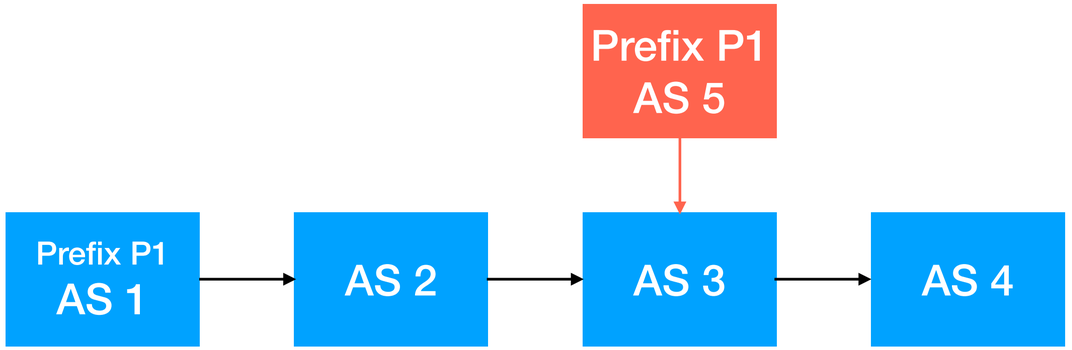
RIPE NCC
RIPE NETWORK COORDINATION CENTRE

RPKI: ROV Deployment in Central Asia

Qasim Lone

Qasim Lone | 29 May 2024 | IMD 2024

Route Origin Hijacks

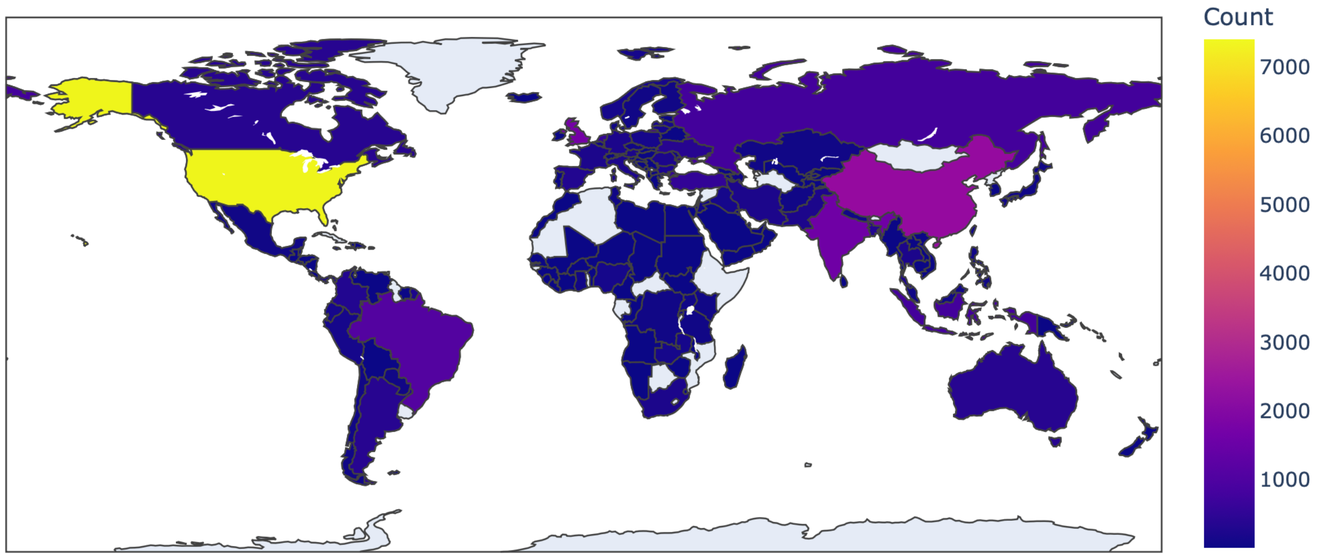


Valid Route
4 -> 3 -> 2 -> 1

Hijacked Route
4 -> 3 -> 5

BGP Incidents

- Cloudflare Radar reported more than 47K BGP incidents in past year (May 2023- May 2024)

