Routing Security:

A Global Perspective with a Spotlight on Iran and Central Asia

Milad Afshari
CAPIF3
September, 2024

Who am I ?

- Milad Afshari
- Enterprise Network Planning Manager @ MTN-Irancell(AS44244)
- Co-founder & PC chair of IRNOG
- PC member of CAPIF

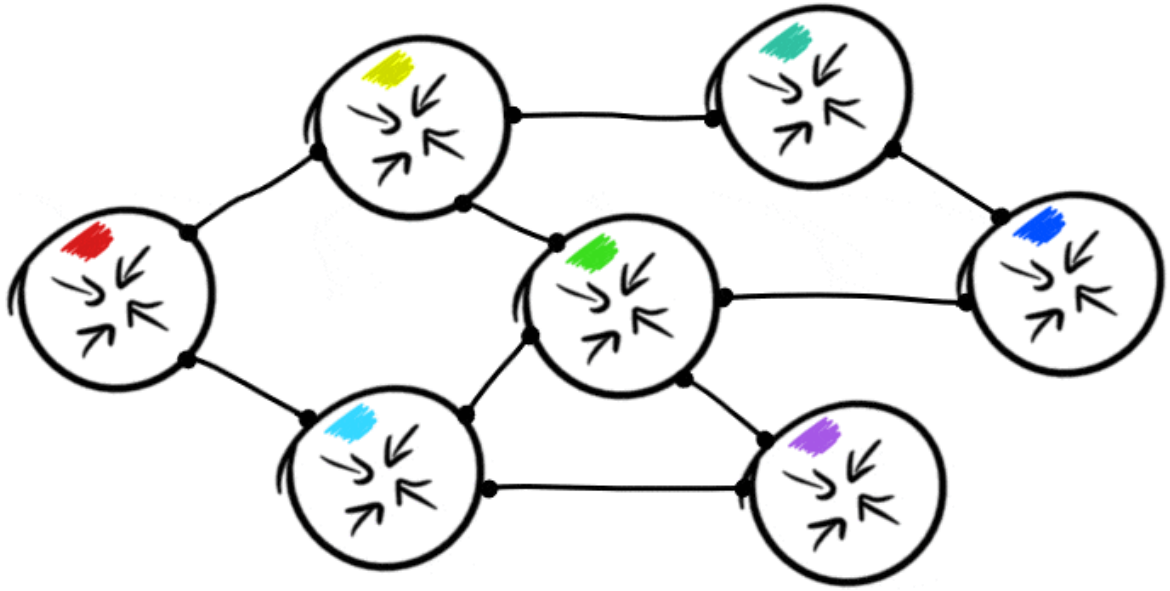
Agenda

- Introduction and history to the BGP and routing vulnerabilities
- Avoidance mechanisms (MANRS)
- Statistics in Iran and Central Asia
- Conclusion
- References

BGP & Routing Vulnerabilities

BGP Protocol

- The Border Gateway Protocol(BGP) has been **essential for the operation of the Internet** for nearly 30 years, but it has come with security challenges.
- BGP was originally designed when the **Internet was much smaller** and based on a **trust model** between network operators, so the protocol has no built-in security mechanisms to address accidental or malicious configurations.



What are Routing Incidents?

Event	Explanation	Repercussions	Solution
Prefix/Route Hijacking	A network operator or attacker impersonates another network operator, pretending that a server or network is their client.	Packets are forwarded to the wrong place; this can cause Denial of Service (DoS) attacks or traffic interception.	Stronger filtering policies
Route Leak	A network operator with multiple upstream providers announces (often due to accidental misconfiguration) to one upstream provider that is has a route to a destination through the other upstream provider.	Can be used for traffic inspection and reconnaissance.	Stronger filtering policies
IP Address Spoofing	Someone creates IP packets with a false source IP address to hide the identity of the sender or to impersonate another computing system.	The root cause of reflection DDoS attacks.	Source address validation

Routing Incidents Cause Real World Problems

- Insecure routing is one of the most common paths for malicious threats.
- Attacks can take anywhere from hours to months to recognize.
- Inadvertent errors can take entire countries offline, while attackers can steal an individual's data or hold an organization's network hostage.

History of some BGP Incidents!

AS7007 Incident

- **Event:** Software bug led to a large part of IP address ranges being misannounced as originating from AS7007.
- **Impact:** Traffic was redirected and overwhelmed AS7007's equipment, causing widespread disruption.

Pakistan Telecom and YouTube

Event: Pakistan Telecom attempted to block YouTube locally but accidentally propagated the block globally.

Impact: Global internet access to YouTube was disrupted.

Belarus BGP MITM Attack

Event: BGP-based man-in-the-middle attack targeting major US credit card companies and governments.

Impact: Interception of sensitive communications.

MyEtherWallet Attack

Event: BGP hijacking led to DNS redirection and phishing of cryptocurrency wallets.

Impact: $17 million stolen from users due to compromised TLS connections.

1.1.1.1 Route Leak

Event: The issue started on June 27, when Eletronet S.A. (AS267613) mistakenly announced a very specific route (1.1.1.1/32) to its peers and upstream providers.

Impact: The incident impacted around 300 networks across 70 countries, though Cloudflare noted that the overall impact was relatively low and many users did not notice significant disruption.

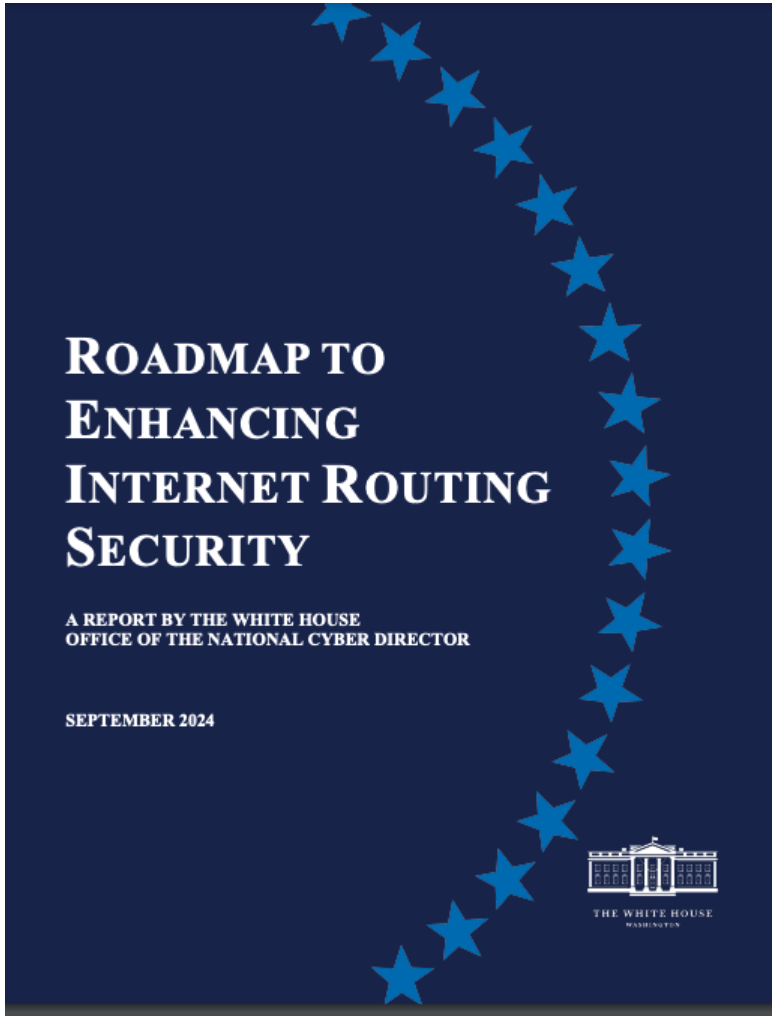
Importance of the Internet Routing Security

In September 2024, the White House's Office of the National Cyber Director released the **White House's Roadmap to Enhancing Routing Security**. This is another important step toward strengthening the Internet's routing system in the United States and improvement within the US would have global effects on the Internet.

The Roadmap also recognizes that **US government's federal networks** still have a lot of work to do in terms of routing security.

	August 2023	August 2024
Valid	87	215
Unknown	15,755	17,788
Invalid	2	2

Figure 1. Route Announcements with RPKI validated prefixes from August 2023 to August 2024, US Federal Networks. Data collected from the MANRS Observatory.



Tools to Help

- Prefix and AS-PATH filtering
- RPKI validator, IRR toolset, BGPQ3
- BGPSEC

But…

- Not enough deployment
- Lack of reliable data

Avoidance Mechanisms (MANRS)

The Role of the MANRS Community

- Mutually Agreed Norms for Routing Security (MANRS) is a global, **community-driven initiative**. In 2014, a small group of network operators recognized the need to join forces to **improve the security and resilience of the Internet's global routing system**. With support from the Internet Society, MANRS was born.
- MANRS improves the security and reliability of the global Internet routing system, based on collaboration among participants and shared responsibility for the Internet infrastructure.

