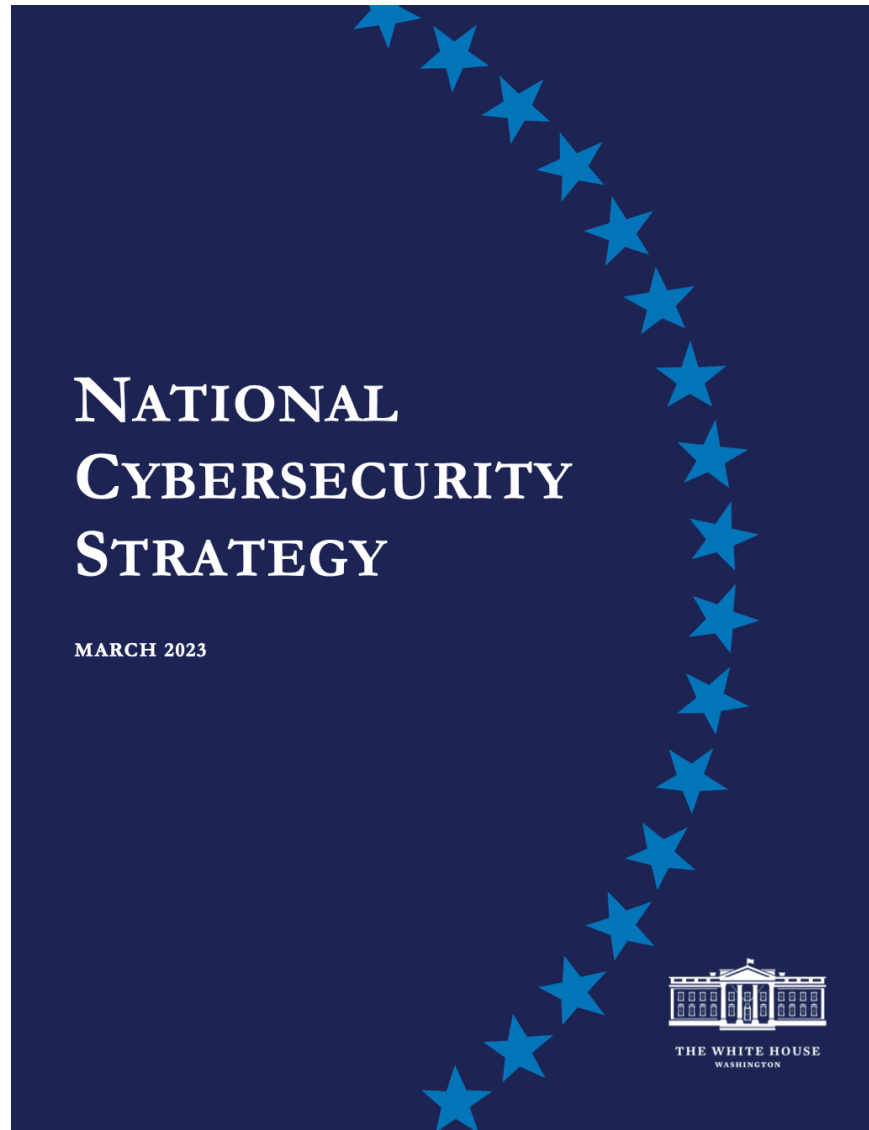


# Identifying Current Barriers in RPKI Adoption

Cecilia Testart, Josephine Wolff, Deepak Gouda,  
and Romain Fontugne

Sept. 21, 2024

# Routing Security as a Policy Priority



“Many of the technical foundations of the digital ecosystem are inherently vulnerable ... We must take steps to mitigate the most urgent of these pervasive concerns such as Border Gateway Protocol vulnerabilities”

**Media Contact:**

MediaRelations@fcc.gov

**For Immediate Release****FCC CHAIRWOMAN PROPOSES INTERNET ROUTING SECURITY REPORTING REQUIREMENTS*****Broadband Providers Would Need BGP Security Plans and Largest Providers Would File Quarterly Reports***

WASHINGTON, May 15, 2024—FCC Chairwoman Jessica Rosenworcel today proposed requiring the largest broadband providers to file confidential reports on Border Gateway Protocol (BGP) security so the FCC and its national security partners can for the first time collect more up-to-date information about this critical internet routing intersection. BGP is the technology used for routing information through the physical and digital infrastructure of the internet.

National security experts have raised concerns that, by accessing vulnerabilities in BGP, bad actors can disrupt critical services that rely on the internet and result in misdirection, interception, inspection, or manipulation of data. A bad network actor may deliberately falsify BGP reachability information to redirect traffic. Russian network operators have been suspected of exploiting BGP's vulnerability for hijacking in the past. "BGP hijacks" can expose Americans' personal information, enable theft, extortion, state-level espionage, and disrupt otherwise-secure transactions.



