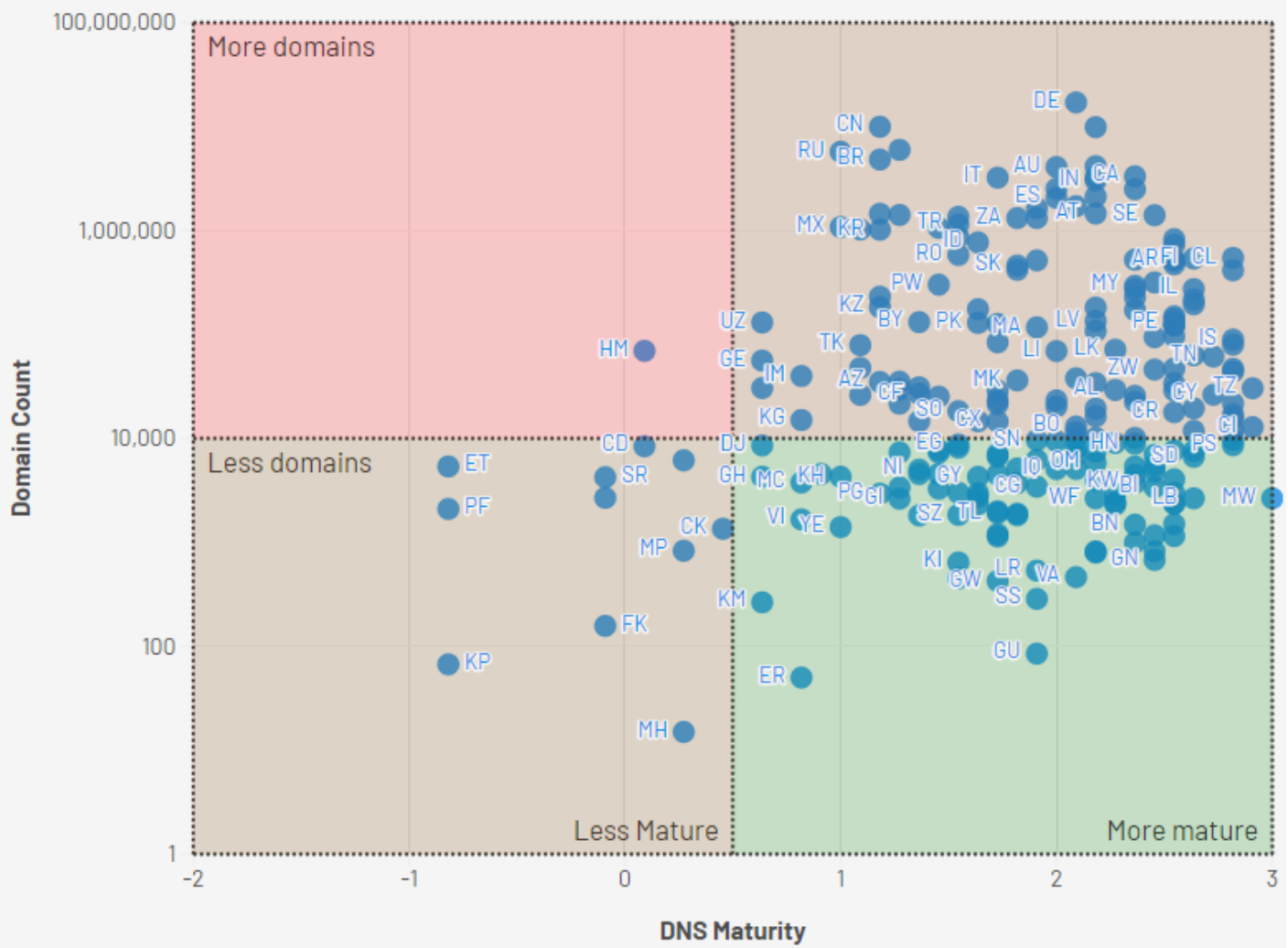
- Among ccTLDs with the least DNS maturity, BQ and EH remain unassigned to their designated countries, Caribbean Netherlands and Western Sahara, due to territory dispute.
- Internet access limitation for North Korean citizens might cause its ccTLD (KP) low DNS maturity.
- Adoption of more recent technologies such as Anycast and IPv6 are the lowest among these ccTLDs.