MANRS

MANRS Programs

Network Operators

Internet Exchange Points (IXPs)

Content Delivery Networks (CDNs) and Cloud Providers

MANRS Actions for Network Operators

Filtering

Prevent propagation of incorrect routing information

Ensure the correctness of your own announcements and announcements from your customers to adjacent networks with prefix and AS-path granularity

Anti-spoofing

Prevent traffic with spoofed source IP addresses

Enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure

Coordination

Facilitate global operational communication and coordination between network operators

Maintain globally accessible, up-to-date contact information in common routing databases

Global Validation

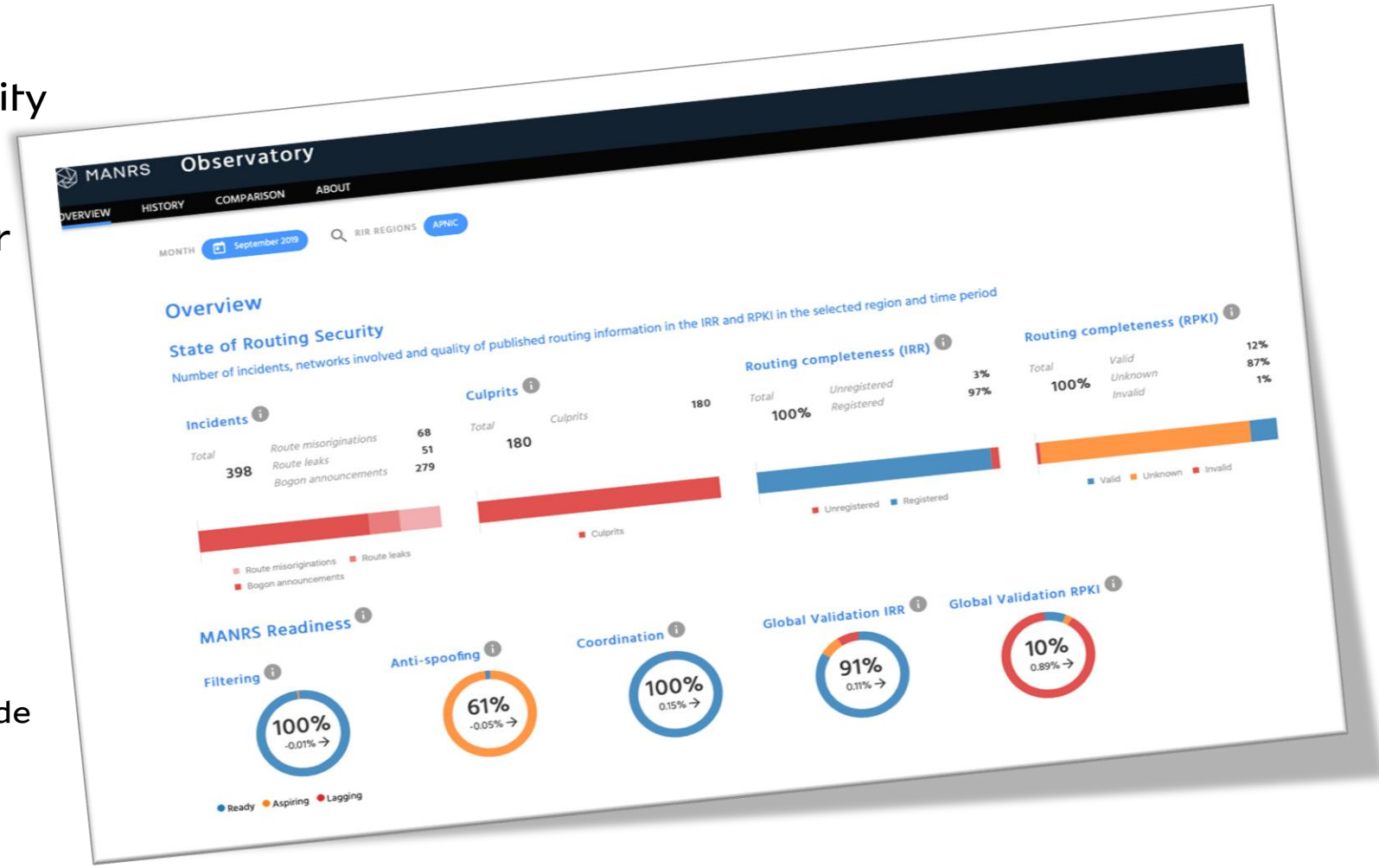
Facilitate validation of routing information on a global scale

Publish your data so others can validate

Blue shading = Mandatory Action

MANRS Observatory

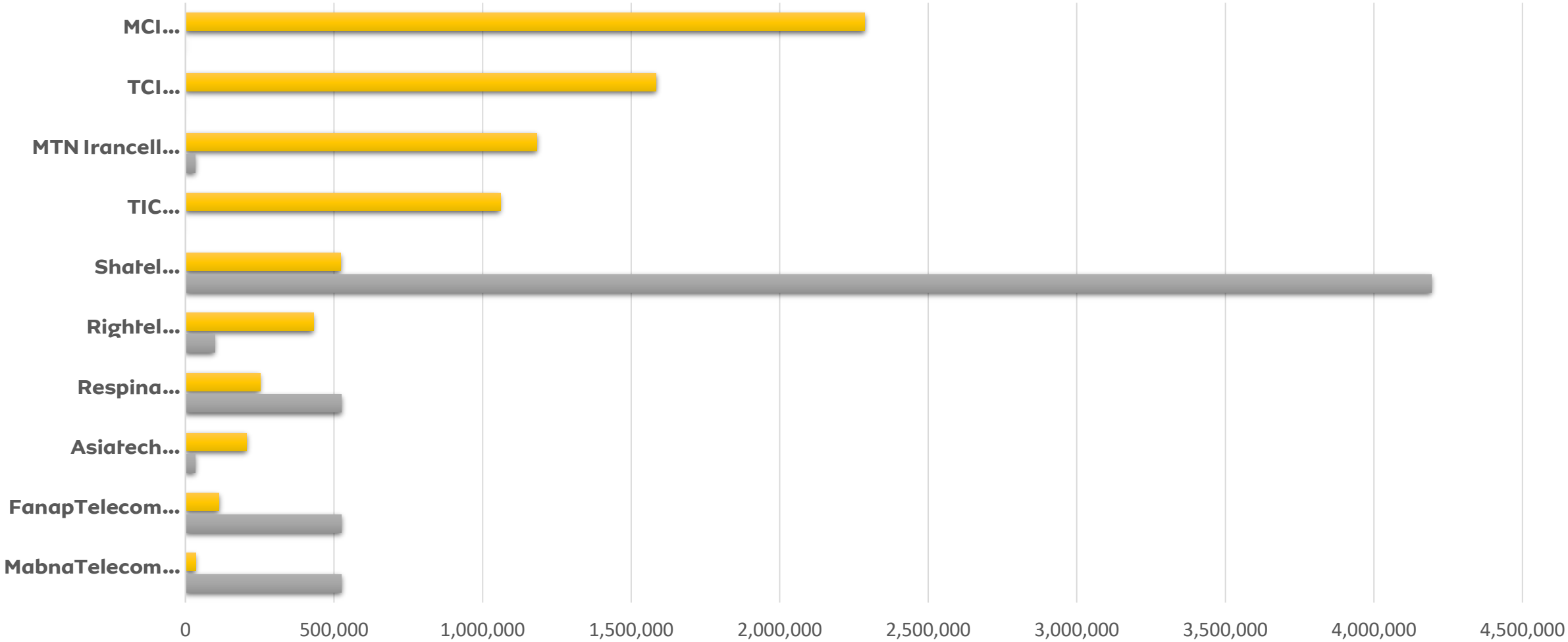
- Provide a factual state of security and resilience of the Internet routing system and track it over time
- Measurements are:
  - Transparent – using publicly accessible data
  - Passive – no cooperation from networks required
  - Evolving – MANRS community decide what gets measured and how



Statistics
(Iran and Central Asia)