Voer uw zoekterm in

## Beter beveiligde internetroutering overheid voor eind 2024

# Beter beveiligde internetroutering overheid voor eind 2024

04 apr 2023

Alle ICT-systemen van de overheid dienen voor het einde van 2024 gebruik te maken van de standaard RPKI, zodat de internetroutering van de overheid veiliger wordt. Dit doel stelde het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) op 30 maart vast in een streefbeeldafpraak. Het betekent dat RPKI niet alleen bij nieuwe aanschaffen vereist is, maar ook op alle bestaande overheidssystemen geïmplementeerd moet worden. Onderaan dit bericht leest u hoe u dat doet.

# All Dutch govt networks to use RPKI to prevent BGP hijacking

By **Bill Toulas**

April 9, 2023

11:21 AM

0



The Dutch government will upgrade the security of its internet routing by adopting before the end of 2024 the Resource Public Key Infrastructure (RPKI) standard.

# What is the problem?

- Border Gateway Protocol (BGP) lacks a built-in mechanism for validating the information that networks share and use to select global routes for data traffic

## Orange Spain Faces BGP Traffic Hijack After RIPE

### Account Hacked by Malware

 Jan 05, 2024  Ravie Lakshmanan

## Attackers exploit fundamental flaw in the web's security to steal \$2 million in cryptocurrency

MARCH 9, 2022 BY HENRY BIRGE-LEE

## Russian telco hijacks internet traffic for Google, AWS, Cloudflare, and others


Rostelecom involved in BGP hijacking incident this week impacting more than 200 CDNs and cloud providers.



