RIPE NCC
RIPE NETWORK COORDINATION CENTER

RPKI Deployment and IPv6 Uptake in South East Europe

Qasim Lone, Anastasiya Pak | RIPE NCC | SEE 13 | 8 April 2025

Routing Security

The Need for RPKI

- Attackers or misconfigurations can redirect traffic, causing outages or data theft.
  - **Example**: Pakistan Telecom (2008) accidentally hijacked YouTube’s IPs, resulting in a global outage.
- Why RPKI?
  - Prevents such incidents by cryptographically verifying the legitimacy of route announcements.
  - Helps mitigate both accidental and malicious BGP misconfigurations.

The Need for RPKI

- **Border Gateway Protocol**
  - Extremely trustful, “routing by rumour”
  - Attackers or misconfigurations can redirect traffic and cause outages or data theft
  - Can we get rid of it? Can we update it? Can we add something out of band?

- **Why RPKI?**
  - Resource Public Key Infrastructure
  - Initially introduced to make informed routing decisions (by verifying the legitimacy of BGP announcements with digitally signed statements)
  - Helps mitigate both accidental and malicious BGP incidents

Enhancing Routing Security with RPKI

- RPKI has two parts:
  - Signing and Validating

- The most known usage is to validate the origin of BGP announcements
  - i.e. “Is this ASN authorised to originate this particular prefix?”
  - Route Origin Authorisation (ROA): objects stating which ASNs are authorised to announce specific IP prefixes (signed by the prefix holder)
  - Route Origin Validation (ROV): verifying the origin of BGP announcements based on ROAs and ensuring only valid routes are accepted (done by every network operator)

Enhancing Routing Security

- Used to validate the origin of BGP announcements
  - Is the originating ASN authorised to originate this particular prefix?

- Has two parts:

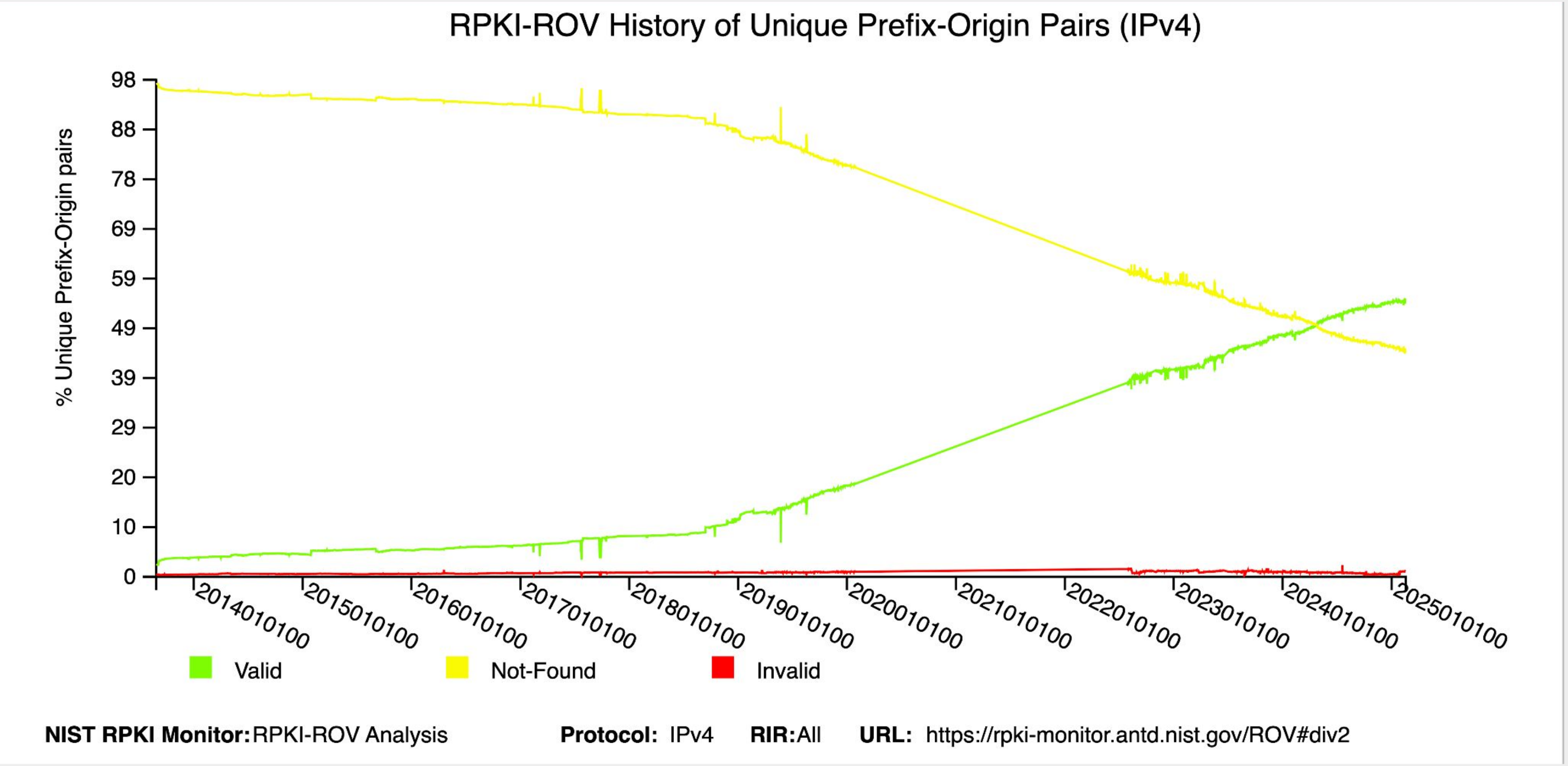
  - **Route Origin Authorisation (ROA):** Defines which ASes are authorised to announce specific IP prefixes

  - **Route Origin Validation (ROV):** Validates routes based on ROAs, ensuring only legitimate routes are accepted.

The RPKI Era – Enhanced Routing Security

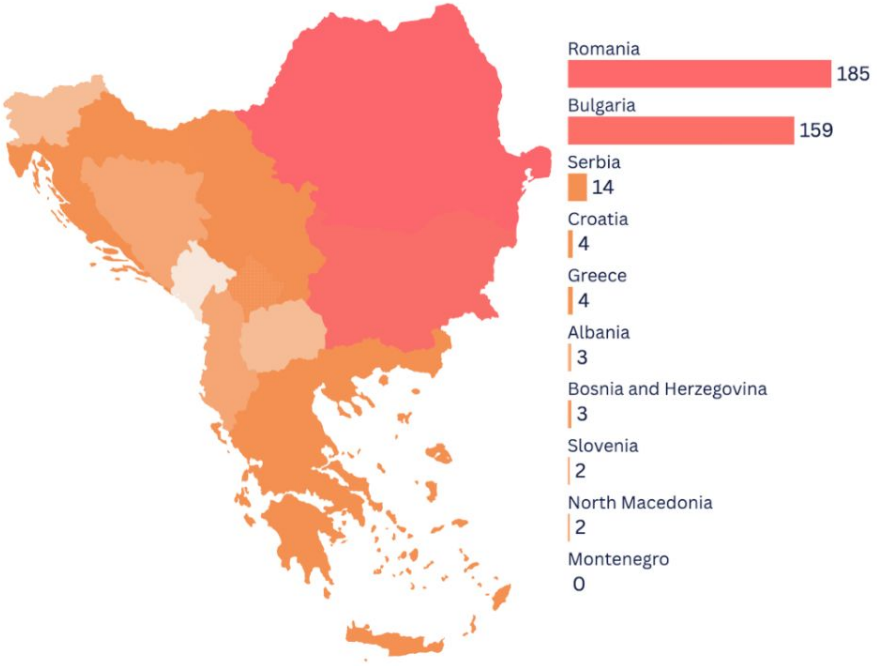
- Telegram Block Attempt (July 2023):
    - Misconfigured BGP advertisement blackholed global traffic
    - Networks doing ROV rejected incorrect routes
- Cloudflare 1.1.1.1 Incident (June 2024):
    - Routing misconfiguration caused service disruption
    - ROV helped prevent incorrect route propagation lowering the impact