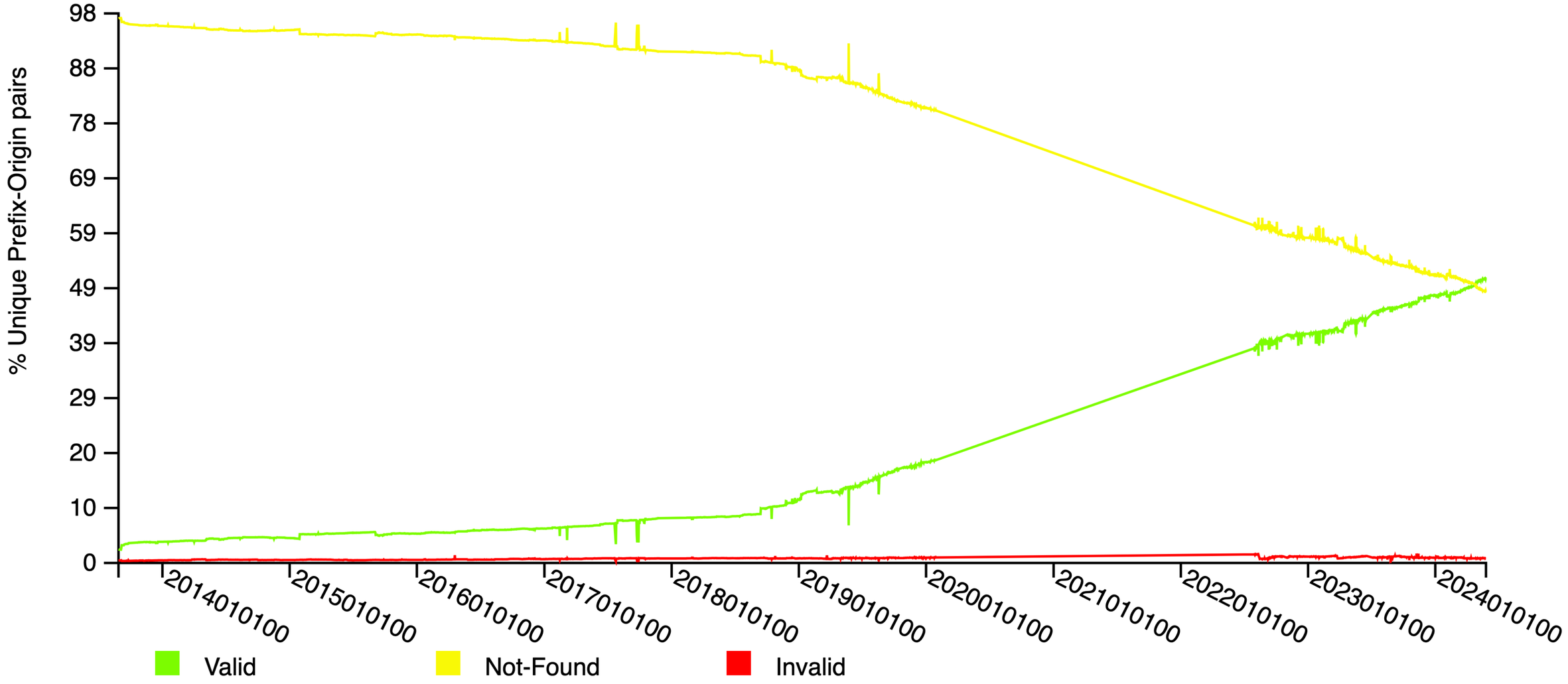


Country	Victim	Hijacker	Total
Uzbekistan	2	2	4
Kyrgyzstan	2	0	2
Kazakhstan	38	46	84
Tajikistan	12	13	25
Turkmenistan	0	0	0