Written by **Catalin Cimpanu**, Contributor  
April 5, 2020 at 2:53 p.m. PT

## Cloudflare blames recent outage on BGP hijacking incident

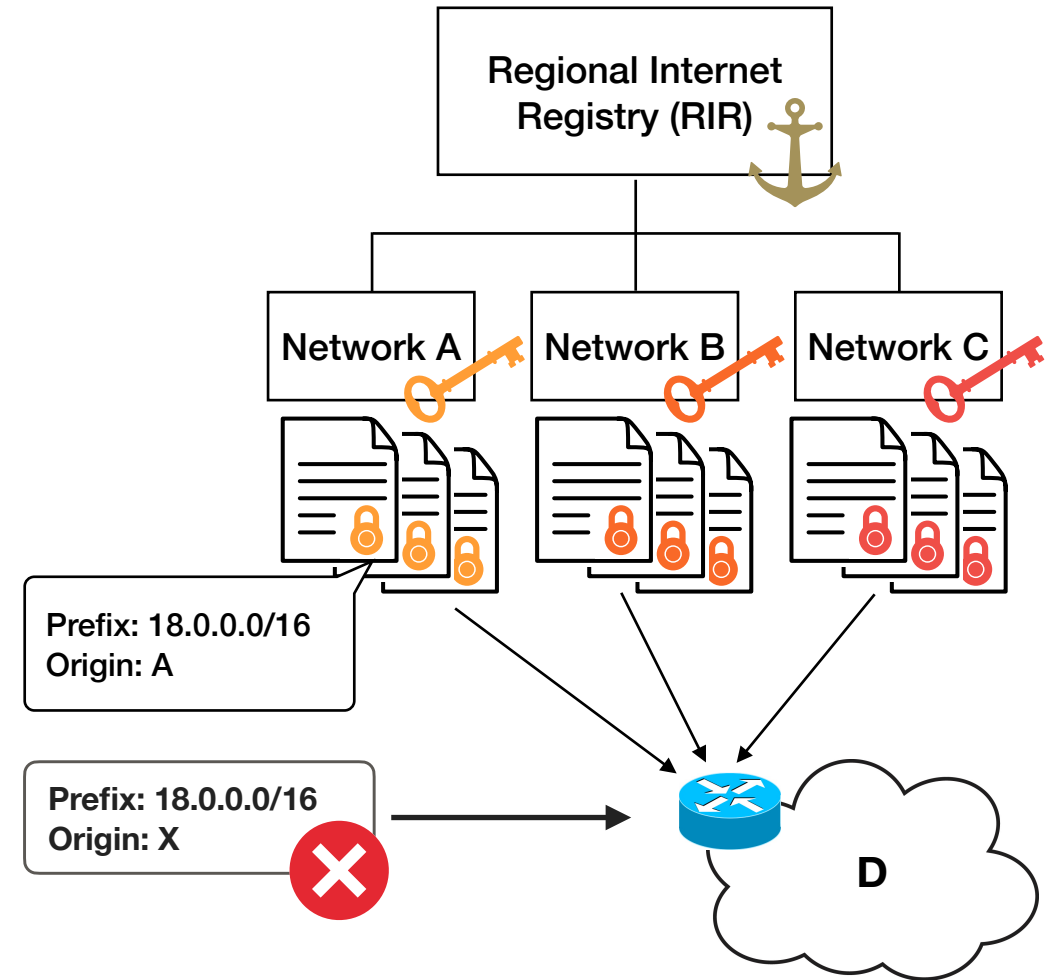
By **Bill Toulas**

 July 5, 2024

# The Resource Public Key Infrastructure (RPKI)

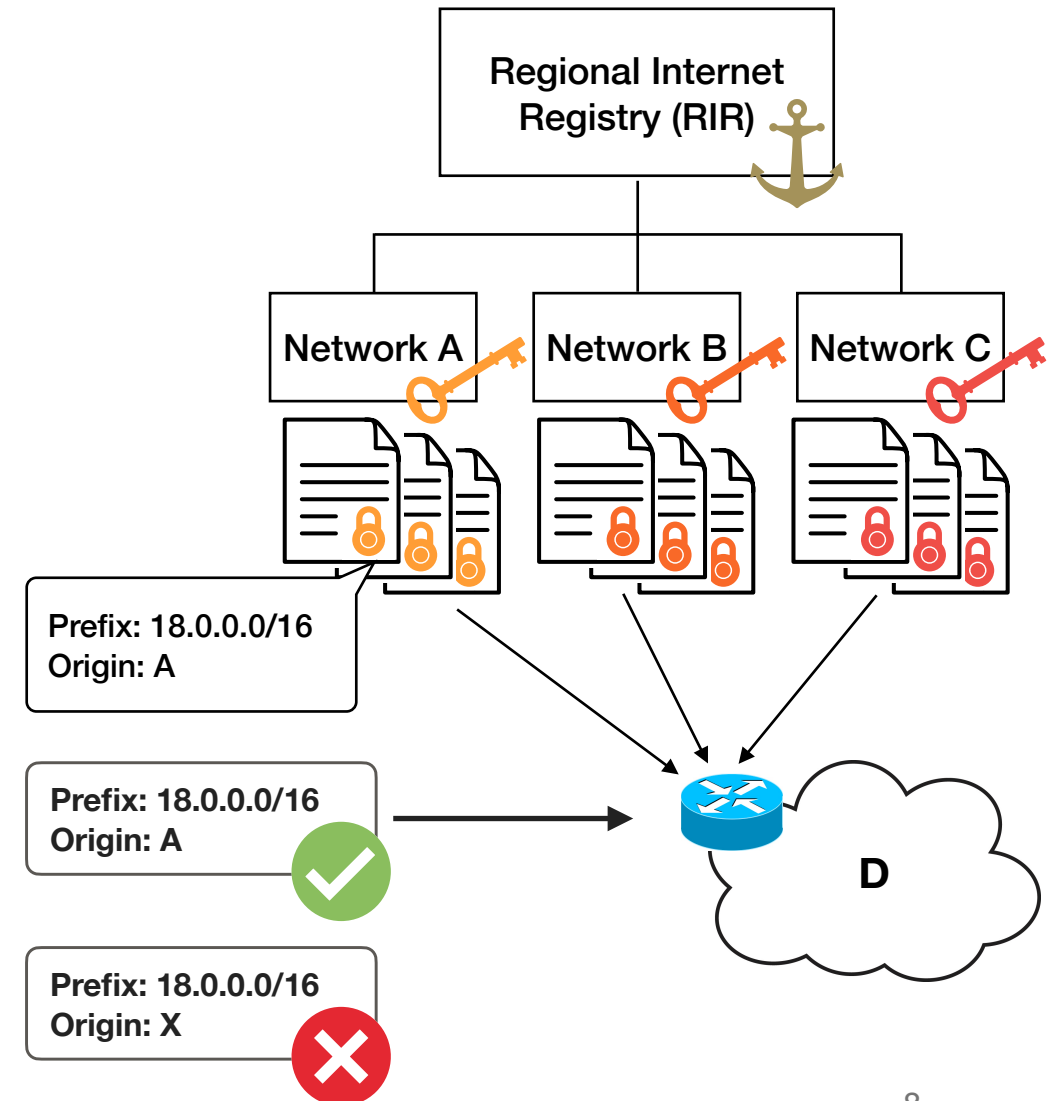
- Framework to secure routing using cryptographic records to validate **prefix** and **origin** in BGP announcements.

- (1) Route Origin Authorizations (ROAs) map IP prefixes with valid origins.
- (2) Networks can use these assertions to validate announcements in BGP (Route Origin Validation, ROV)



# The Resource Public Key Infrastructure (RPKI)

- Framework to secure routing using cryptographic records to validate **prefix** and **origin** in BGP announcements.
- (1) Route Origin Authorizations (ROAs) map IP prefixes with valid origins.
  - (2) Networks can use these assertions to validate announcements in BGP (Route Origin Validation, ROV)