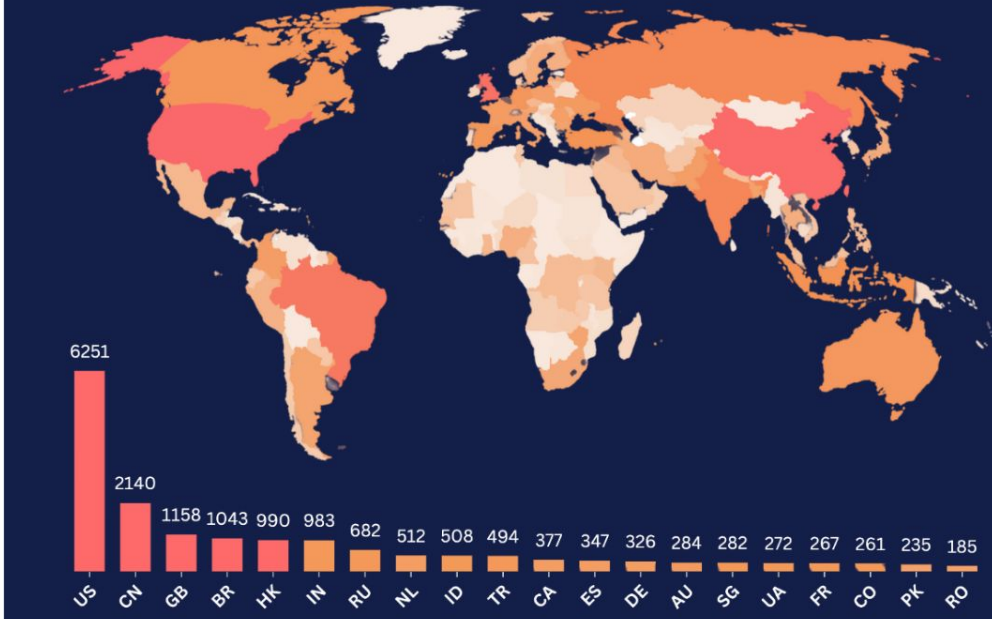
Global RPKI Adoption (NIST)



BGP Incidents in the Region and Globally

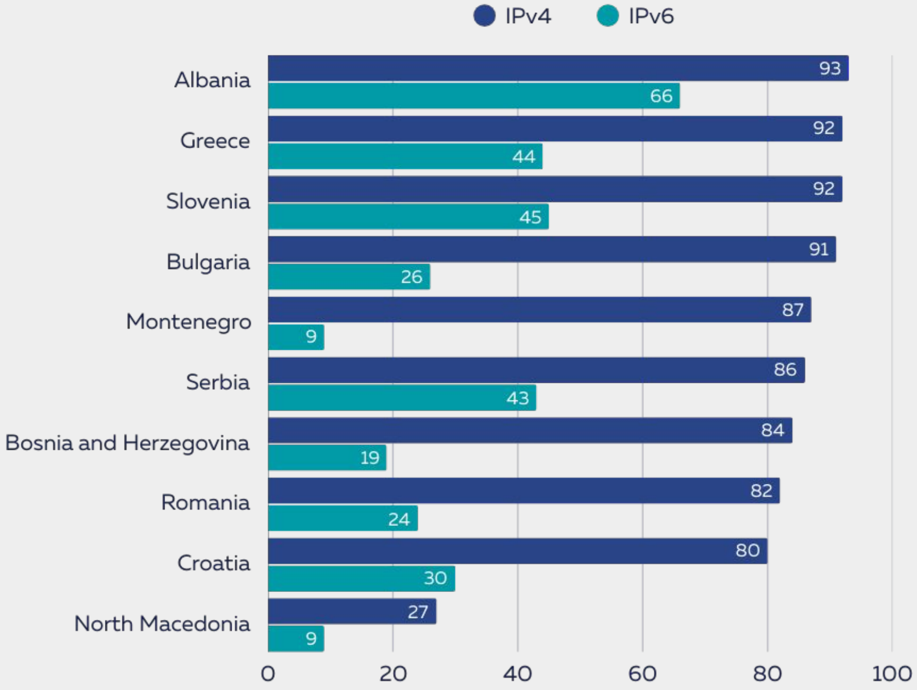
March 2024 - March 2025, source: Cloudflare



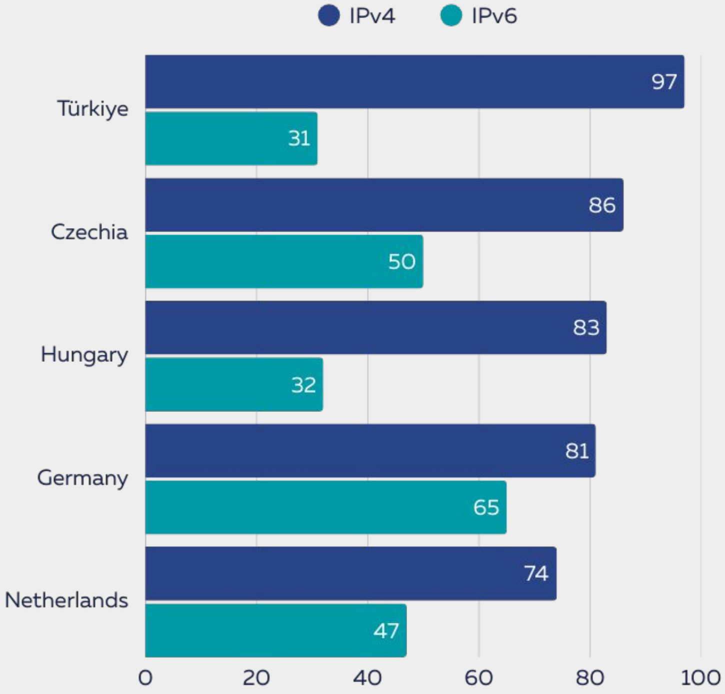


Route Origin Authorisation (ROA)

ROA Coverage in the region and beyond (IPv4 and IPv6, %)