Interactive Visualization



- We visualized the data in an interactive and customizable dashboard on Fluorish
- Visit the visualization here

Risk level of ccTLDs



- We introduced domain count data from DomainTools[1] to estimate the potential impact of DNS disruption of ccTLDs
- The more domain names under a ccTLD, the larger the impact
- e.g., if DNS of **.de** is down, ~17 millions domain names will be inaccessible
- ccTLDs with many domain names but less mature DNS are at a higher risk
- With aggregate the metrics into a single maturity score per ccTLD, where:
  - Good = +1
  - Better = +2
  - Bad = -1
- For an interactive dashboard, visit this link

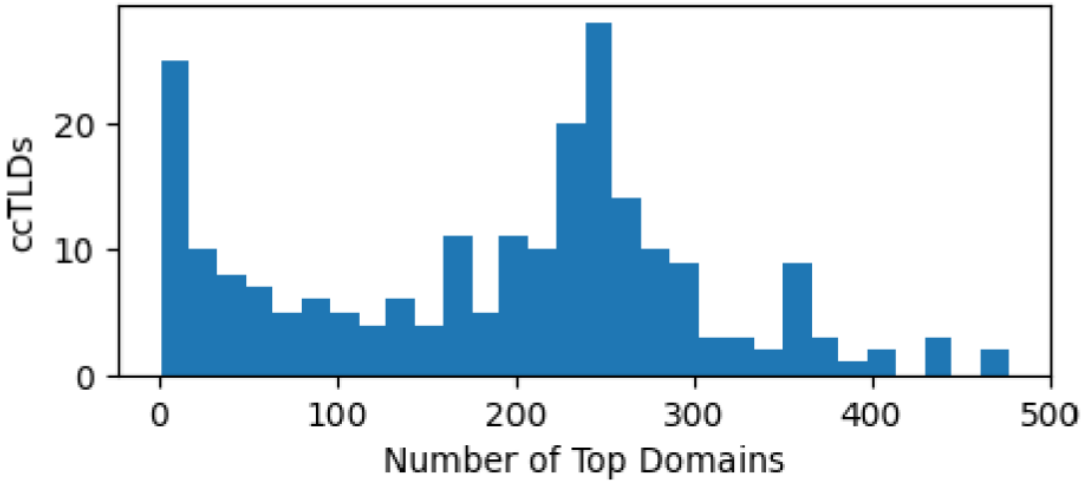
[1] Domain Count Statistics for TLDs - DomainTools

DNS Maturity of Country Top Domain Names

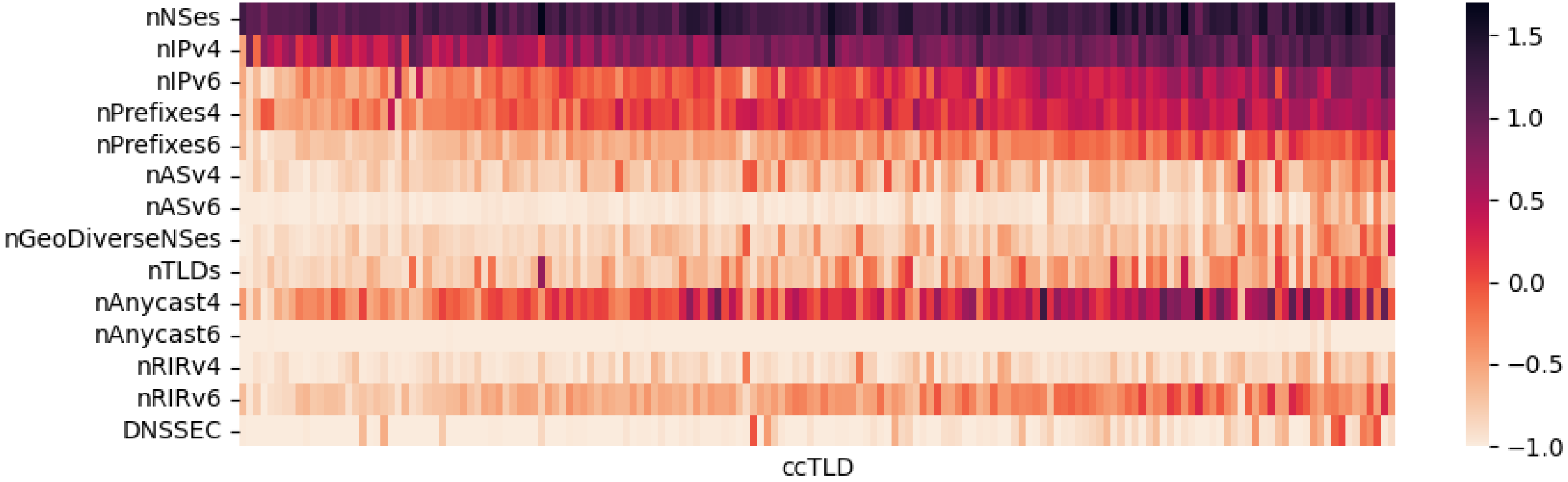
- Not every ccTLD is popular among users from the associated country
- Some ccTLDs are more popular to promote other identities rather than the national identities
- E.g., .AI is the ccTLD of Anguilla, a British Teritory, but is more popular with companies in the artificial intelligence (AI) industry