RPKI

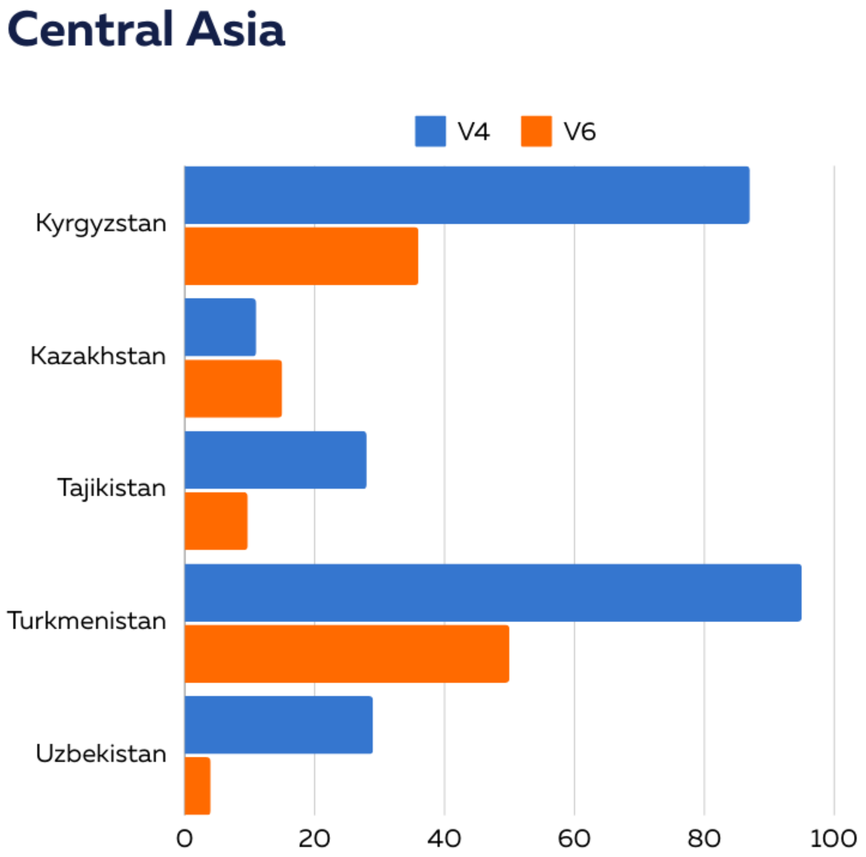
- RPKI helps prevent route origin hijacks, whether due to misconfigurations or by malicious actors
- Used to validate the origin of BGP announcements
  - Is the originating ASN authorised to originate this particular prefix?
- Has two parts:
  - Signing own prefixes (ROA = Route Origin Authorisation)
  - Verification of others' announcements (ROV = Route Origin Validation)

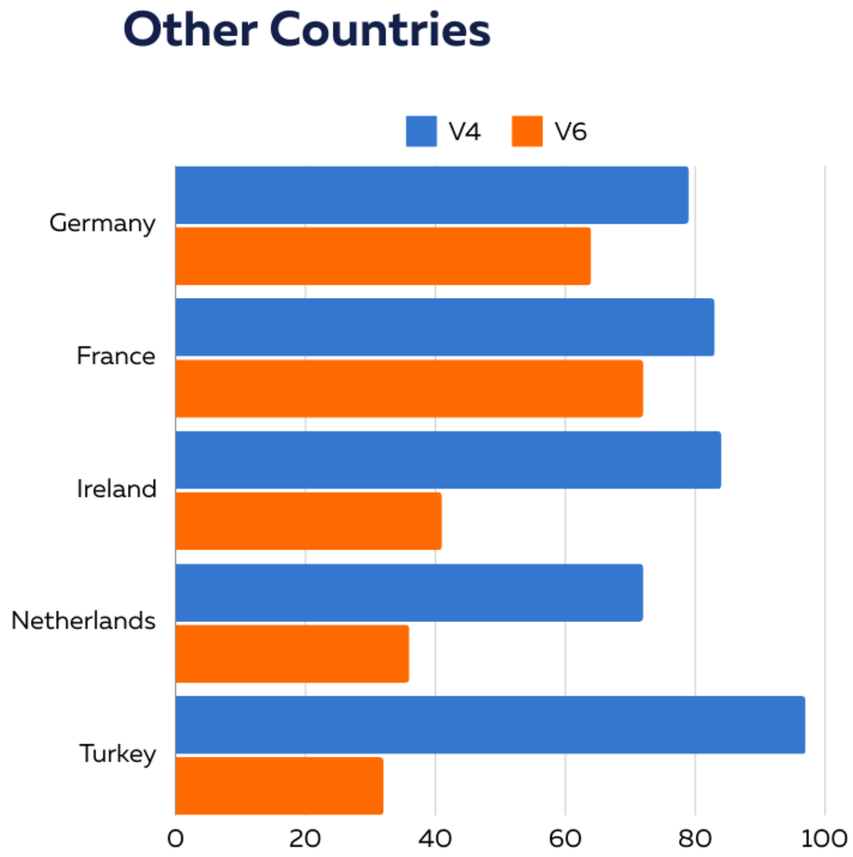
RPKI-ROV History of Unique Prefix-Origin Pairs (IPv4)