South East Europe

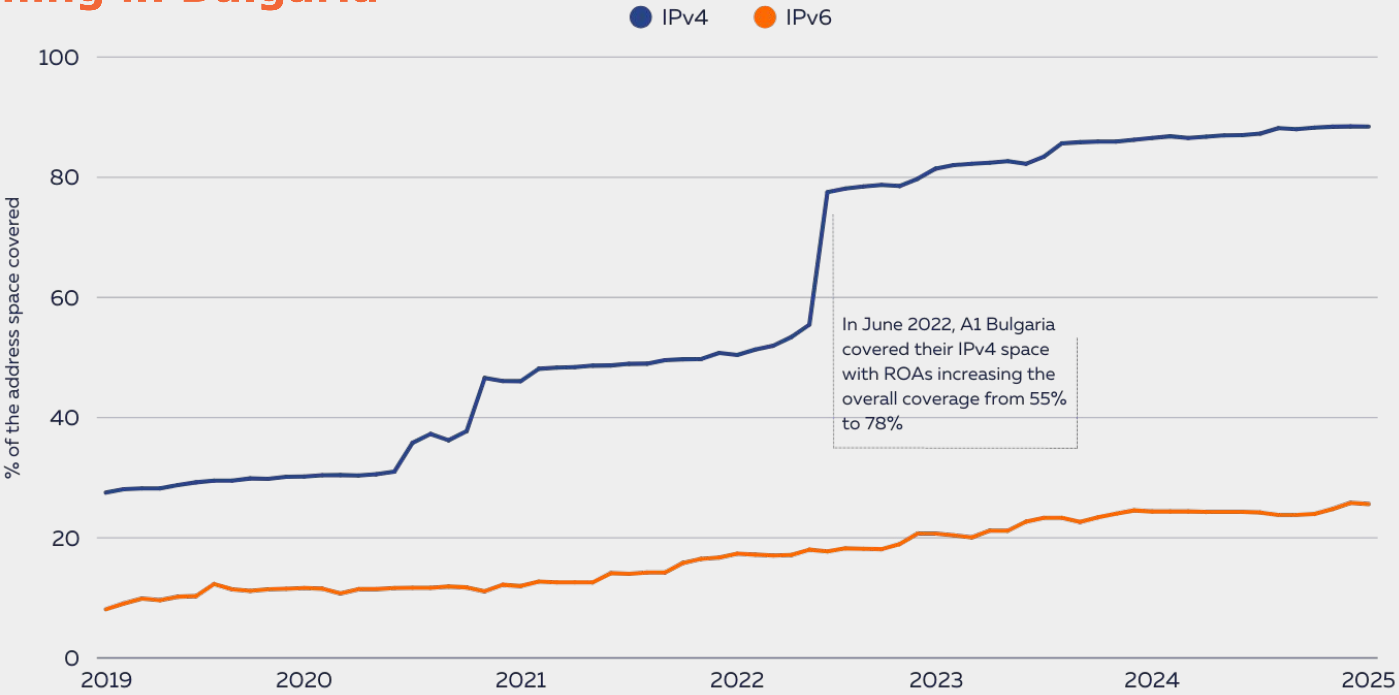


Other Countries

Source: RIPE NCC
Snapshot from March 2025

ROA Coverage in the region (IPv4)

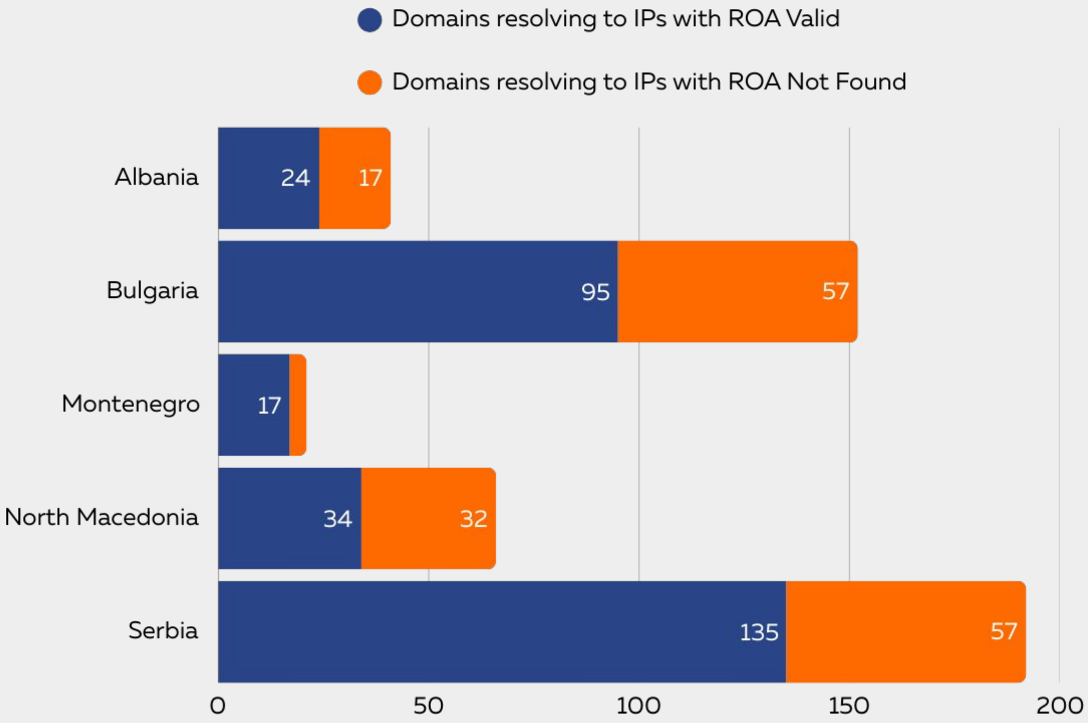
Zooming in Bulgaria



In June 2022, A1 Bulgaria covered their IPv4 space with ROAs increasing the overall coverage from 55% to 78%

Source: RIPEstat, RIPE NCC

ROA Coverage: Government Domains in SEE



Source: RIPE NCC, RIS

We analysed whether IP addresses resolved to the government domains in certain SEE countries are covered by ROAs. We chose a sample of countries that experienced cyber attacks on government websites in the past few years.

The methodology involves extracting BGP routing data from RIS and then validating against RIPE NCC’s RPKI Validator, categorising each prefix as Valid (properly authorised), Invalid (violating a ROA), or Not-Found (lacking RPKI protection).

IP addresses that resolved to these domains and fell under RPKI Invalid or Not-Found prefixes—and were not concurrently covered by a more specific Valid ROA—were classified as belonging to RPKI Invalid or Not-Found prefixes

Help us make the domain lists comprehensive!

Route Origin Validation (ROV)

ROV Deployment in South East Europe

As the ‘second step’ in ensuring routing security through RPKI, **ROV** verifies that route announcements adhere to the authorisations specified by ROAs.