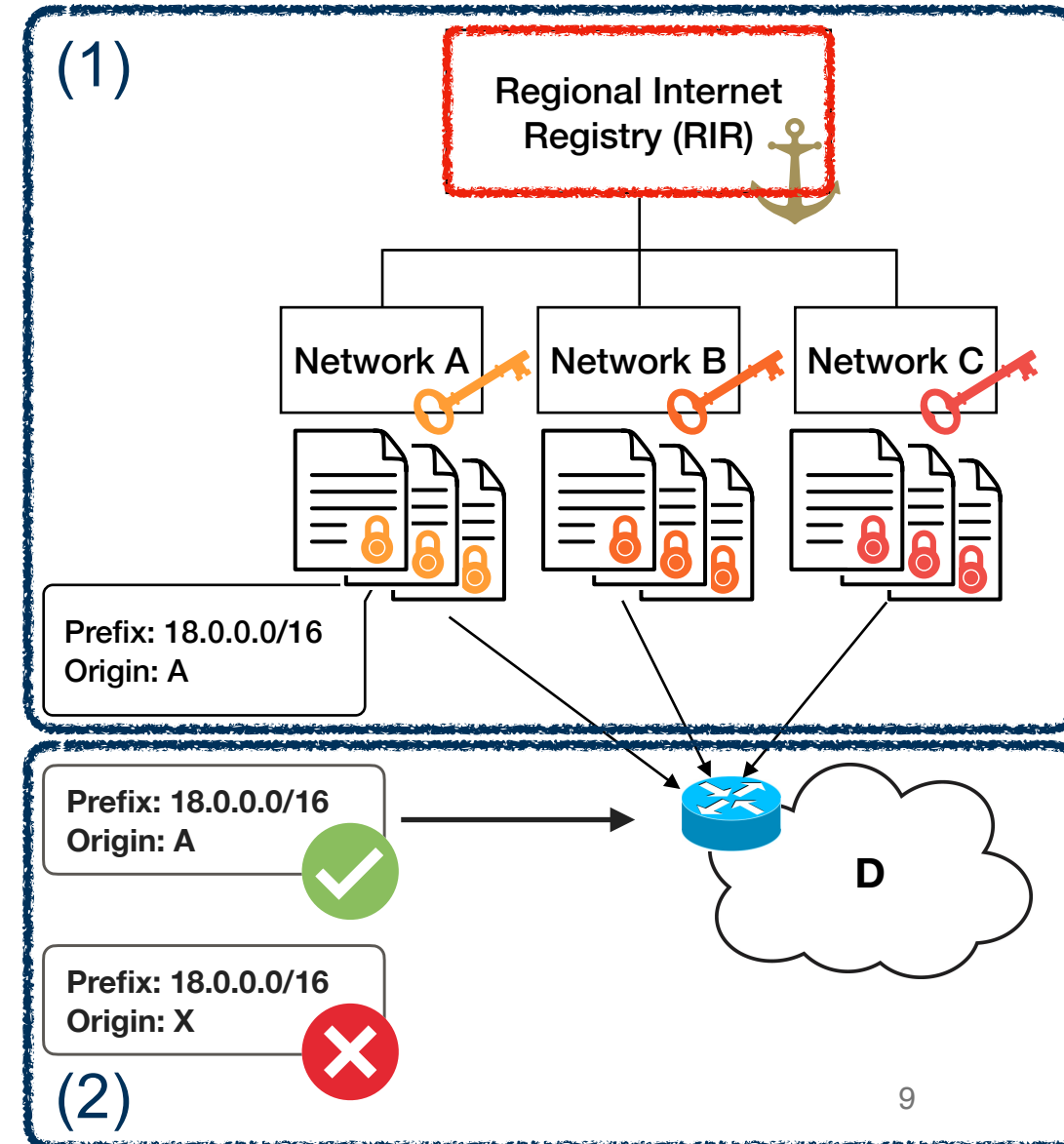




# The Resource Public Key Infrastructure (RPKI)

- Framework to secure routing using cryptographic records to validate **prefix** and **origin** in BGP announcements.

- (1) Route Origin Authorizations (ROAs) map IP prefixes with valid origins.
- (2) Networks can use these assertions to validate announcements in BGP (Route Origin Validation, ROV)