NIST RPKI Monitor: RPKI-ROV Analysis **Protocol:** IPv4 **RIR:** All

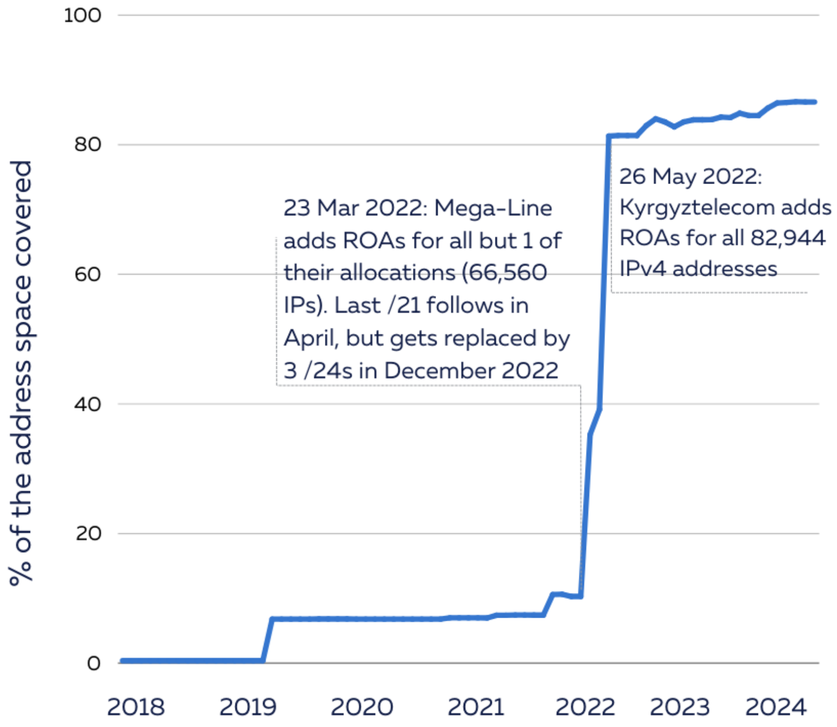
ROA Coverage



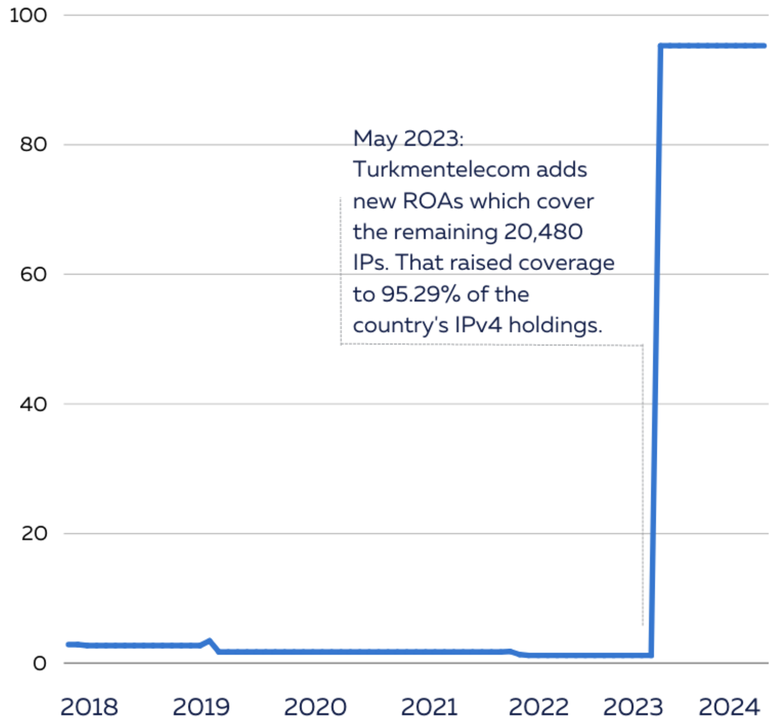


ROA Coverage (IPv4)