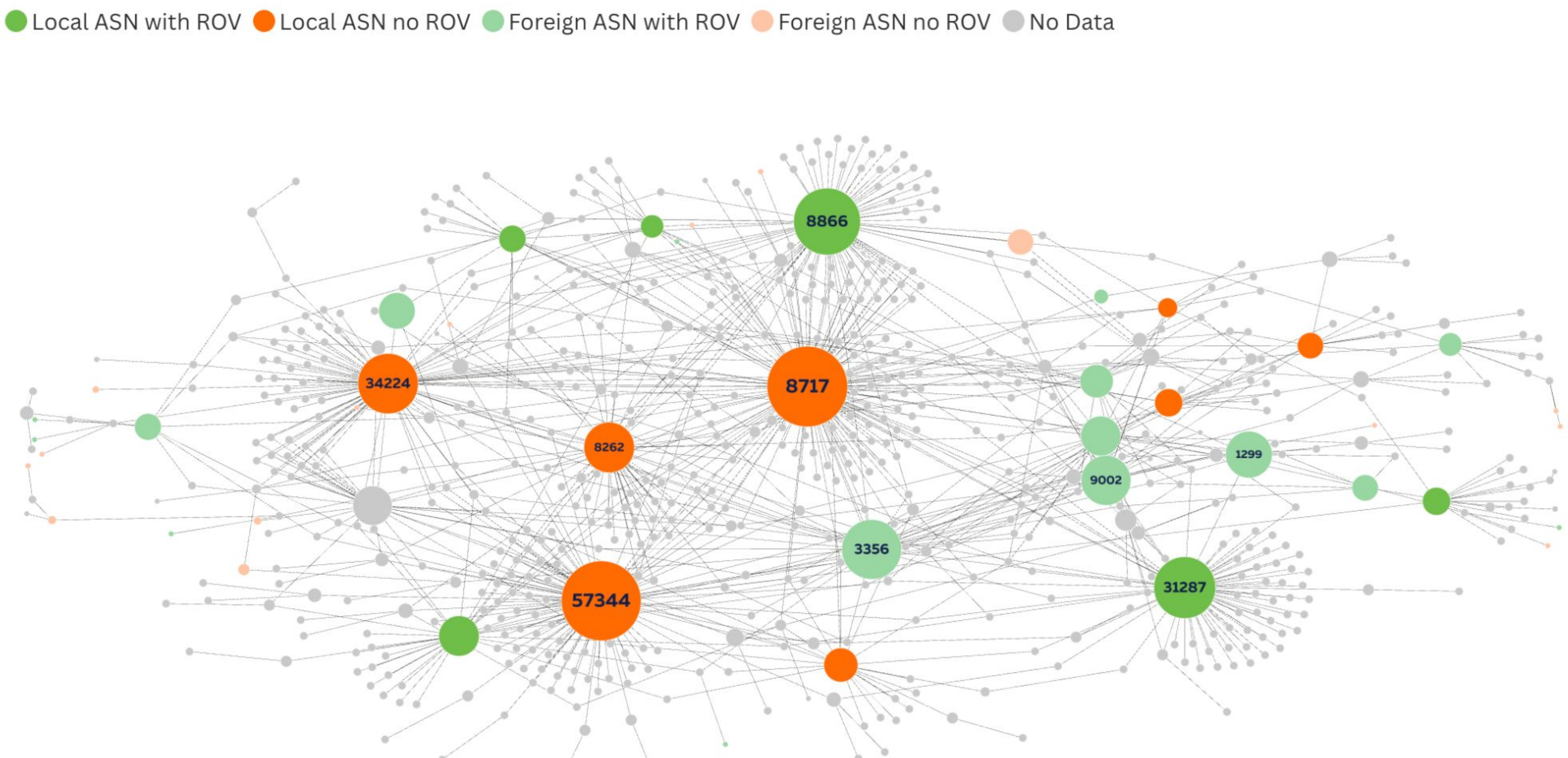
We analysed the deployment of ROV in the region using RoVISTA, which calculates scores based on the number of RPKI-invalid prefixes an AS can reach. We assessed ROV impact from the perspective of network centrality, utilising AS Hegemony methodology to measure the centrality of autonomous systems within a country. We visualised the results as follows, with the size of each AS effectively indicating how central a role it plays in Internet routing.

Measuring ROV

- We used RoVISTA to analyse deployment of ROV across the SEE region
  - RoVISTA 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.

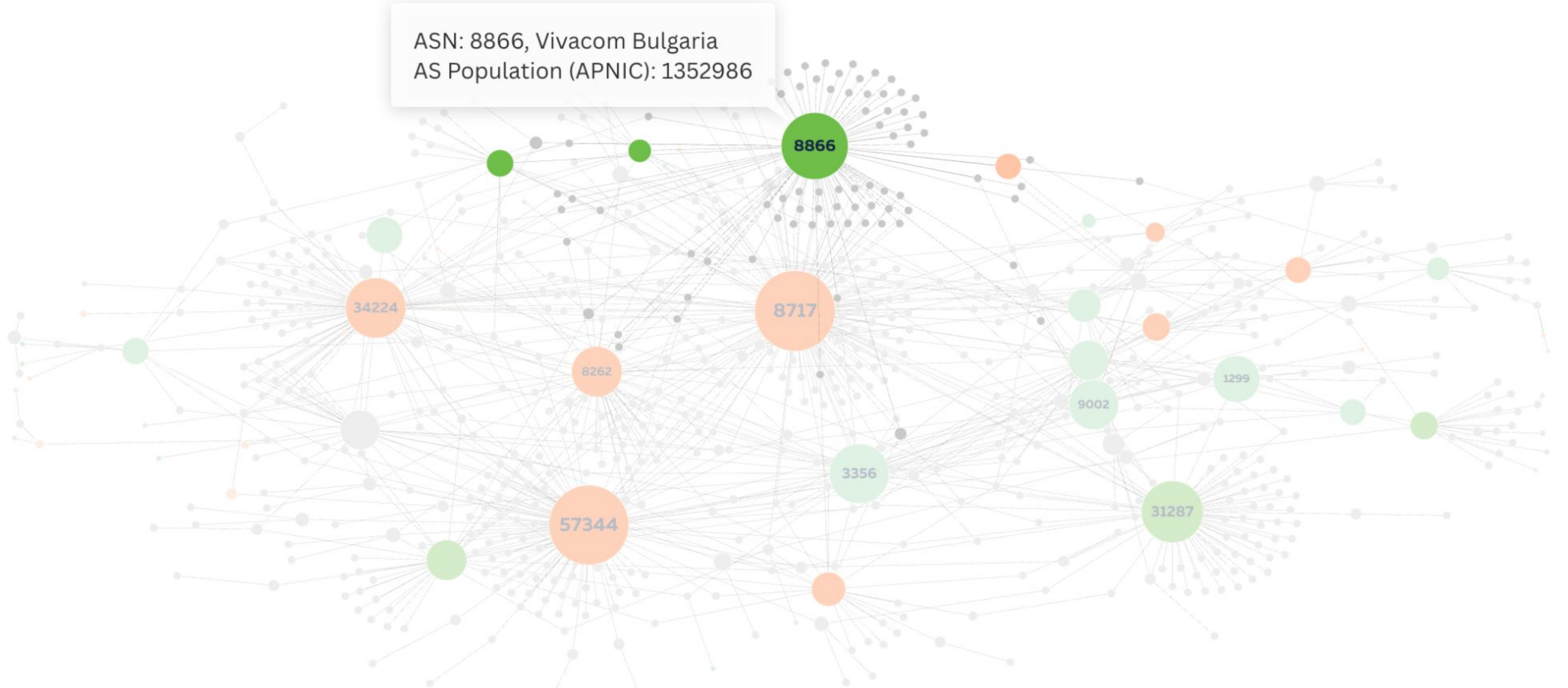
- **Collateral benefit**
  - We assessed ROV impact from the perspective of network centrality, utilising the AS Hegemony methodology, which measures the centrality of autonomous systems within a country.
  - The methodology measures the common transit networks to a local AS and how much this AS relies 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.