Table 1: Data overview

Category	Count	Percentage
Total all TLDs	1,591	503.48%
All ccTLDs	316	100.00%
IDNs of ccTLDs (excluded)	61	19.30%
ccTLDs without IDNs	255	80.70%
ccTLDs with CrUX report	226	71.52%
ccTLDs with ≥100 PLDs	164	51.90%



Aggregated DNS Maturity Score

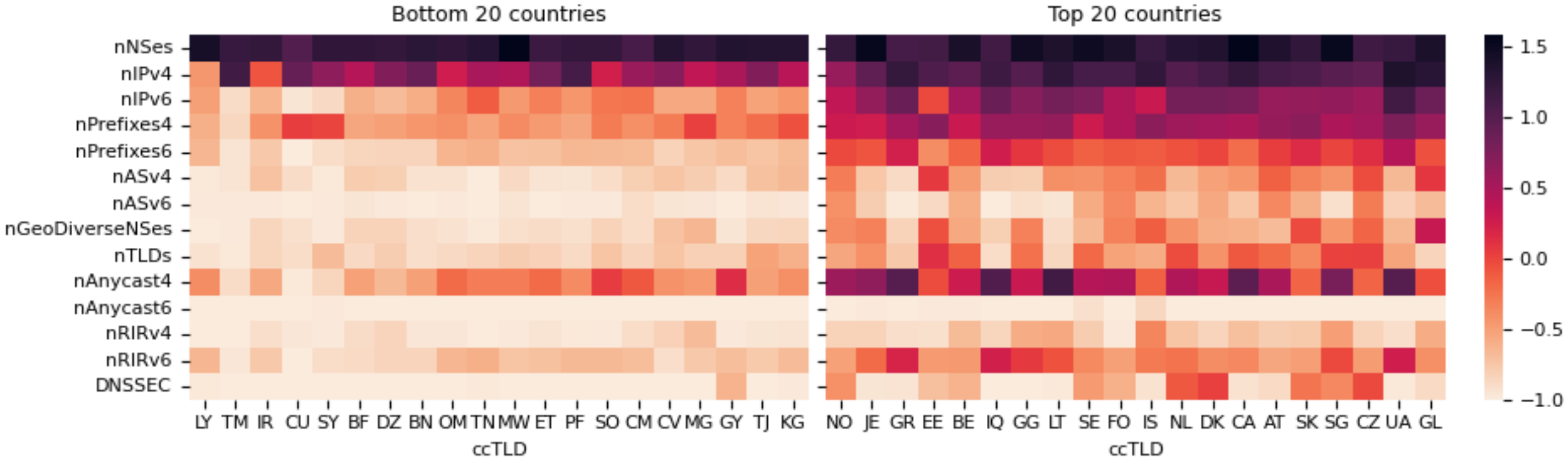


- For each DNS best practice metric, we aggregated the practices of the top domain names per country where: Good = +1, Better = +2, and Bad = -1
- We normalized the score with the number of top domain names per country