# RIRs Delegate Internet Resources (IP & ASNs)

## Regional Internet Registries (RIRs)

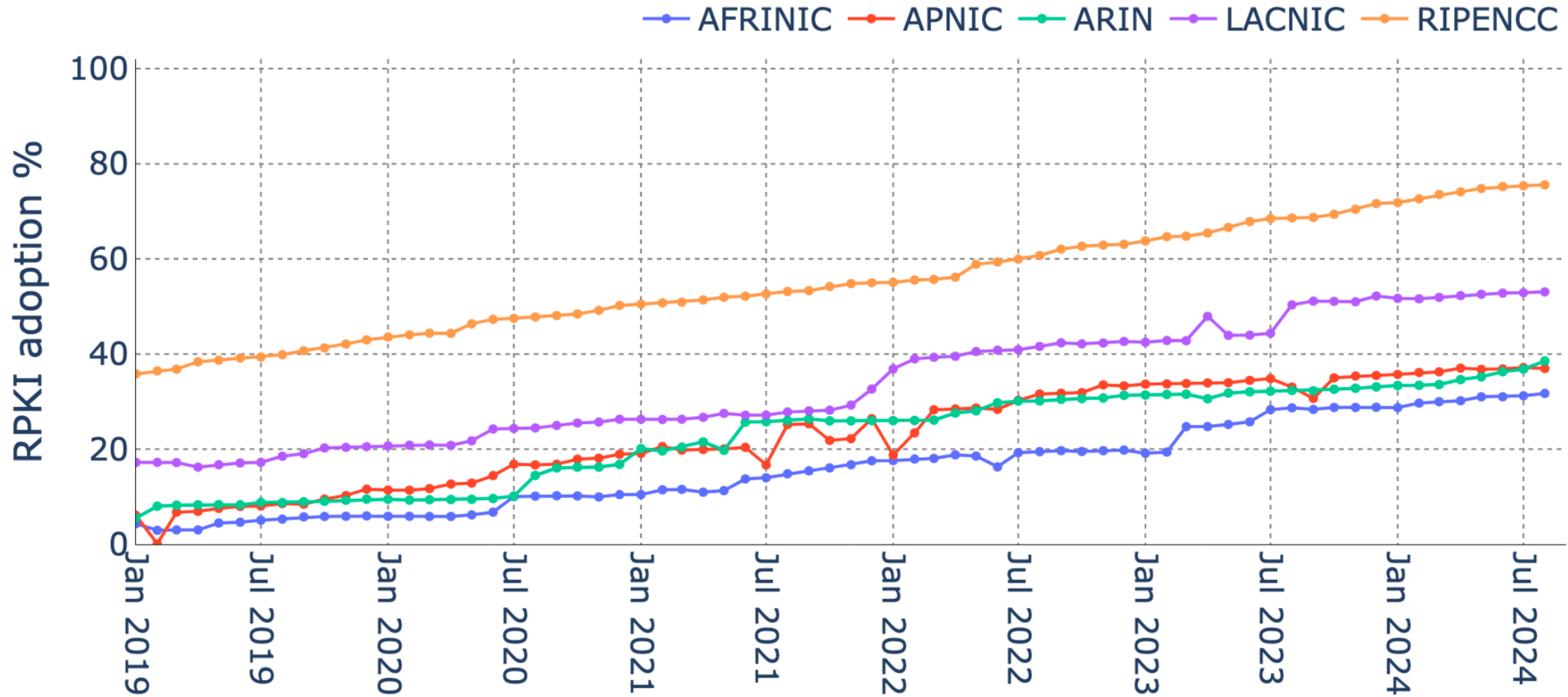


# Research Questions & Data

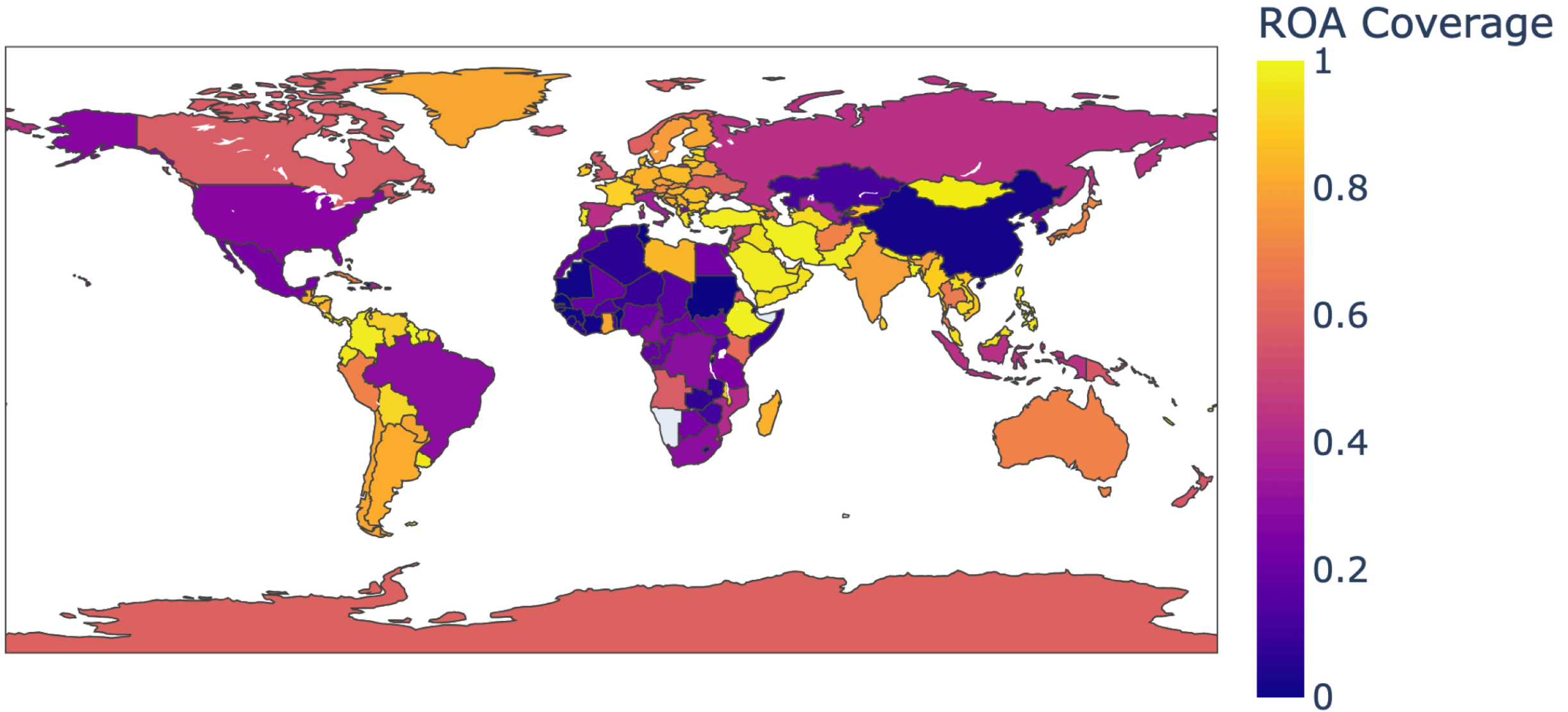
- In 2024, about 50% of IP address blocks advertised in BGP are still not covered by RPKI records
  - Which types of networks are lagging in RPKI adoption and why?
  - How might policymakers better target and support those lagging networks?
- Data sources:
  - Publicly available routing data
  - RPKI and Internet resources' delegation data from the Regional Internet Registries and the Internet Routing Registries
  - Geolocation data from the Internet Health Report/IIJ