Bulgaria Interconnectivity Map (AS Hegemony, ROV)



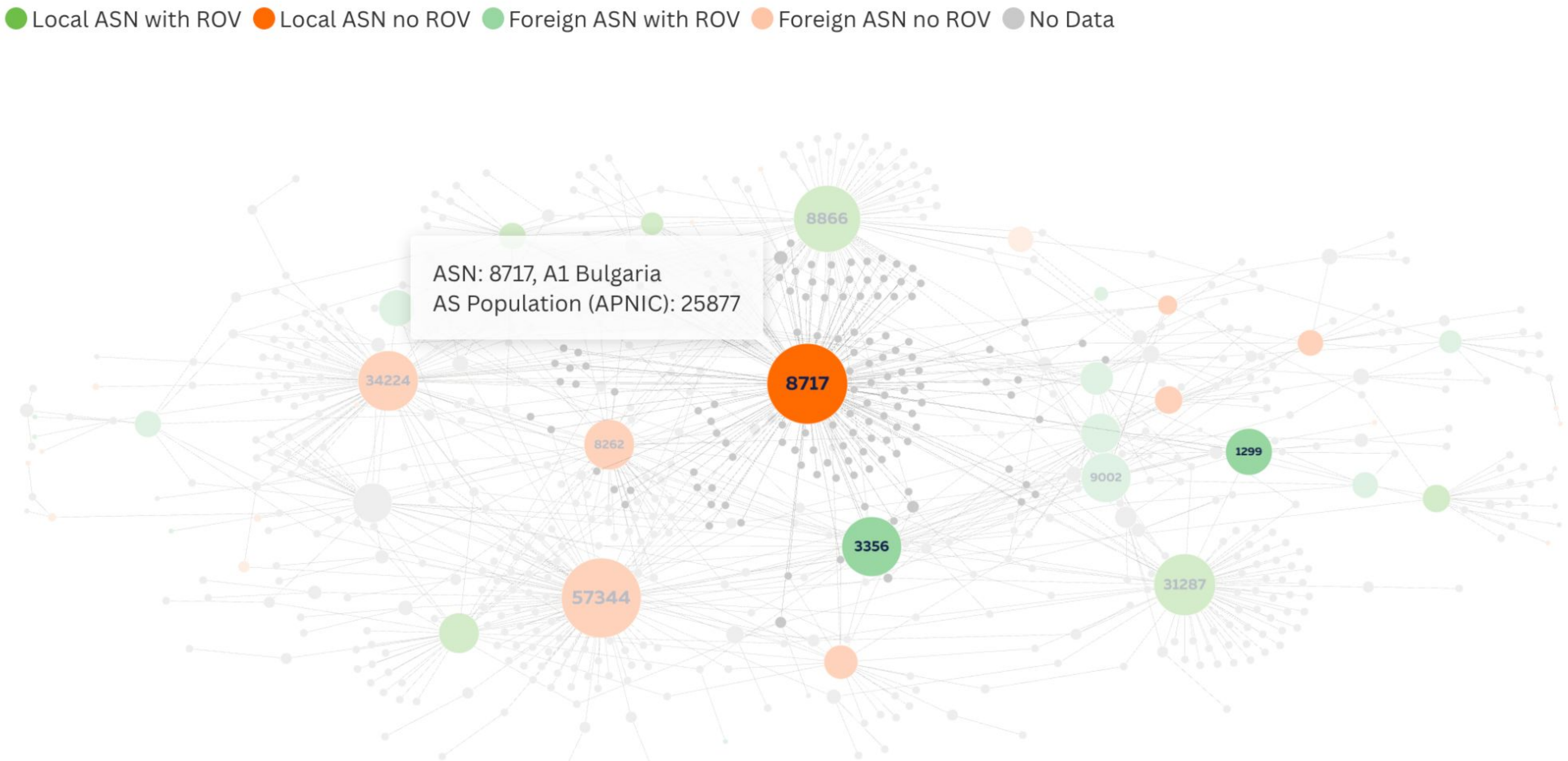
Bulgaria Interconnectivity Map (AS Hegemony, ROV)

● Local ASN with ROV ● Local ASN no ROV ● Foreign ASN with ROV ● Foreign ASN no ROV ● No Data



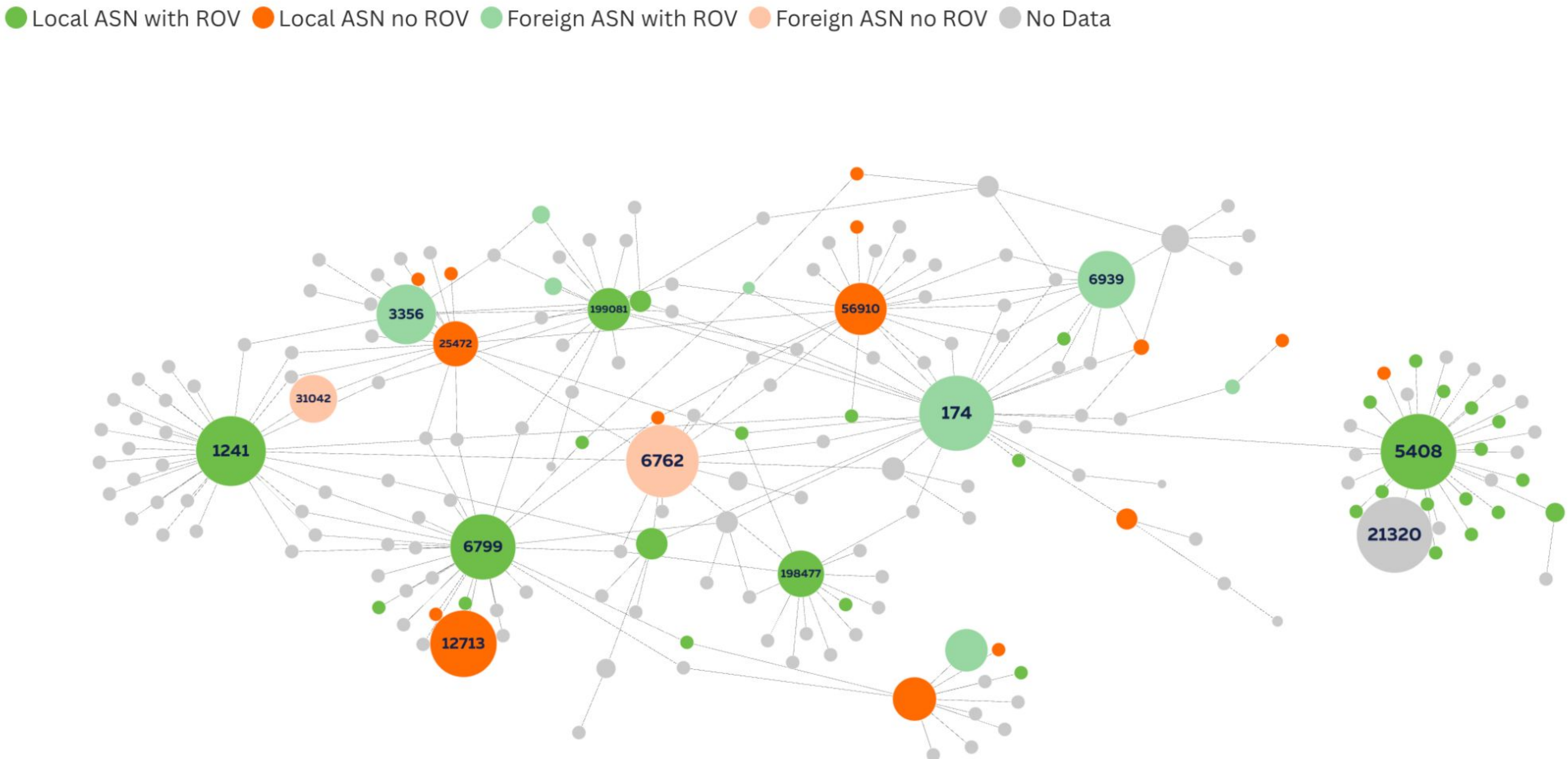
ASN: 8866, Vivacom Bulgaria
AS Population (APNIC): 1352986