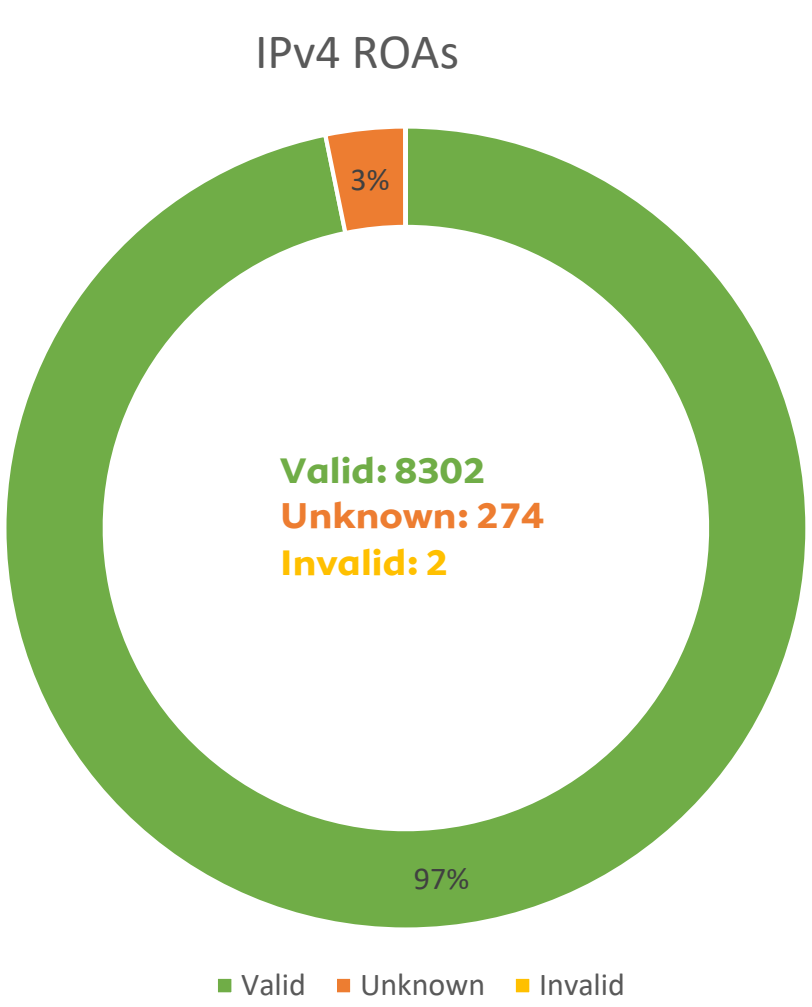
Iran

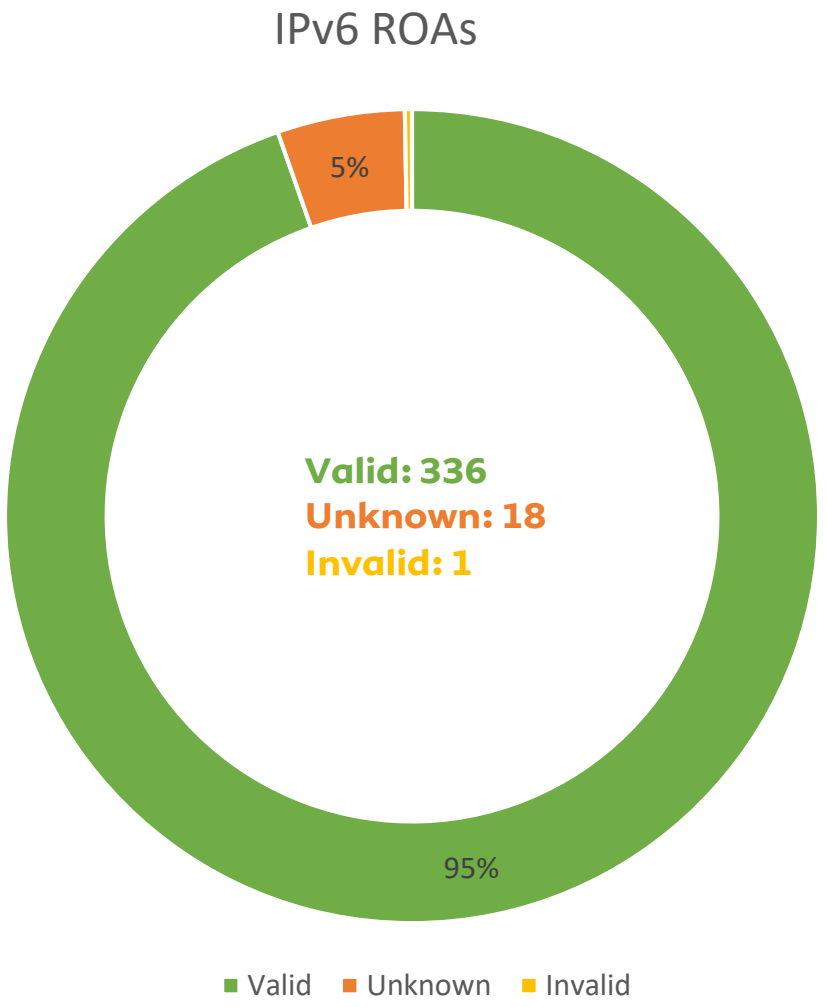
Announced IPv4/IPv6 (Top10)



	MabnaTelecom (AS51074)	FanapTelecom (AS24631)	Asiatech (AS43754)	Respina (AS42337)	Rightel (AS57218)	Shatel (AS31549)	TIC (AS12880, AS49666)	MTN Irancell (AS44244)	TCI (AS58224)	MCI (AS197207)
Announced IPv4	34,304	112,640	205,312	251,904	431,104	523,008	1,060,096	1,182,720	1,584,640	2,286,592
Announced IPv6 (/48)	524,288	524,288	32,768	524,289	98,305	4,194,304	1	32,768	2	1,025

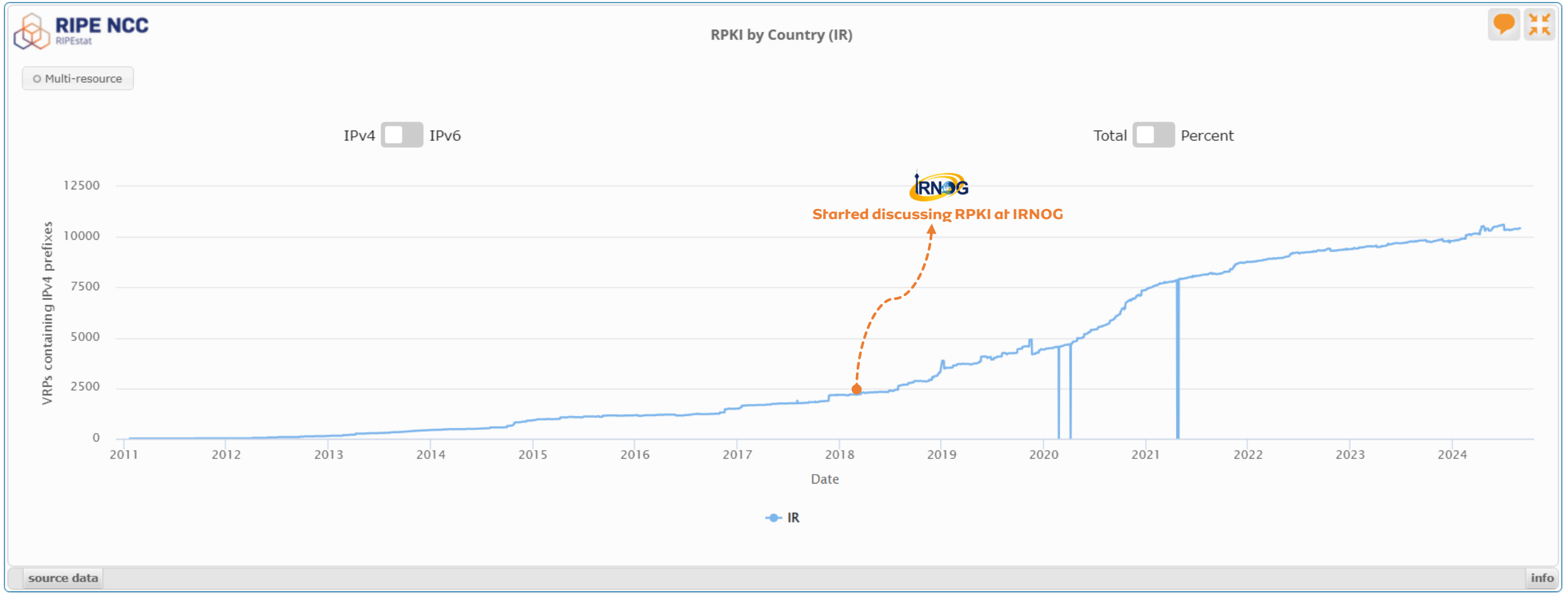
IR ROA Stats





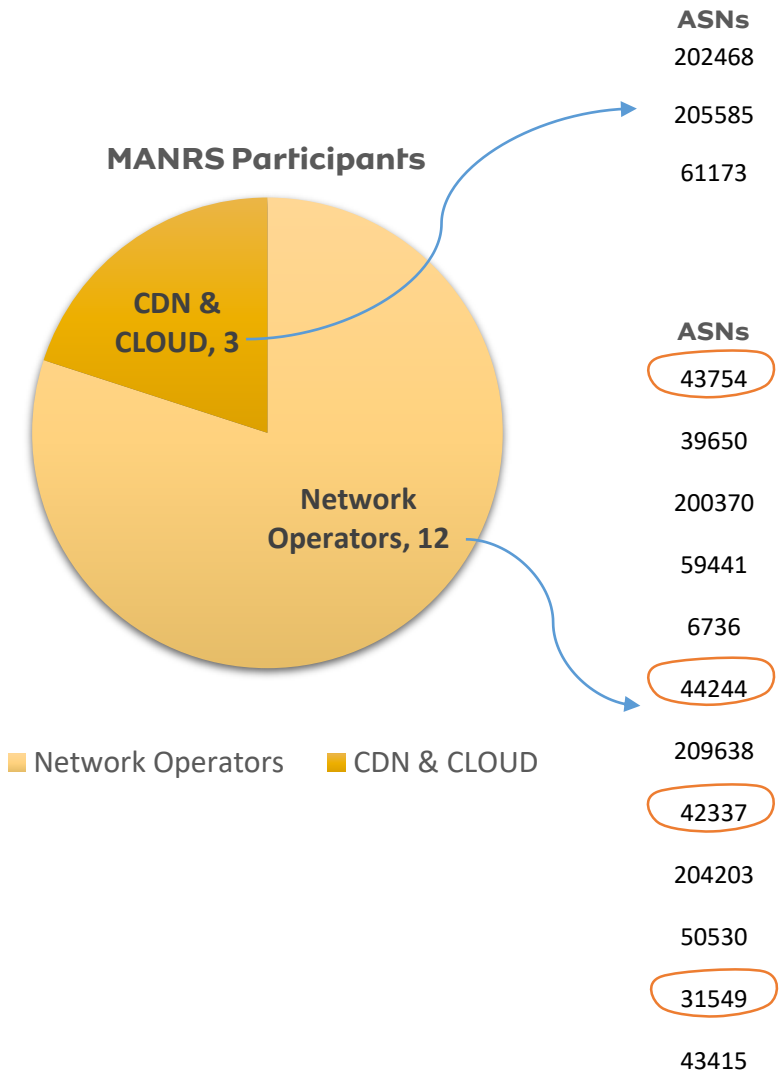
https://observatory.manrs.org/#/roas/country/ir