# Results

- Four key characteristics impact organizations' RPKI adoption levels:
  1. Geography
  2. Network size
  3. Business category
  4. Complexity of the address space



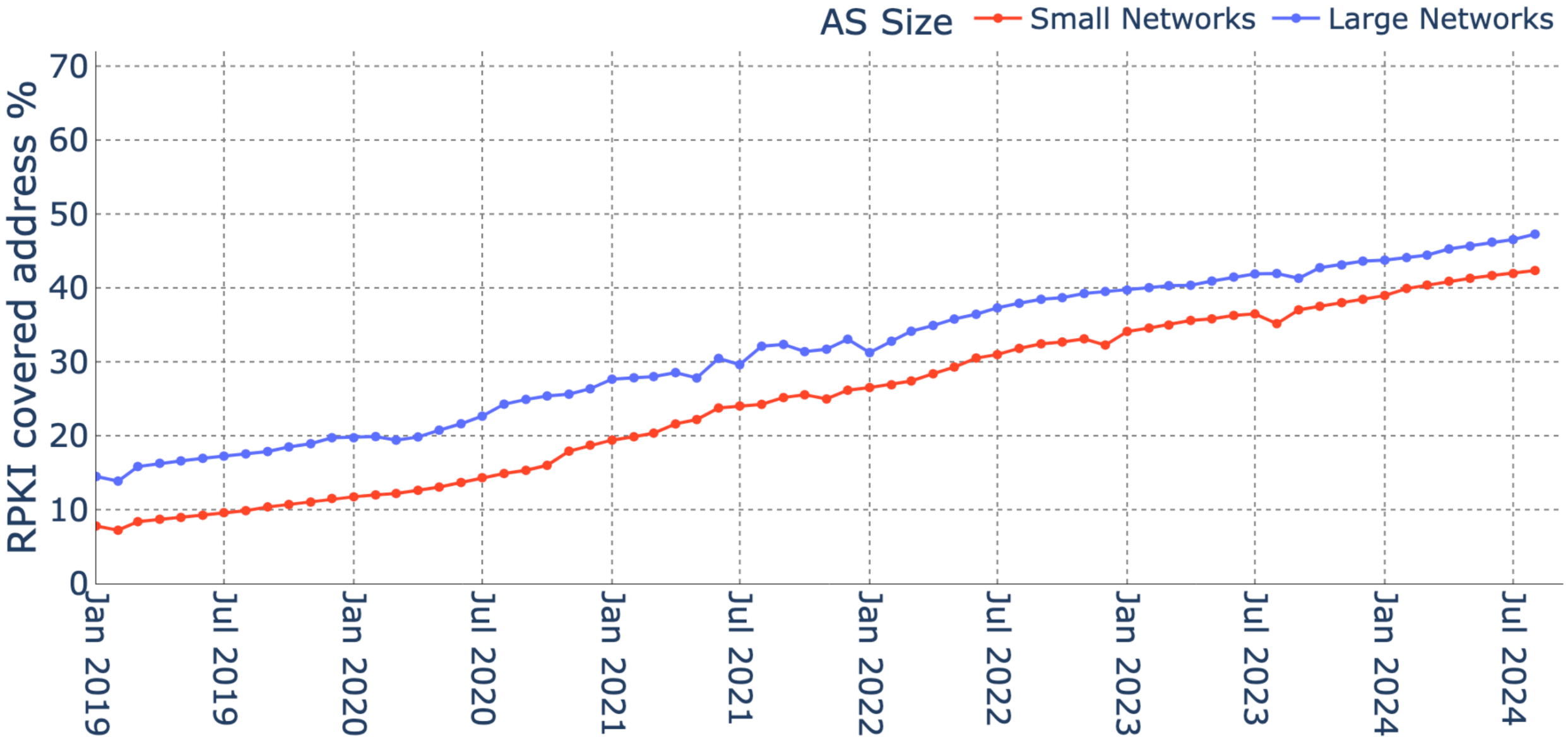
Regional Internet Registries (RIRs) are the root of trust to verify the cryptographic validity of RPKI records. Each RIR has independently set up the process to issue and publish ROAs in their region