Bulgaria Interconnectivity Map (AS Hegemony, ROV)



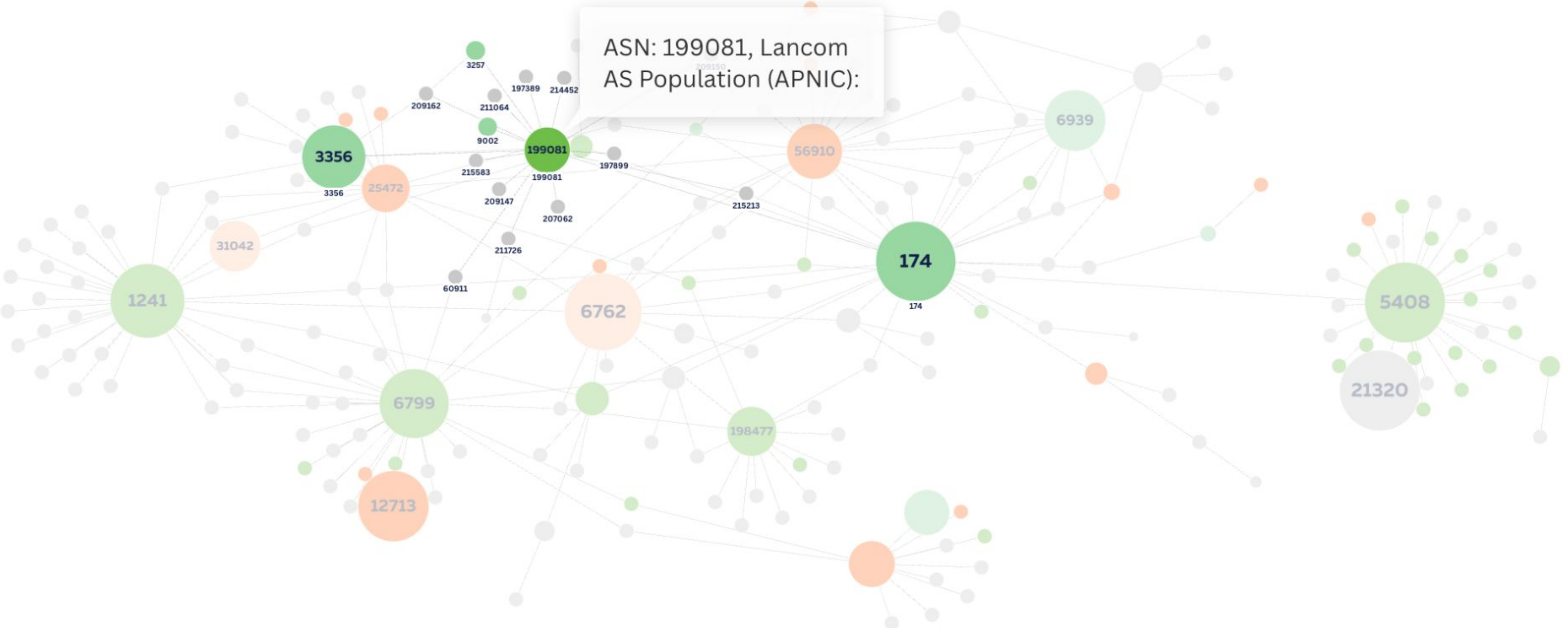
ASN: 8717, A1 Bulgaria
AS Population (APNIC): 25877

Greece Interconnectivity Map (AS Hegemony, ROV)



Greece Interconnectivity Map (AS Hegemony, ROV)

● Local ASN with ROV ● Local ASN no ROV ● Foreign ASN with ROV ● Foreign ASN no ROV ● No Data

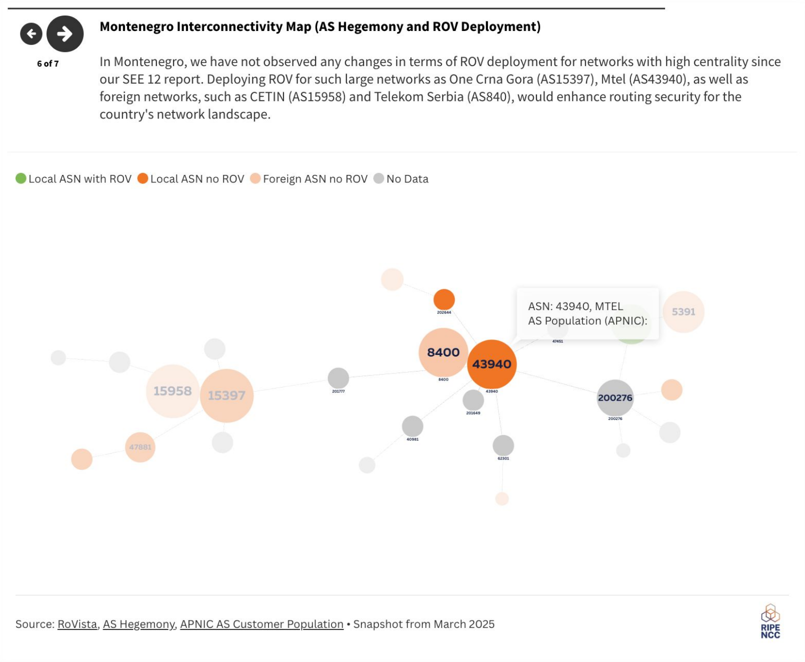


ASN: 199081, Lancom
AS Population (APNIC):

Find your AS!