Kyrgyzstan



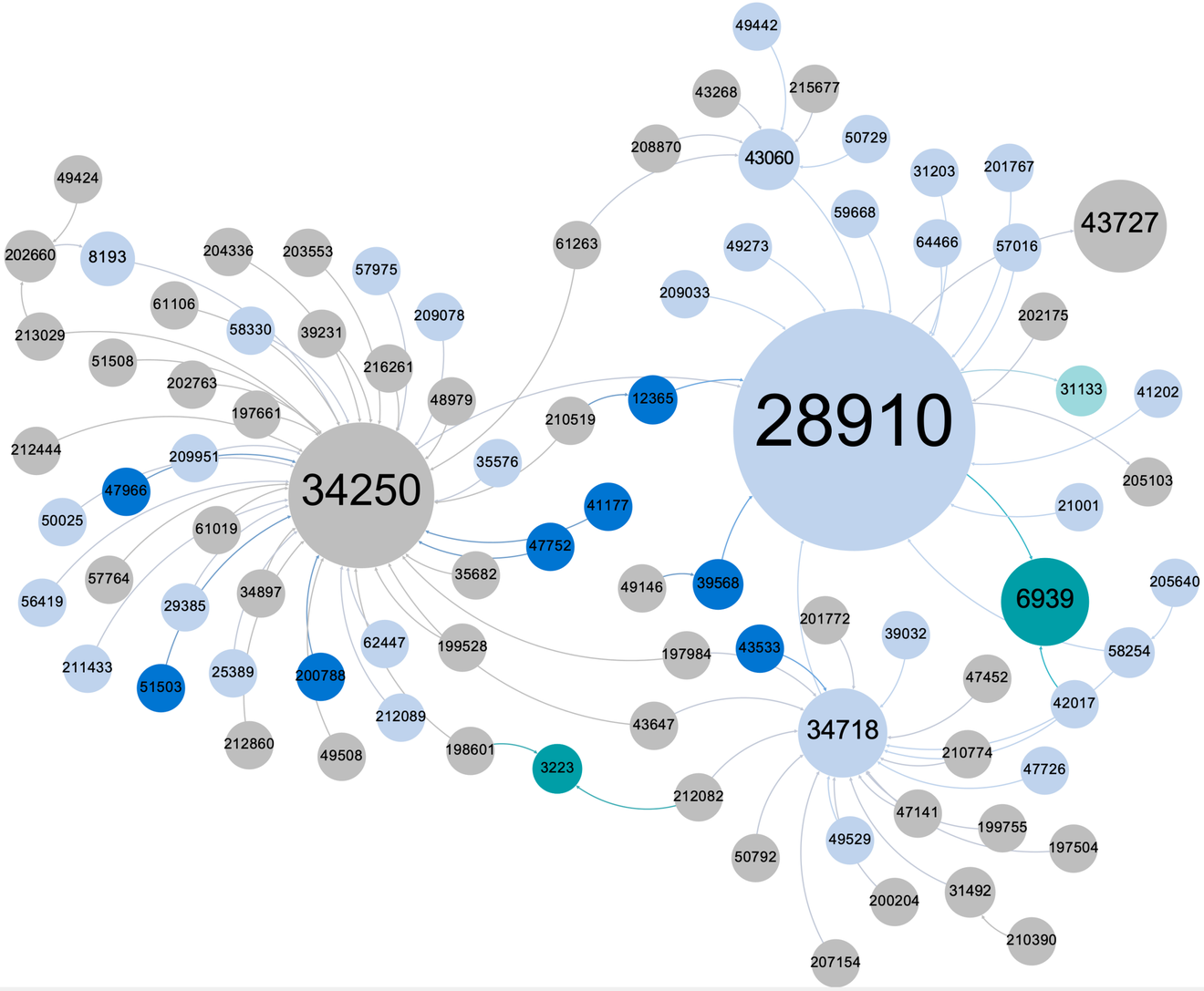
Turkmenistan



Measuring ROV

- We used RoVISTA to analyse deployment of ROV across Central Asian countries
  - RoVISTA[1] calculates the scores based on the number of RPKI-invalid prefixes that an AS can reach. We used a more inclusive approach where we classify an AS as having implemented ROV if its score is greater than 0, indicating any level of ROV deployment.
- Collateral benefit:
  - We assessed ROV impact from the perspective of network centrality, utilising the AS Hegemony [2] methodology, which measures the centrality of autonomous systems within a country.
  - The methodology measures the common transit networks to a local AS and how much this AS relies on these transit networks based on BGP data. AS hegemony values range between 0 and 1 and indicate the fraction of paths crossing a node.