Coverage of countries in January 2024; Middle-east nations have the highest ROA coverage, while China has the lowest coverage among large nations

# Possible explanations

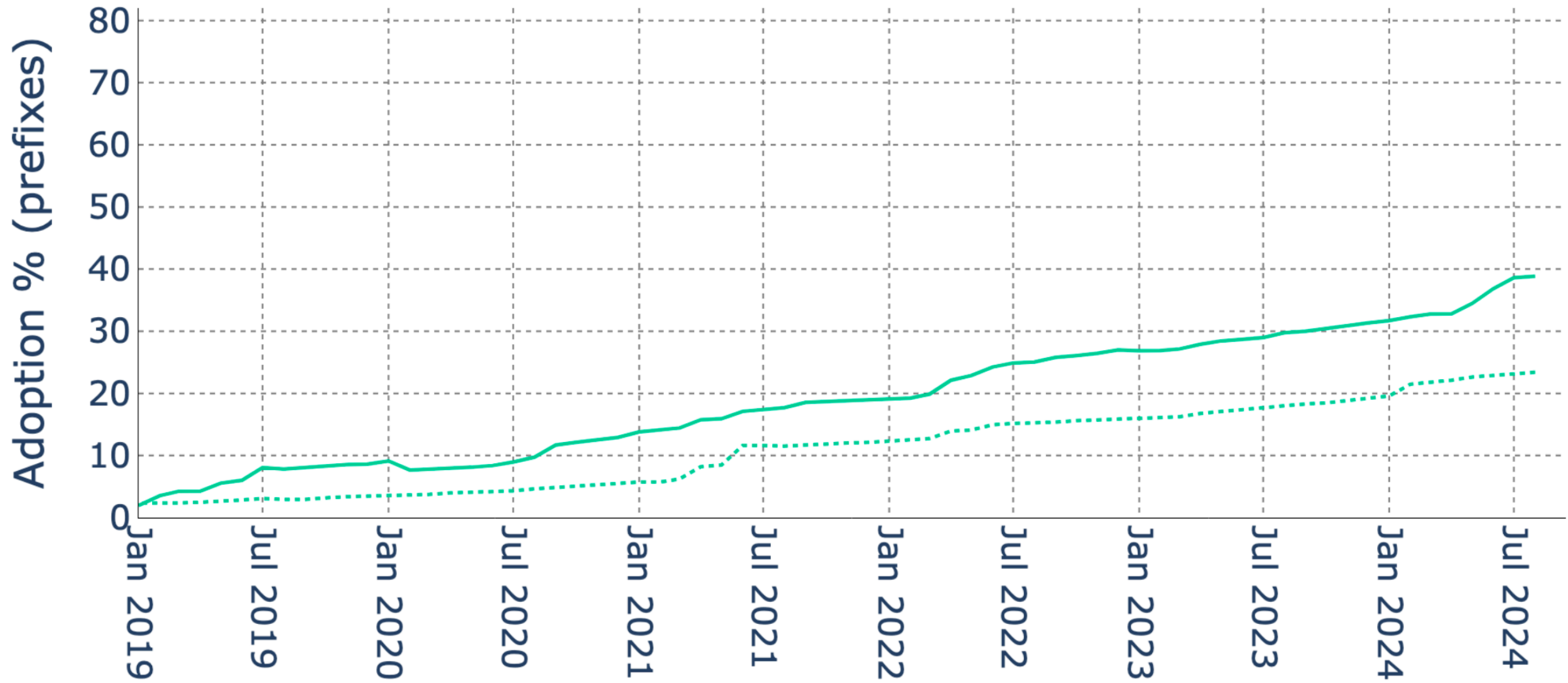
- In the RIPE zone, most countries have over 50% adoption of RPKI
  - Possibly due to RIPE's community efforts to train and promote RPKI adoption as well as the development of tools for RPKI certificate issuance and management
  - Middle Eastern countries including Israel, Turkey, Iraq, Iran, Lebanon, Oman, Saudi Arabia exhibit more than 90% RPKI adoption, possibly due to market concentration of network operators at a country level
- In the LACNIC zone, most countries have more than 80% RPKI adoption possibly due to proactive initiatives led by LACNIC, including training and pushing RPKI registration



Lack of incentives and awareness, as well as the complexity of operationalizing the issuance of RPKI ROAs may deter smaller networks