Check out the interactive graph

Network graph made with Flourish
Sources: AS Hegemony, RoVista, APNIC
Available for Bulgaria, Greece, Montenegro, Serbia



6 of 7

Montenegro Interconnectivity Map (AS Hegemony and ROV Deployment)

In Montenegro, we have not observed any changes in terms of ROV deployment for networks with high centrality since our SEE 12 report. Deploying ROV for such large networks as One Crna Gora (AS15397), Mtel (AS43940), as well as foreign networks, such as CETIN (AS15958) and Telekom Serbia (AS840), would enhance routing security for the country's network landscape.

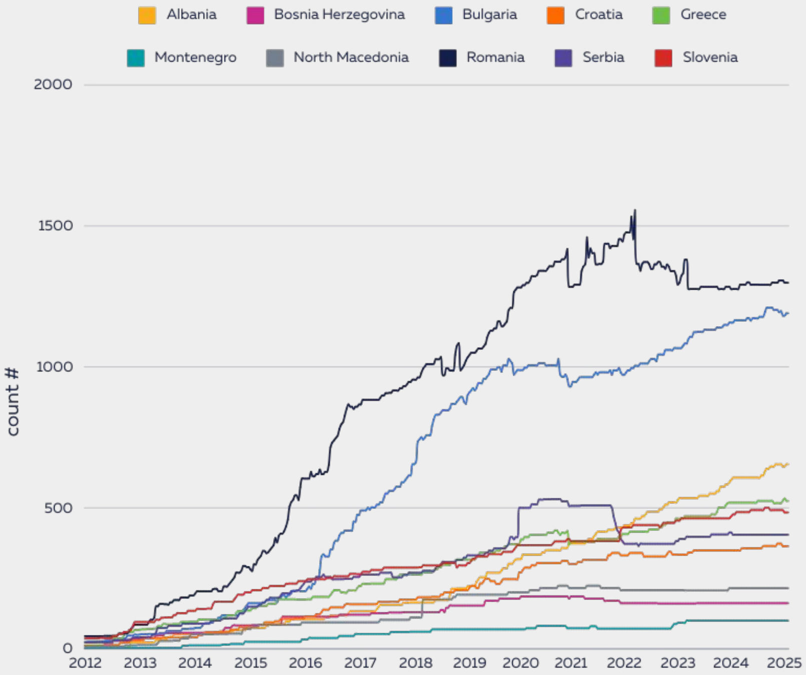
● Local ASN with ROV ● Local ASN no ROV ● Foreign ASN no ROV ● No Data

ASN: 43940, MTEL
AS Population (APNIC):

Source: RoVista, AS Hegemony, APNIC AS Customer Population • Snapshot from March 2025

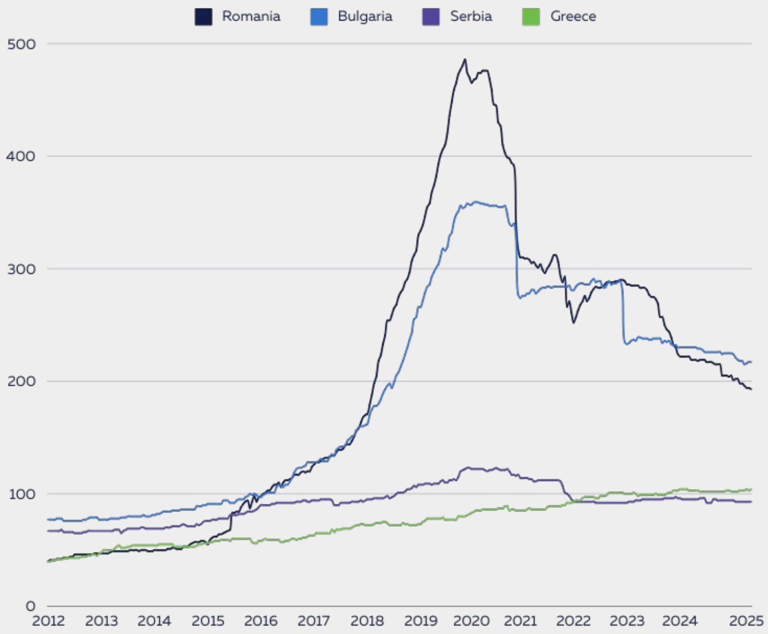
IPv6 Uptake in South East Europe

South East Europe: Internet Resources



IPv6 Space (/32s) in SEE

Source: RIPE NCC



Active LIRs
(Bulgaria, Greece, Romania, Serbia)

IPv6 Capability

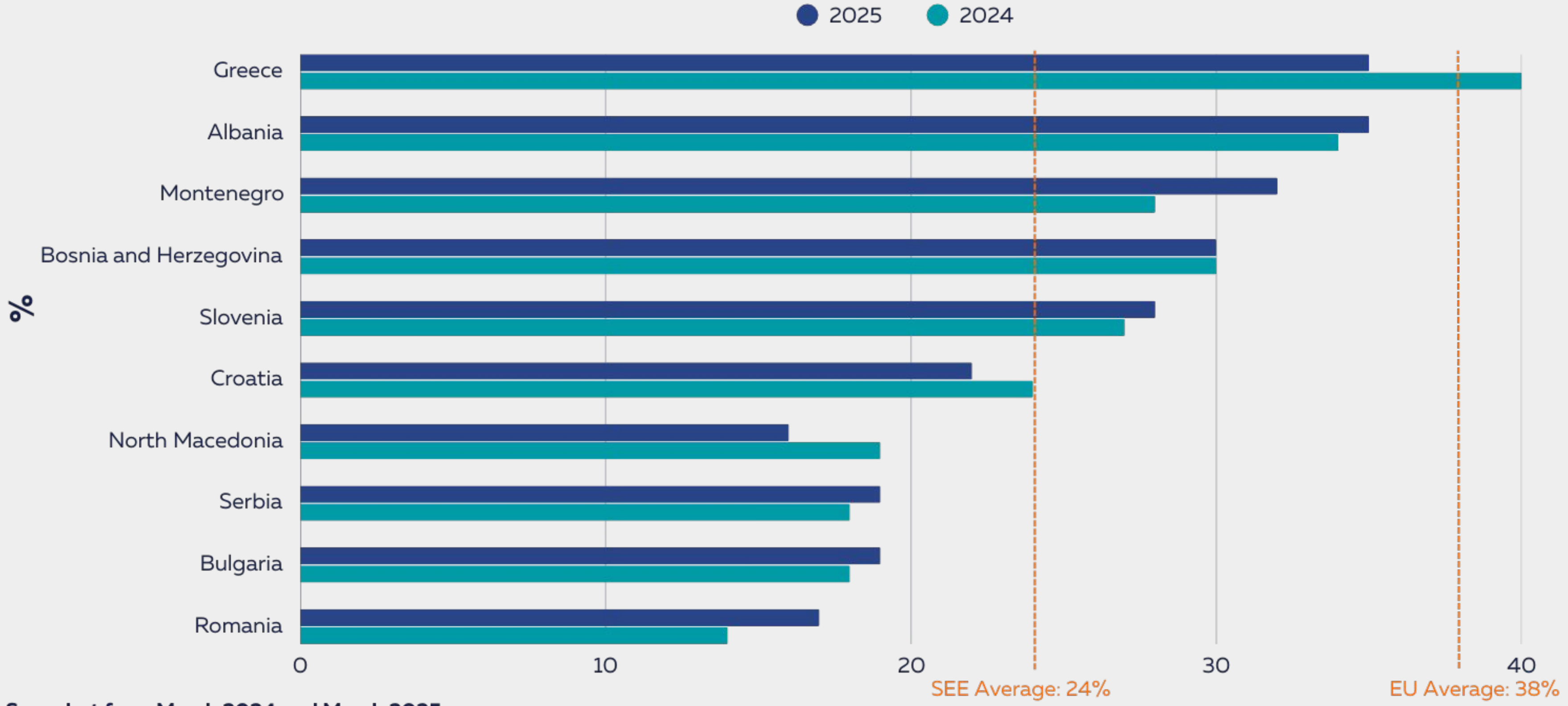
- Given the vast size of the IPv6 address space, counting individual addresses is not an effective metric.