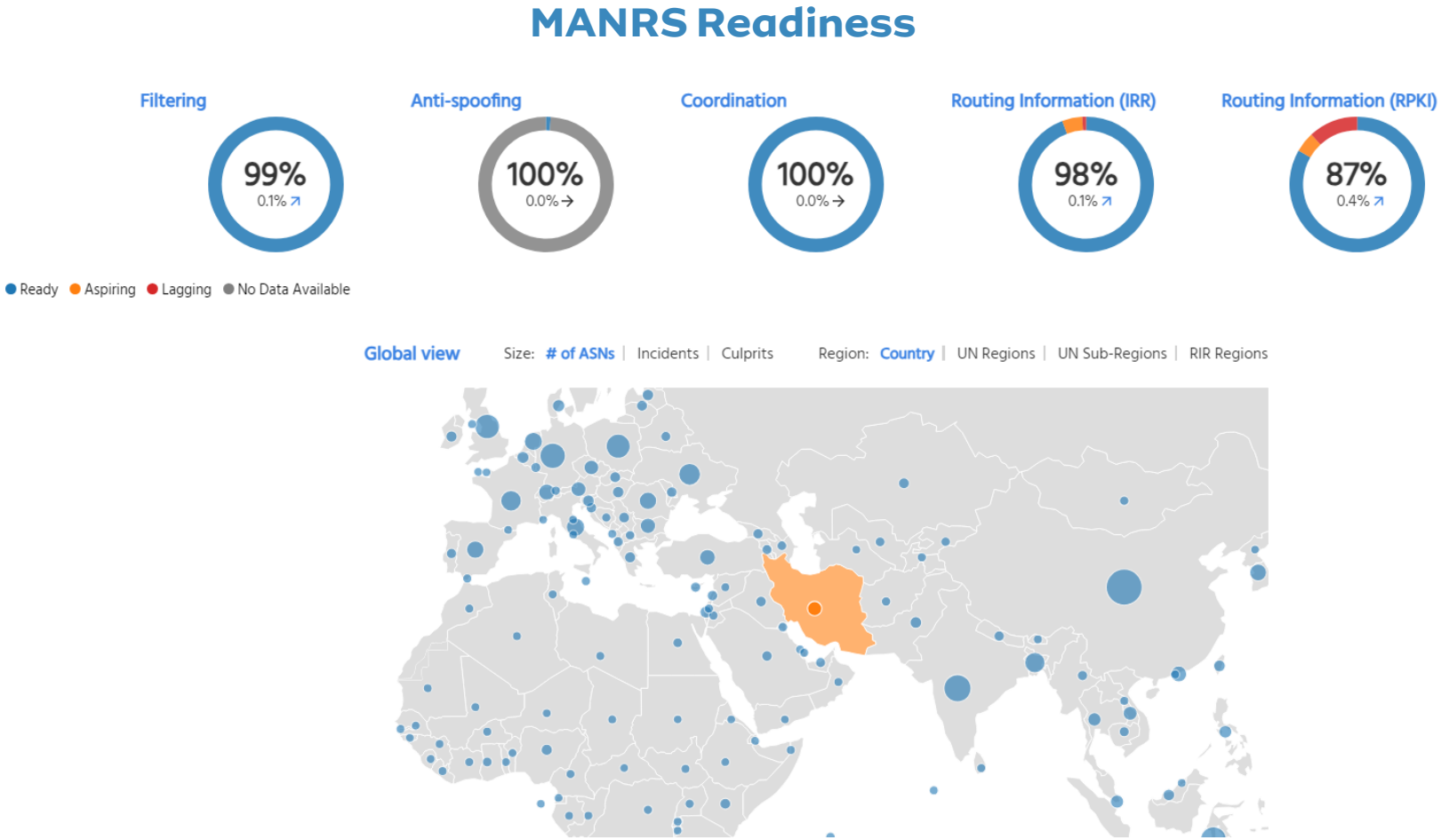
IR IPv4 RPKI



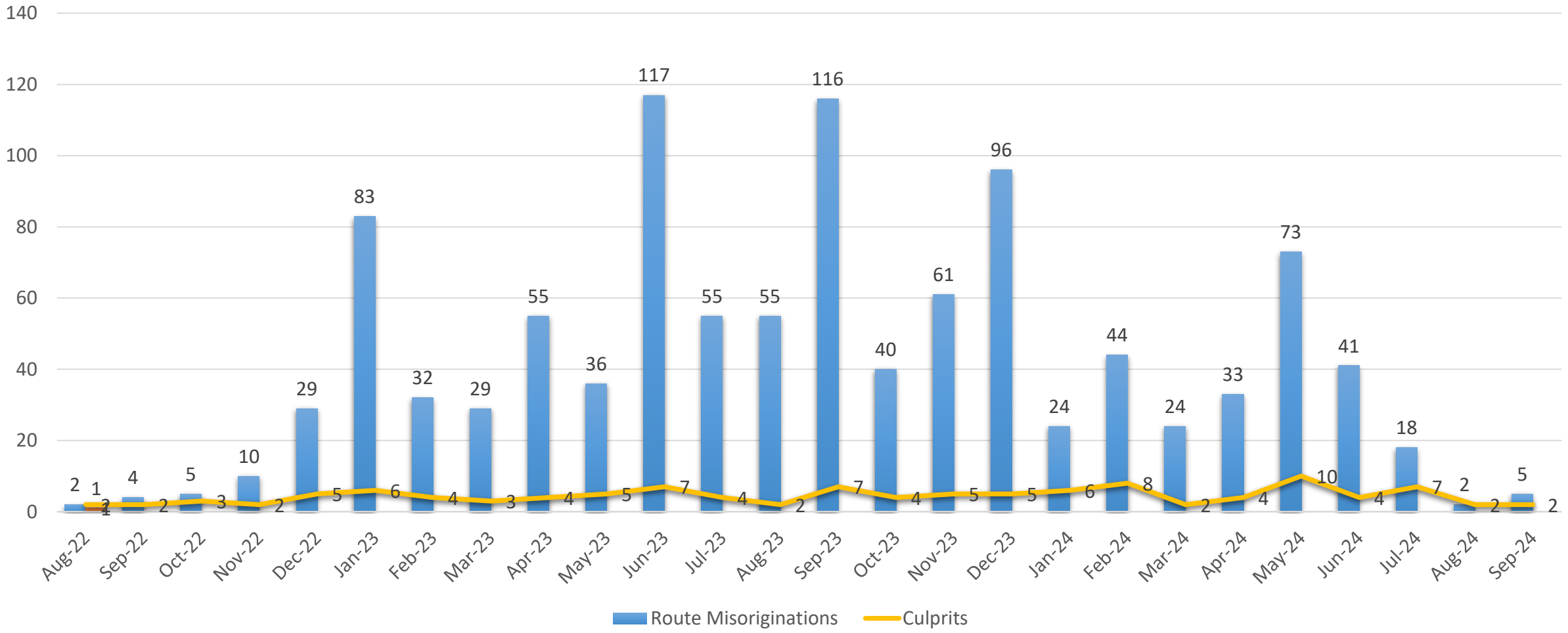
https://stat.ripe.net/ui2013/widget/rpki-by-country#w.resource=IR