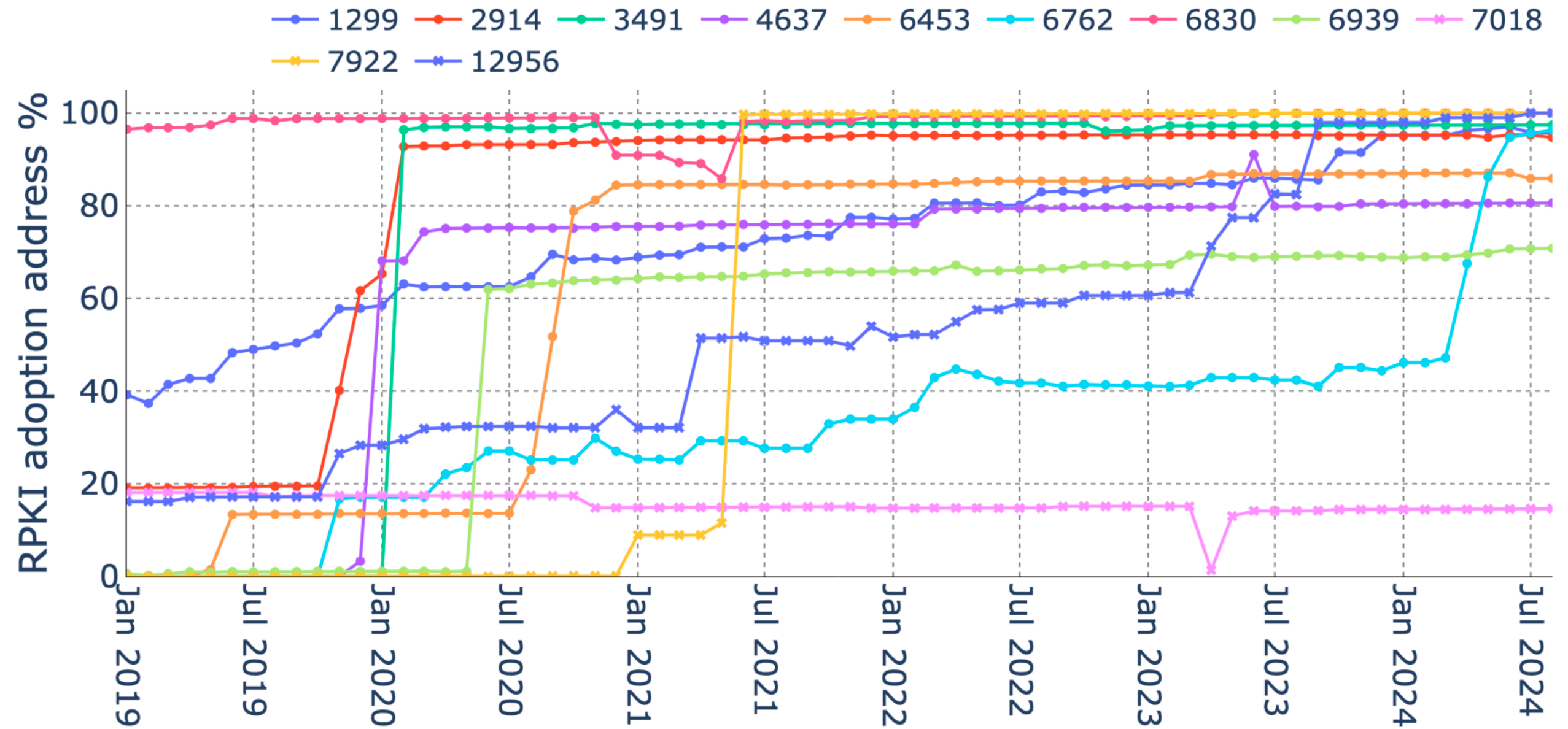
ARIN : AS Size    ⋯ Small Networks    — Large Networks



## RPKI coverage of address space originated by networks (ASNs) from select BGP.Tools and ASdb categories

BGP.Tools labels	RPKI cov.%	ASdb labels	RPKI cov.%
Government	20.3	Gov. and Reg. Agencies <sup>4</sup>	15.5
Academic	23.84	Colleges, Univ., and Prof. Schools	21.99
Mobile Data/Carrier	46.04	Phone Provider	33.34
Server Hosting	51.19	Hosting and Cloud Provider	57.41
Home ISP	45.06	Internet Service Provider (ISP)	44.78
Satellite Internet	85.84	Satellite Comm.	52.05

- Government and academic networks are mostly **small networks** and face the challenges small networks have for RPKI adoption (lack of awareness, training and management tools)
- Networks whose business does not involve Internet services also have **little financial incentive** to adopt RPKI since their users are unlikely to move to a competitor to improve their security stance



IPv4 RPKI adoption over time of selected Tier 1 ASes

# Address Complexity & Delegation

- Tier 1 networks that adopt RPKI more slowly tend to have more complex IP delegation within their address space
- RPKI adoption by the large network requires coordination with the (smaller) networks using the sub-delegations in BGP in order to prevent availability issues in the impacted addresses
- If a large network originates address space that another organization is delegated, the large network cannot create RPKI certificates for that address space (e.g., if an ISP originates address space directly delegated by an RIR to a customer)

# Takeaways for Policymakers

- Small stakeholders need targeted support
- Bottom-up community-driven efforts have paid off
- Additional support is needed for non-ISP networks
- Coordination across the ecosystem is essential to align incentives or pair effort levels between larger transit networks and smaller ISPs, as well as between network providers and their customers with direct IP address delegations

# Questions