- We calculated (IPv6 capability) the percentage of ASes in each country that announce both IPv4 and IPv6 addresses, as well as those that announce only IPv6, compared to those that announce only IPv4

  - IPv6 capability indicates that addresses are being routed, this does not necessarily equate to adoption.

  - IPv6 capability should be viewed as an initial step toward broader adoption.

% of IPv6-capable ASNs in South East Europe



Snapshot from March 2024 and March 2025

Source: RIPE NCC

IPv6 Adoption in the South East Europe, %

Country	IPv6 adoption (Google)	IPv6 adoption (Facebook)	IPv6 adoption (Cloudflare)
Greece	63	56	38
Romania	32	33	18
Bulgaria	21	15	6
Slovenia	14	13	8
Albania	10	8	1
Bosnia Herzegovina	10	15	6
Croatia	9	5	4
Serbia	6	7	5
Montenegro	0	0	0
North Macedonia	0	0	0
Kosovo	0		18

- IPv6 adoption measures if users can actually use IPv6 on their networks.
- We used Content Delivery network (CDN’s) (Google, Facebook, Cloudflare) traffic statistics to measure adoption across the region.
- Generally, low level of IPv6 adoption in the region except Greece. Romania and Bulgaria also have relatively higher level of adoption in comparison to the rest of the region.

Conclusion – RPKI Adoption

- Growing recognition of RPKI importance at government level:
  - White House roadmap advocating RPKI as mature solution for BGP vulnerabilities
  - US government aims to have 60% of advertised IP space under ARIN RSA, explicitly paving the way to ROAs for federal networks

- Regulatory bodies taking action:
  - FCC (in US), proposing annual BGP security risk management plans for ISPs
  - Forum Standaardisatie (in NL), “apply or explain” by the end of 2024 for all governmental entities, both ROAs and ROV

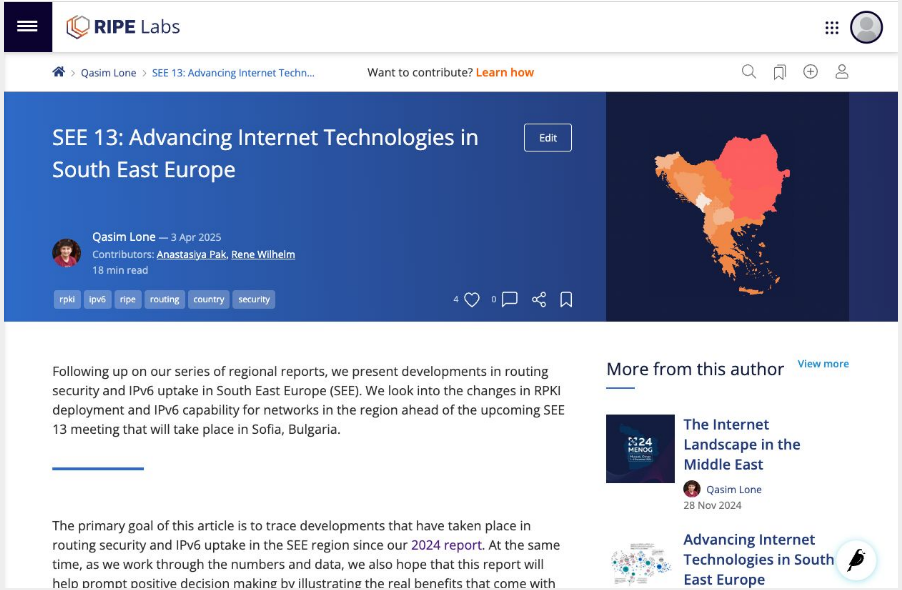
- Implications for South East Europe:
  - Opportunity for operators and policymakers to enhance routing security
  - Potential to establish guidelines and timelines for RPKI adoption

Conclusion – IPv6 Adoption

- Need for policy initiatives and infrastructure investments
- Increased awareness and education is crucial

- **Learning Resources**
  - RIPE NCC Academy courses (IPv6 Fundamentals, IPv6 Security) and Webinars- free for everyone
    - academy.ripe.net
  - In-person trainings (for members)
    - learning.ripe.net

Read More on RIPE Labs!


RIPE Labs
Qasim Lone > SEE 13: Advancing Internet Techn...
Want to contribute? Learn how
Edit
rpki
ipv6
ripe
routing
country
security
4
0

SEE 13: Advancing Internet Technologies in South East Europe

Qasim Lone — 3 Apr 2025
Contributors: Anastasiya Pak, Rene Wilhelm
18 min read

Following up on our series of regional reports, we present developments in routing security and IPv6 uptake in South East Europe (SEE). We look into the changes in RPKI deployment and IPv6 capability for networks in the region ahead of the upcoming SEE 13 meeting that will take place in Sofia, Bulgaria.

The primary goal of this article is to trace developments that have taken place in routing security and IPv6 uptake in the SEE region since our 2024 report. At the same time, as we work through the numbers and data, we also hope that this report will help prompt positive decision making by illustrating the real benefits that come with

More from this author View more

The Internet Landscape in the Middle East
Qasim Lone
28 Nov 2024

Advancing Internet Technologies in South East Europe

Questions & Comments ?

✉ qlone@ripe.net
apak@ripe.net

References

- [1] RoVista https://rovista.netsecurelab.org
- [2] AS Hegemony, https://labs.ripe.net/author/romain_fontugne/as-hegemony-measuring-as-interdependence/
- [3] Cloudflare, https://developers.cloudflare.com/api/resources/radar/subresources/bgp/subresources/hijacks/subresources/events/methods/list/
- [4] RIS, ripe.net/ris