IR MANRS Stats



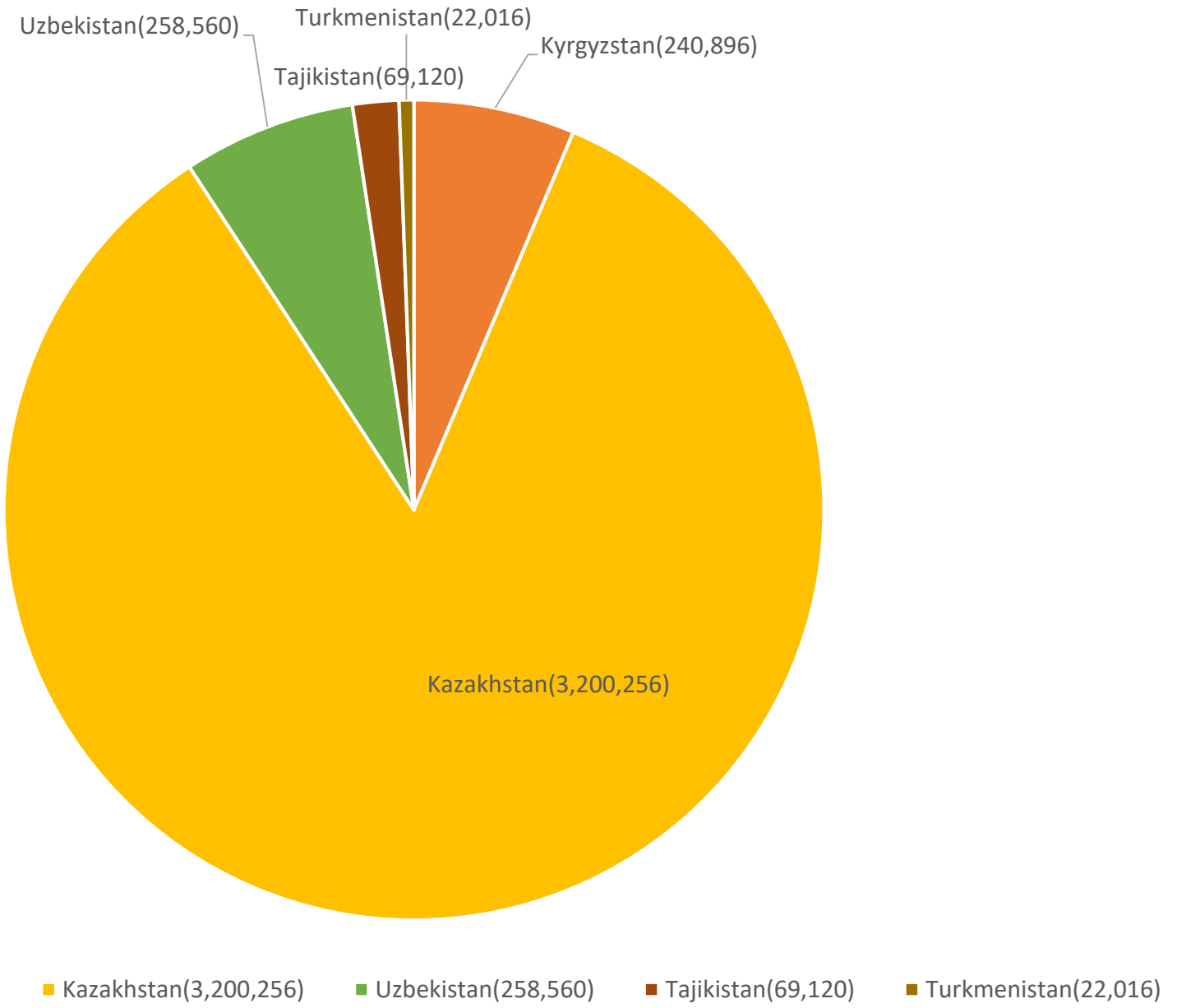


IR Routing Incidents

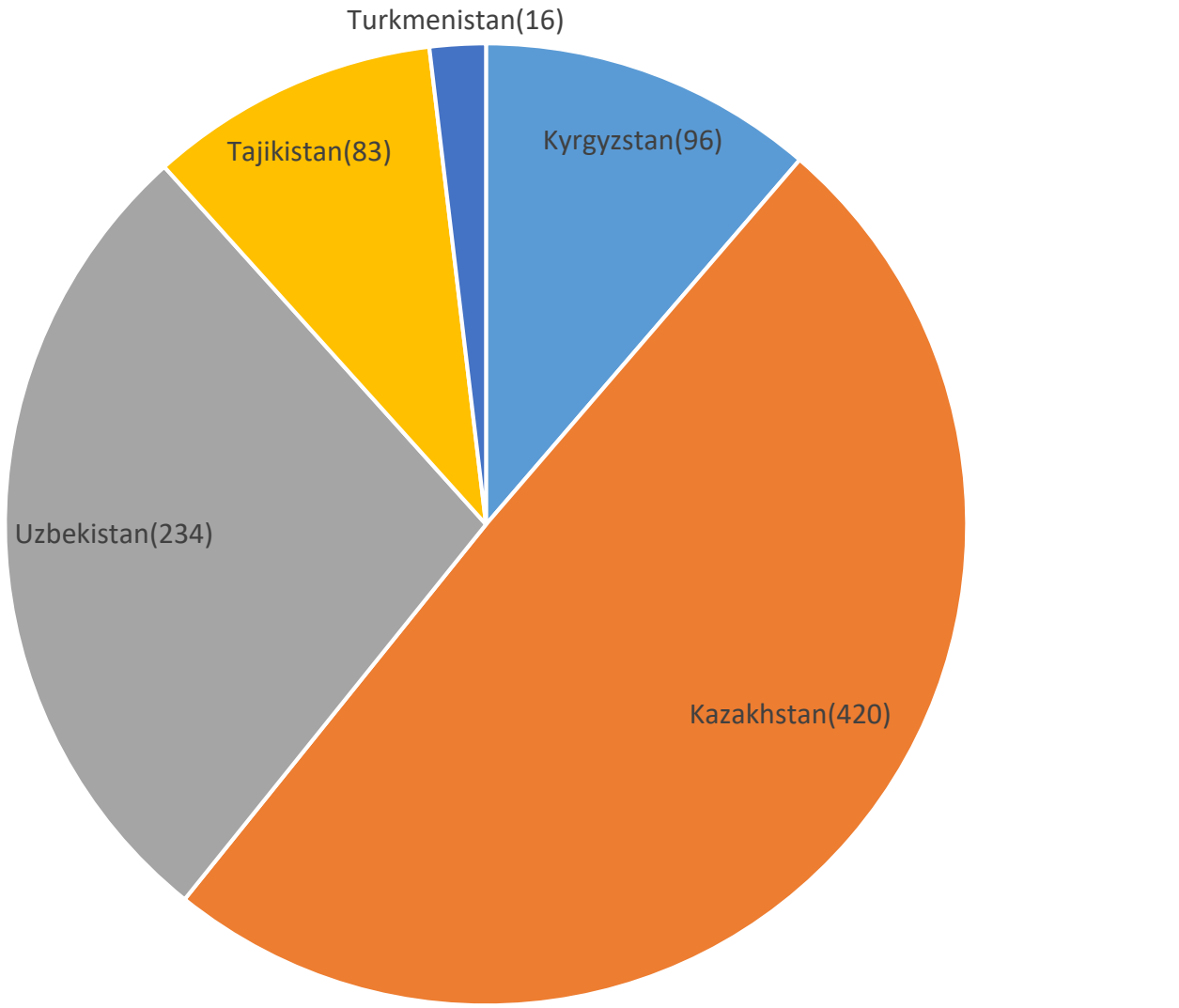


Central Asia

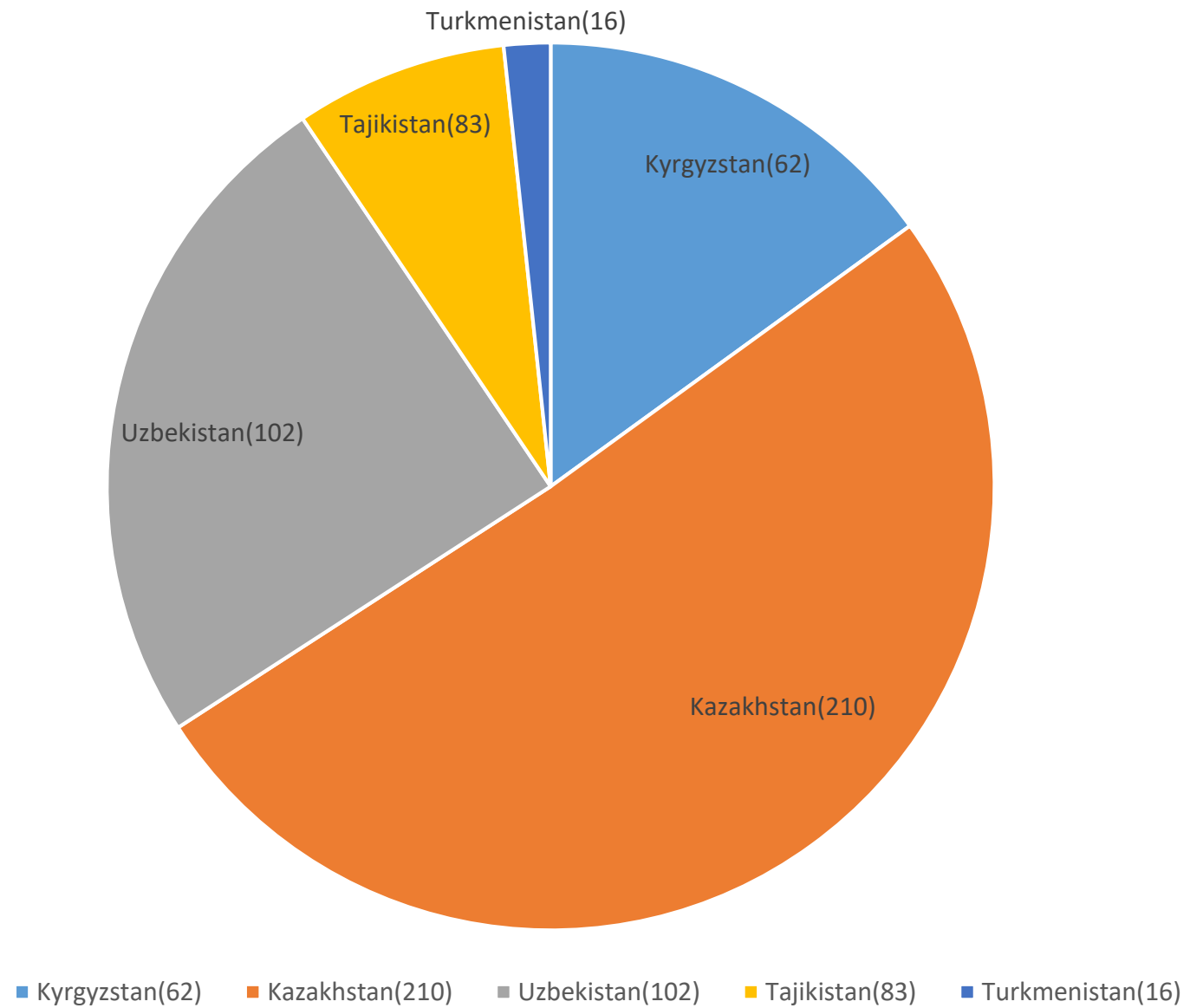
IPv4


Uzbekistan(258,560)
Turkmenistan(22,016)
Kyrgyzstan(240,896)
Tajikistan(69,120)
Kazakhstan(3,200,256)
Kyrgyzstan(240,896)
Kazakhstan(3,200,256)
Uzbekistan(258,560)
Tajikistan(69,120)
Turkmenistan(22,016)