Bottom and Top 20 Countries

Internet Society Pulse

By Top Domains DNS Maturity

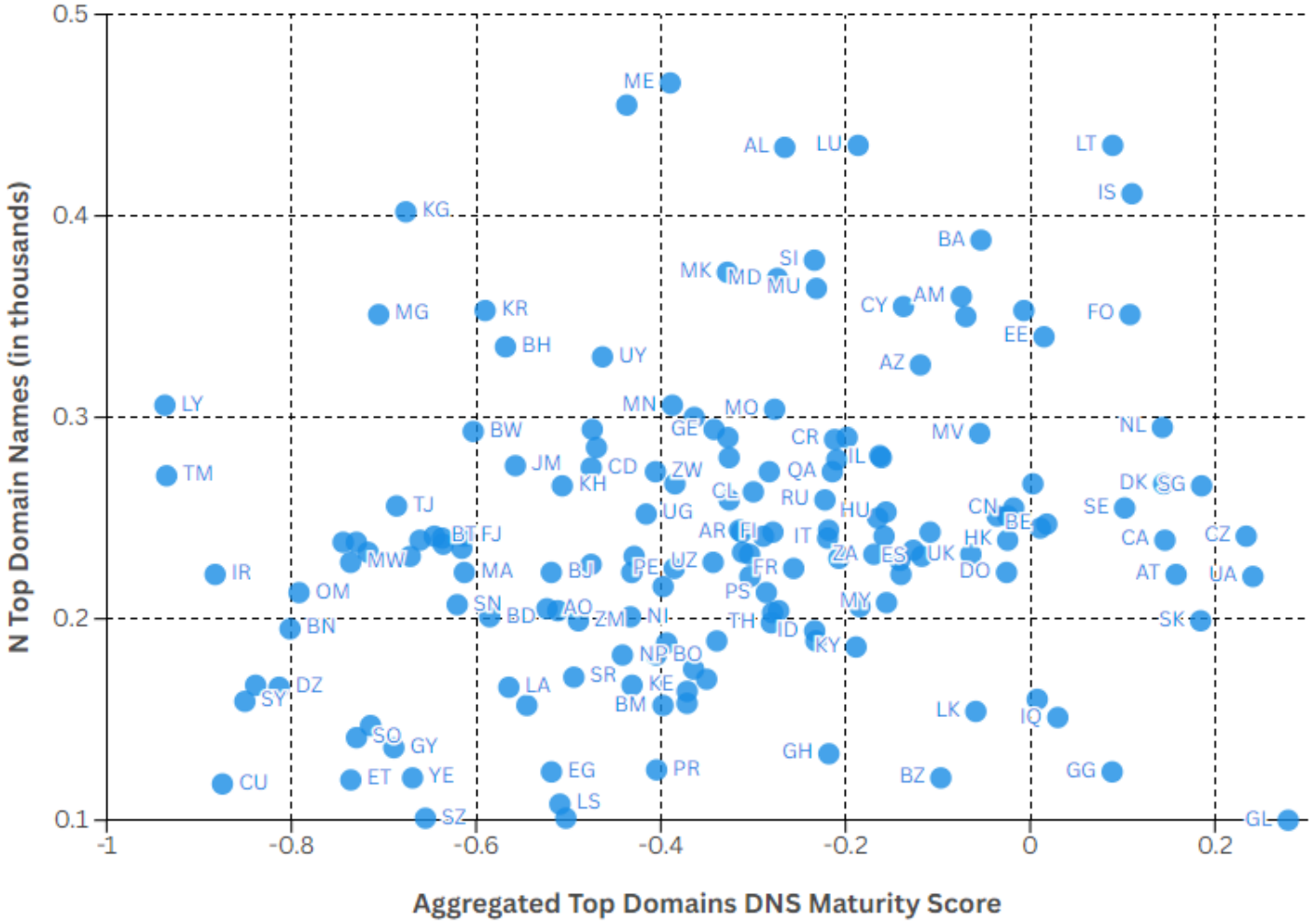


By ccTLD DNS Maturity

Bottom 20 ccTLDs																			
BA	CK	KM	KG	GH	MP	MH	MV	CD	HM	SR	GF	MQ	SL	FK	ET	KP	PF	BQ	EH

Top 20 ccTLDs																			
MW	TZ	CI	UG	PA	TH	IS	EC	DZ	TW	CL	MU	GT	PS	PT	AM	CY	AO	LB	FI

Risk level per country: Top domain names



- We aggregated the metrics of each country into a single score using weighted average with **critical metrics weighted twice**.
- We compared the number of top domain names per country to estimate the potential impact on the country.
- Countries with low maturity score but high in the number of top domain names have a higher risk.
- For the interactive dashboard of this plot, please visit this link

Internet Society Pulse

Conclusions

Key Takeaways

- The economic development of a country does not necessarily correlate with the technical maturity of the DNS infrastructure supporting its country-code Top Level Domain (ccTLD).
- Most ccTLDs have redundancy in place except but not diversity, in particular, in name server TLDs.
- Some ccTLDs possess a higher risk level: more vulnerable to downtime but might impact more users.
- ccTLDs might carry identities other than its national one reflected in the number of domains under the ccTLD which are popular to the local users.

Future Works

- Introduce web categories to evaluate DNS maturity and potential impact of DNS downtime in various industry sectors.
- Prepare a scientific paper for publication.

Thanks! Any question?

Or reach me at m.y.m.haq@utwente.nl