Uzbekistan



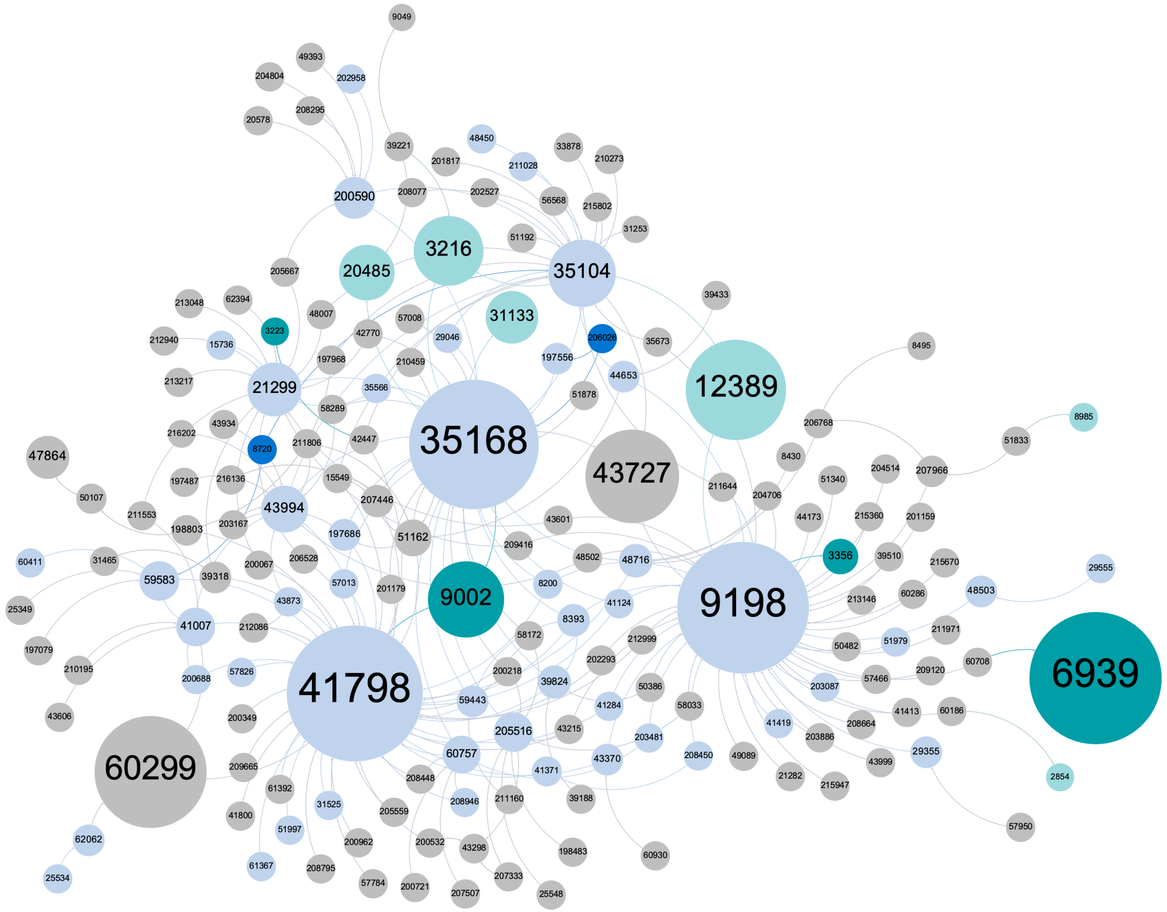
Local AS Foreign AS

ROV

No ROV

No Data

Kazakhstan



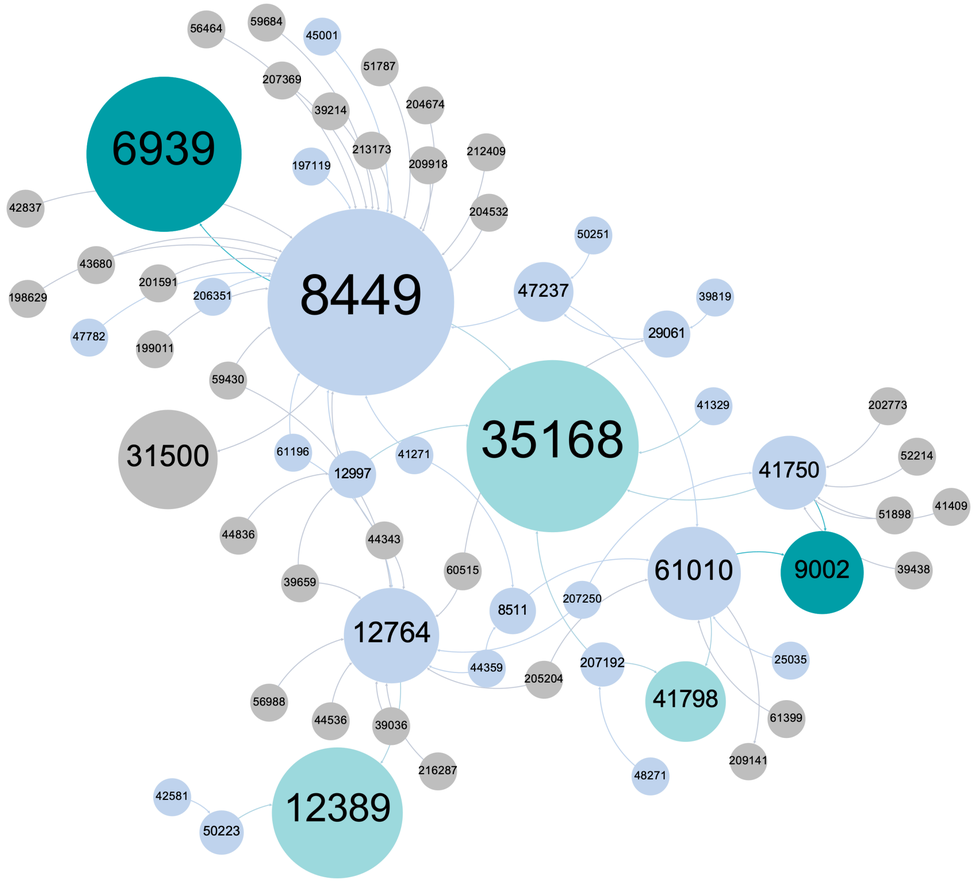
Local AS Foreign AS

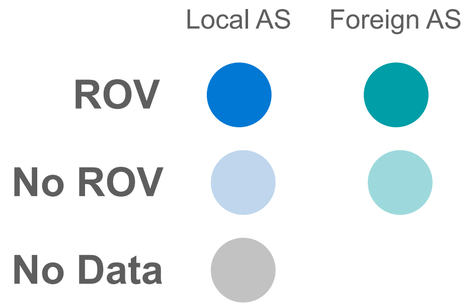
ROV

No ROV

No Data

Kyrgyzstan


56464
59684
45001
51787
207369
39214
204674
213173
212409
197119
209918
6939
42837
204532
50251
43680
201591
206351
198629
8449
47237
39819
29061
47782
199011
59430
41329
202773
35168
31500
61196
41271
52214
12997
41750
41409
51898
44836
44343
60515
61010
9002
39438
39659
207250
8511
12764
25035
44359
205204
207192
41798
56988
61399
44536
39036
209141
216287
48271
42581
12389
50223


Local AS
Foreign AS
ROV
No ROV
No Data

Conclusion

- While strides have been made in RPKI deployment and routing security, there is a significant disparity in technology adoption rates across the region.
- A recent example is from the US FCC's recent fact sheet, which proposes that network providers report on their BGP risk mitigation progress, including status and plan for deployment of ROA and ROV.
- RIPE NCC Survey 2023 show that a primary barrier to RPKI implementation is unfamiliarity with the technology.
  - RIPE NCC Academy offers a variety of courses, trainings, and webinars to help stakeholders learn more about RPKI (visit academy.ripe.net)

Questions

References

- [1] RoVista https://rovista.netsecurelab.org
- [2] AS Hegemony, https://labs.ripe.net/author/romain_fontugne/as-hegemony-measuring-as-interdependence/
- [3] RIPE NCC Academy, https://academy.ripe.net/