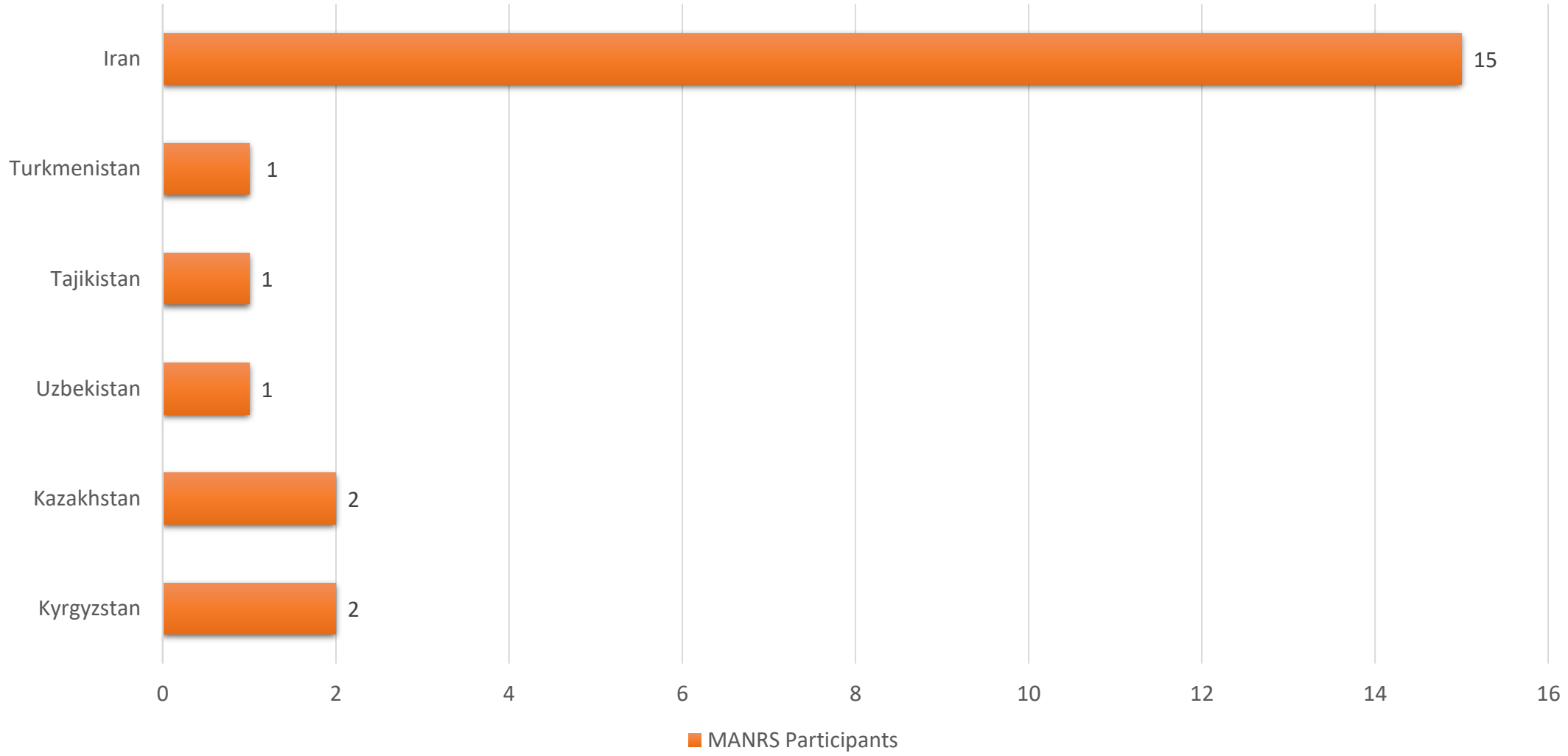
IPv6 (/32)


Turkmenistan(16)
Kyrgyzstan(96)
Tajikistan(83)
Uzbekistan(234)
Kazakhstan(420)
Kyrgyzstan(96)
Kazakhstan(420)
Uzbekistan(234)
Tajikistan(83)
Turkmenistan(16)

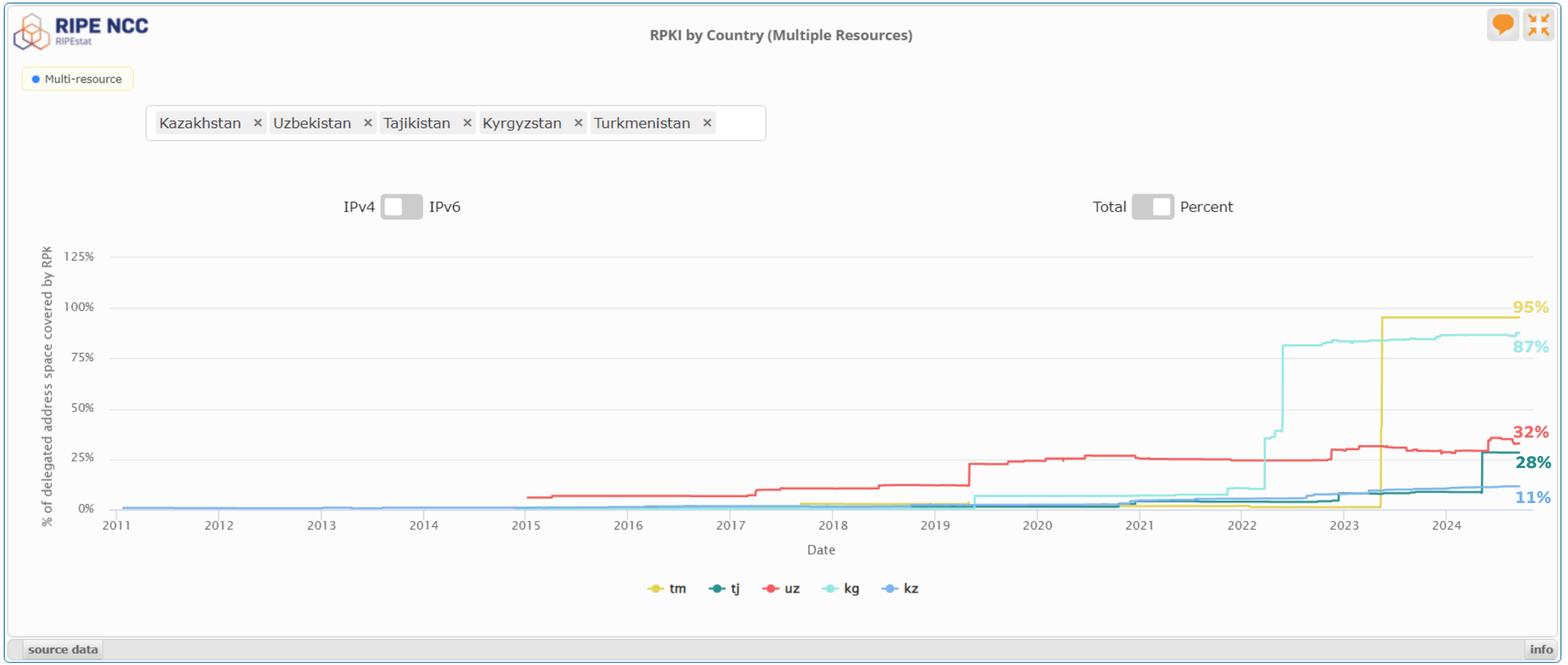
ASNs


Turkmenistan(16)
Tajikistan(83)
Kyrgyzstan(62)
Uzbekistan(102)
Kazakhstan(210)
Kyrgyzstan(62)
Kazakhstan(210)
Uzbekistan(102)
Tajikistan(83)
Turkmenistan(16)

MANRS Participants (Central Asia and IR)

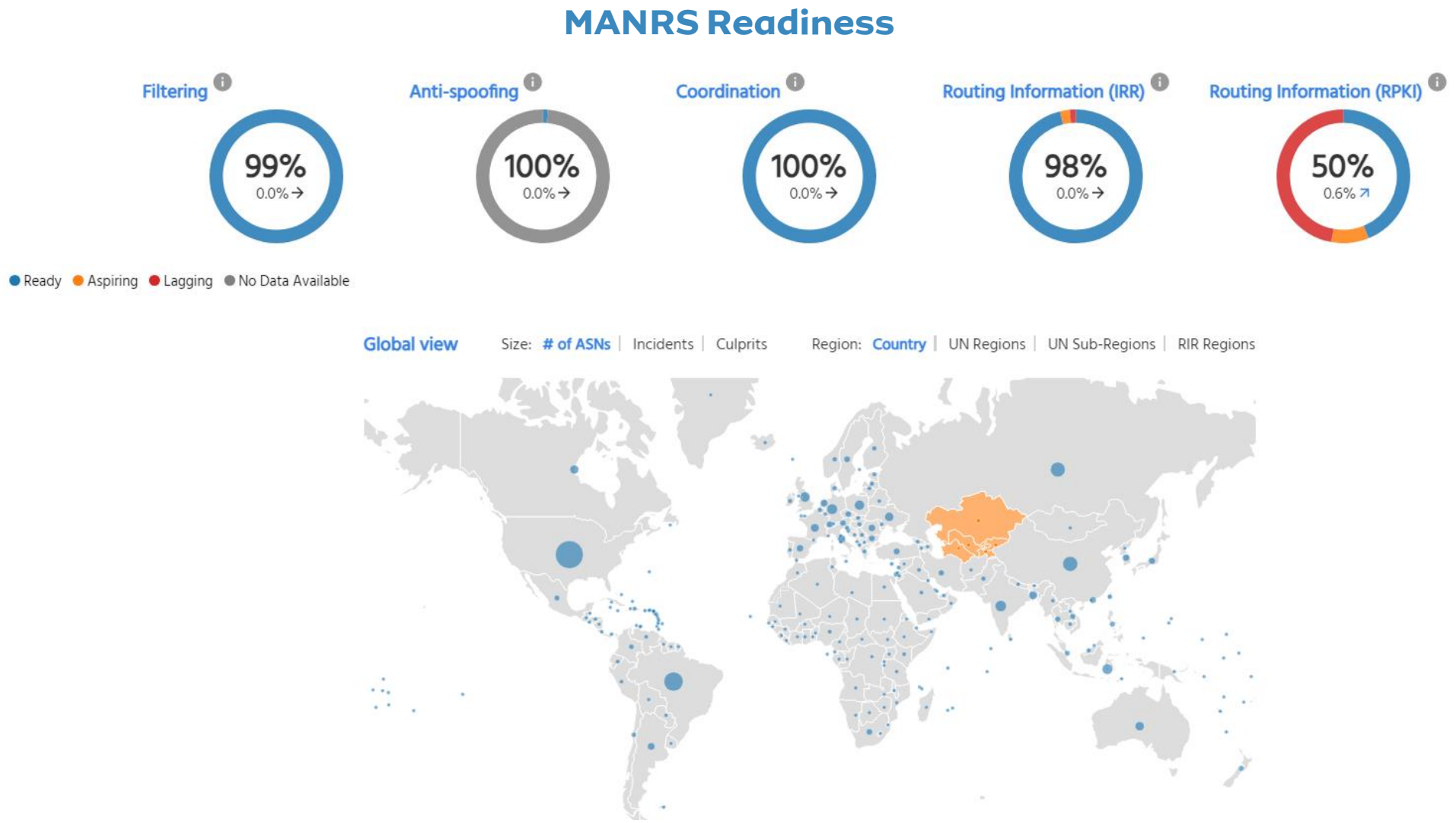


Central Asia IPv4 RPKI

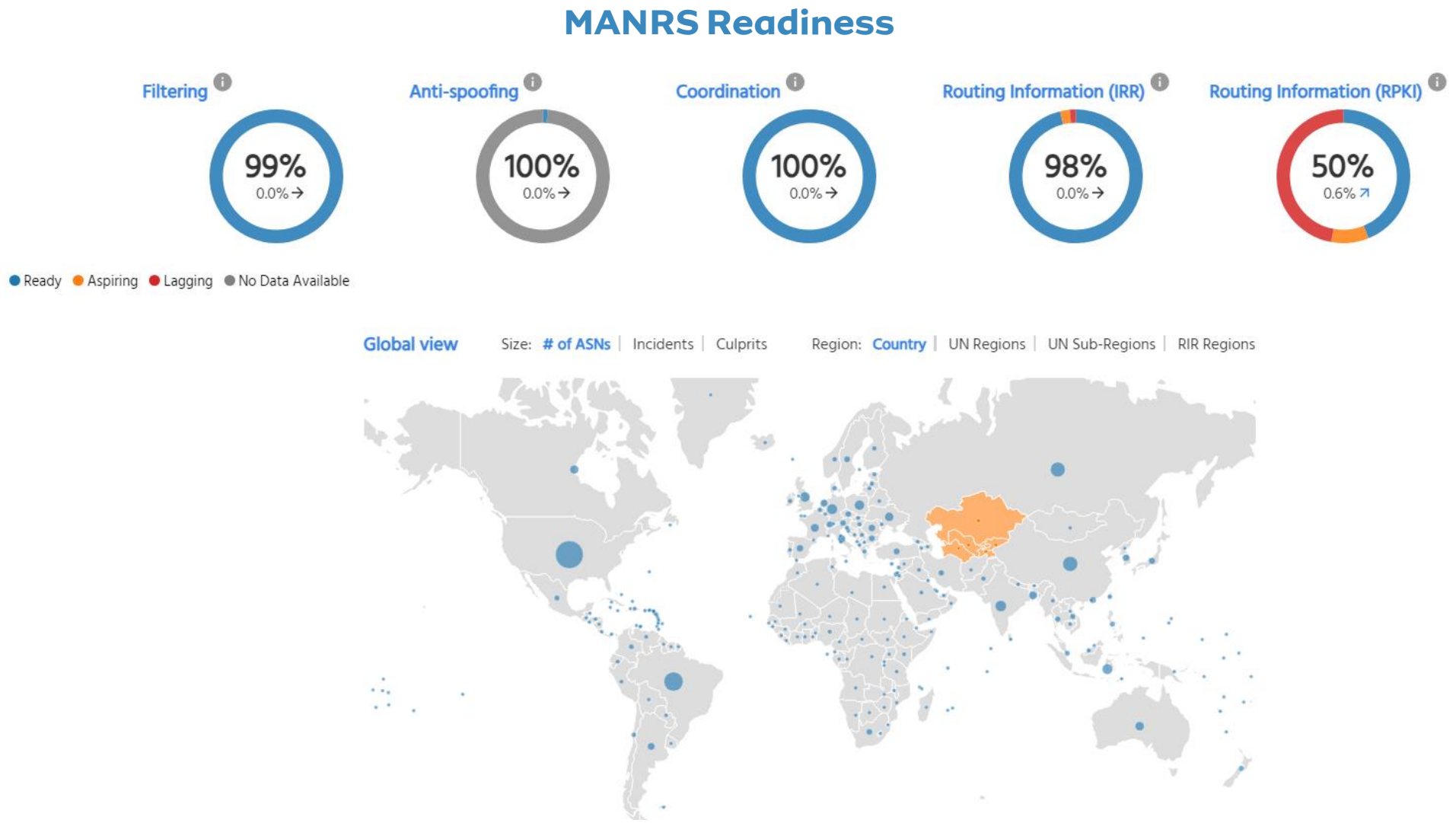


https://stat.ripe.net/ui2013/widget/rpki-by-country

Central Asia MANRS Stats

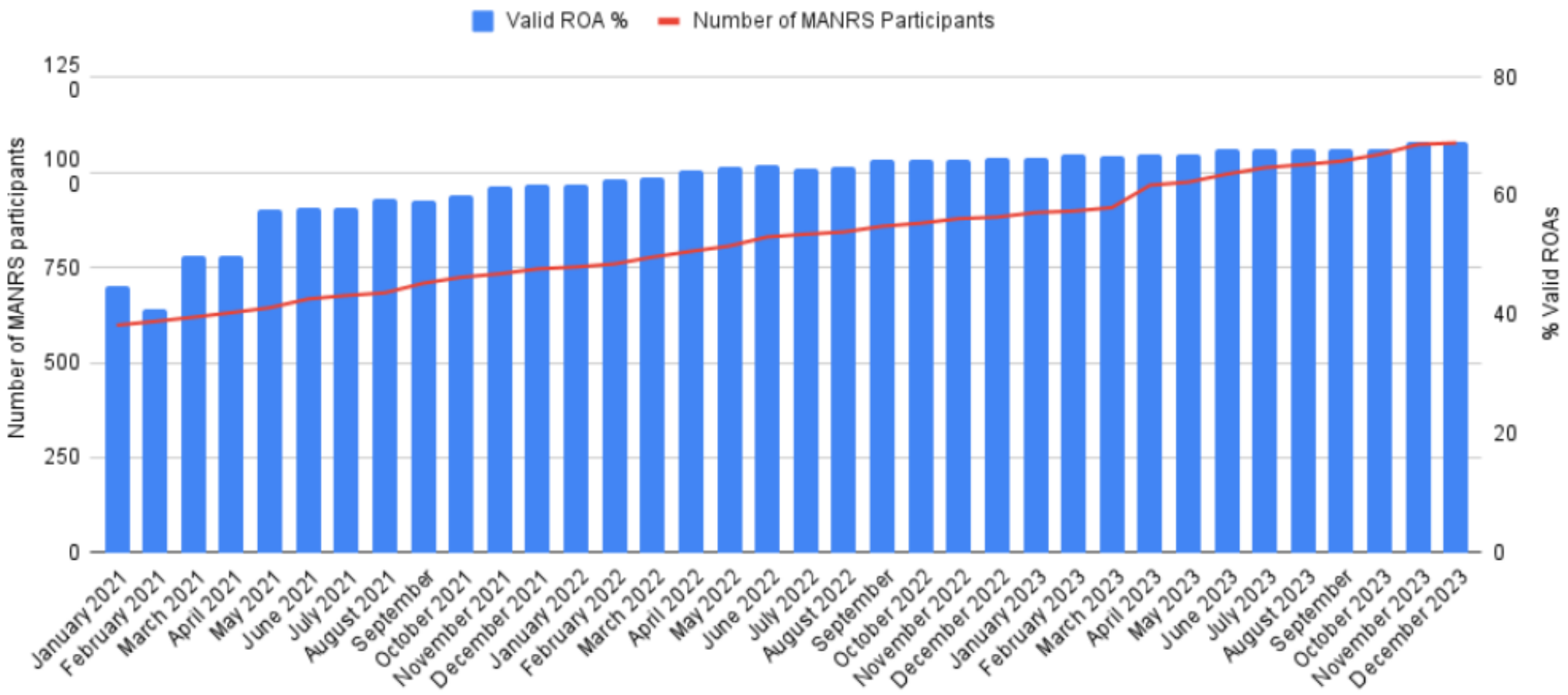


Central Asia MANRS Stats



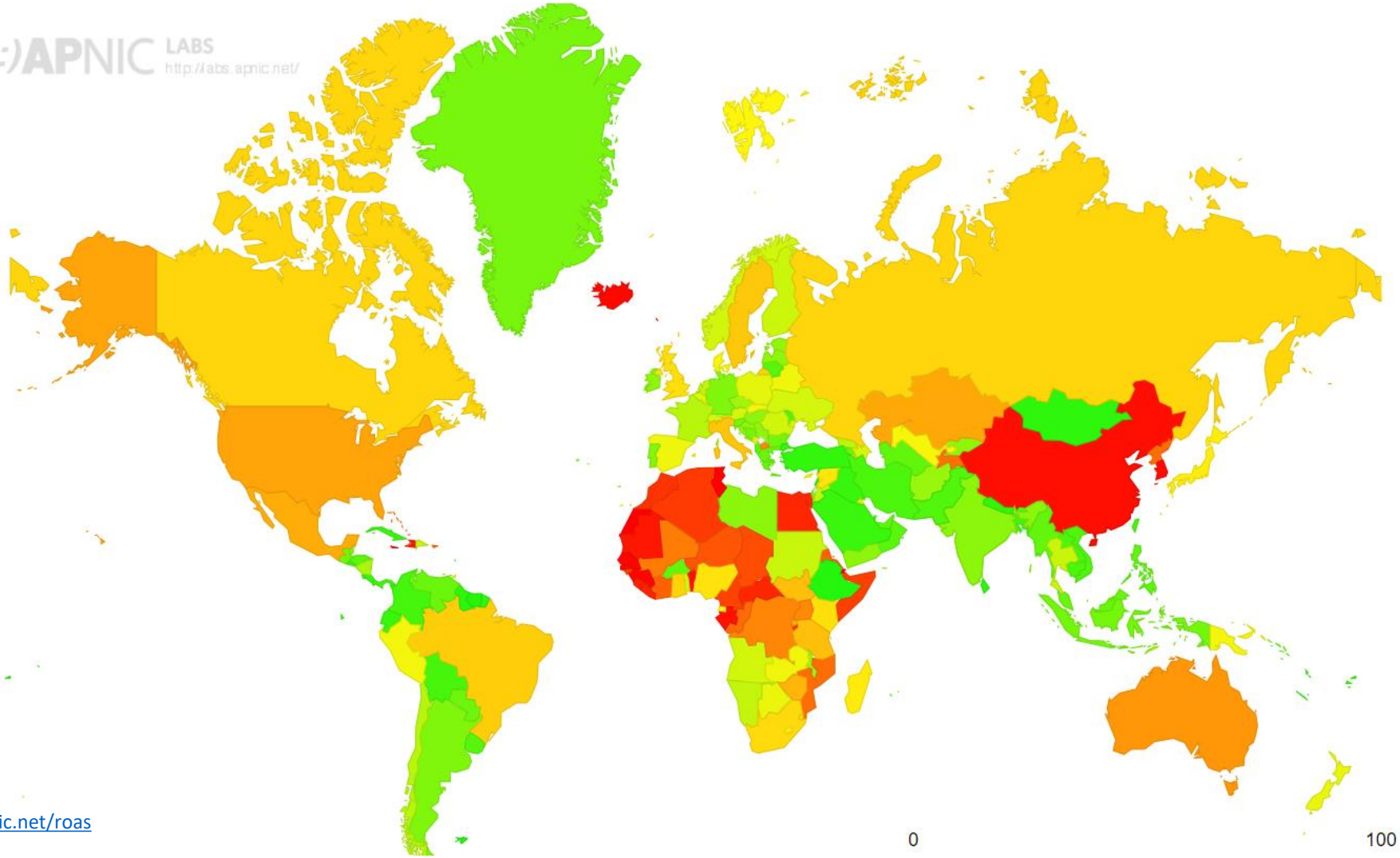
World Stats.

MANRS Impact in 2023



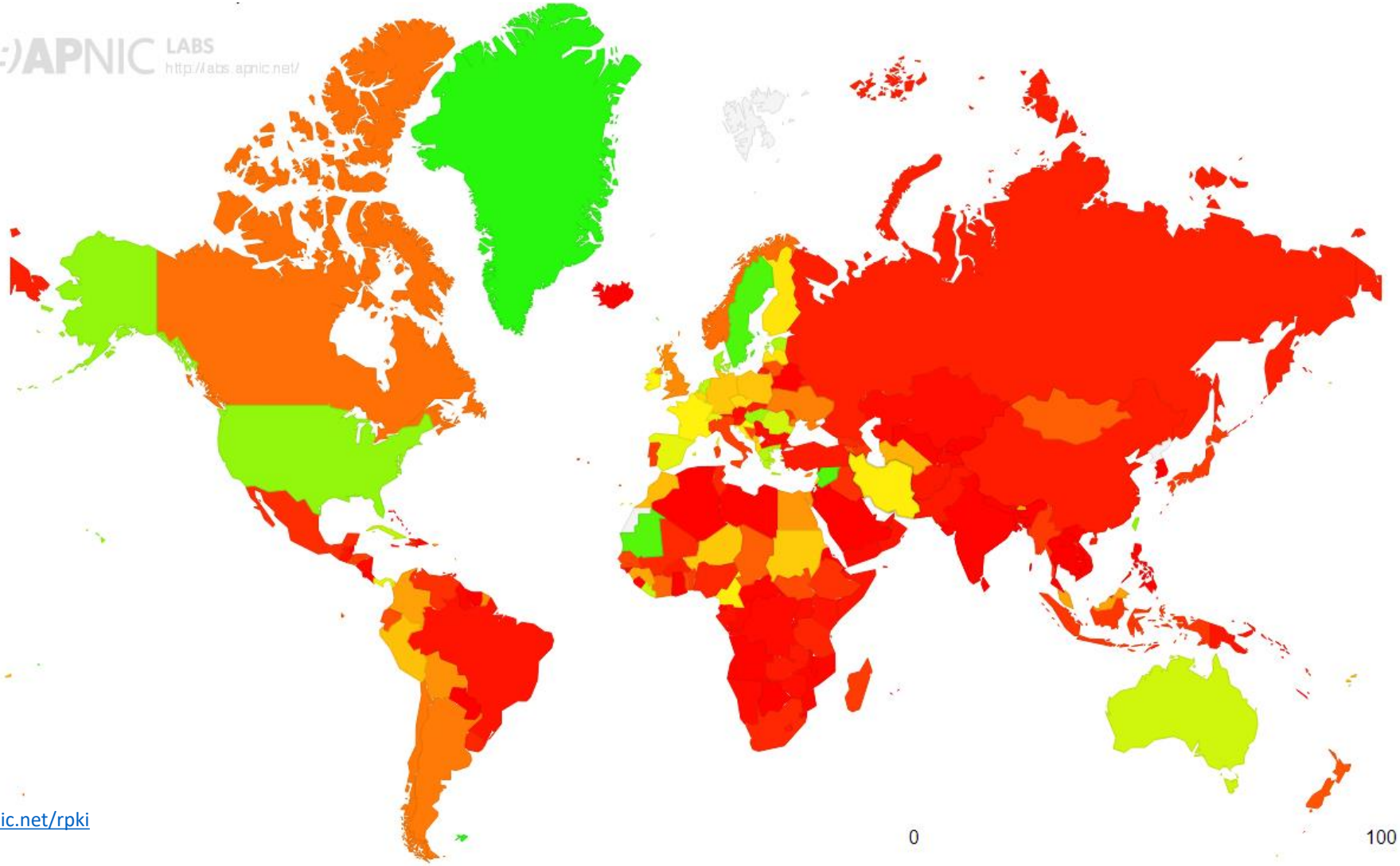
https://manrs.org/wp-content/uploads/2024/01/MANRS-Community-Report_2023.pdf

RPKI ROA Publication



https://stats.labs.apnic.net/roas

Route Origin Validation (ROV)



https://stats.labs.apnic.net/rpki

Conclusion

- **RPKI ROV** remains the most effective defense against accidental BGP hijacks and origin leaks.
  - Steps for success:
    1. Creation of ROAs (Route Origin Authorizations).
    2. ASes (Autonomous Systems) rejecting routes inconsistent with ROAs.
- **Security is a process**, not a final state.
  - The MANRS initiative provides a structured and collaborative approach to addressing Internet routing security challenges.
- **Local Communities (NOGs)**:
  - Network Operator Groups (NOGs) play a crucial role in fostering collaboration, knowledge sharing, and capacity building, which are essential to improving routing security in their regions.
  - Their involvement is key to increasing RPKI adoption and encouraging best practices in routing security.
- **Regional Progress:** While there are advances, **Iran and Central Asia** still face challenges in RPKI adoption and MANRS participation.

References

- https://www.kentik.com/blog/a-brief-history-of-the-internets-biggest-bgp-incidents/
- https://academy.ripe.net/
- https://stat.ripe.net/
- https://observatory.manrs.org/
- https://manrs.org/2024/09/roadmap-to-routing-security/
- https://www.internetsociety.org/blog/2024/09/white-house-roadmap-tackles-routing-vulnerabilities/
- https://manrs.org/wp-content/uploads/2024/01/MANRS-Community-Report_2023.pdf
- https://labs.apnic.net/measurements/

Thank you!
Any Questions?