امنیت زیرساخت اینترنت در آسیای مرکزی

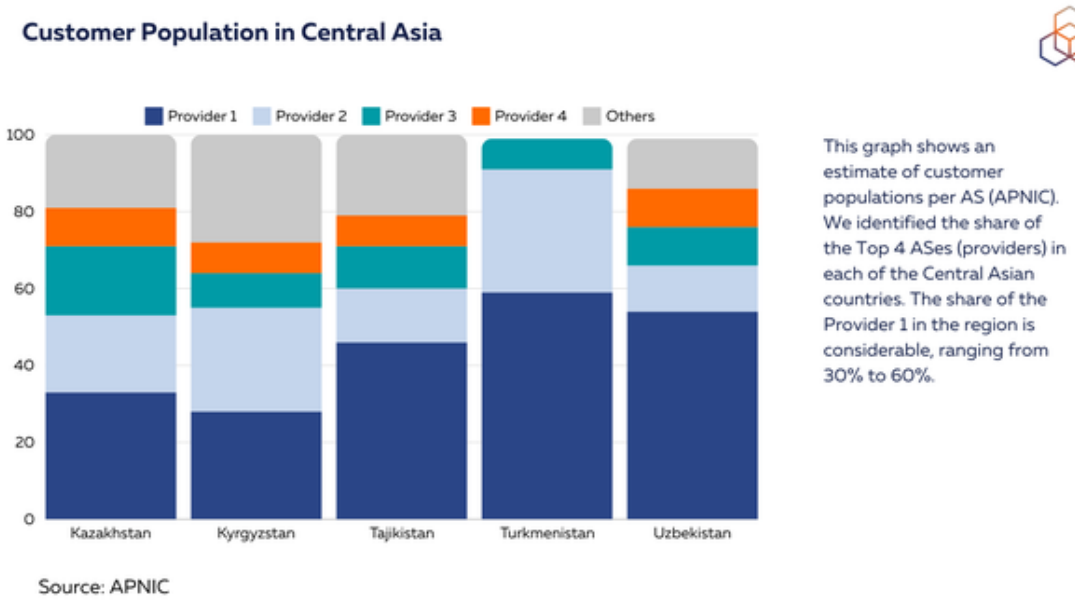
نویسندگان: آناستاسیا پاک، کاسیم لوان، الکس سمینیاکا، وان اووسیپیان

سومین نشست مجمع هم‌پیری و هم‌پیوستگی آسیای مرکزی (CAPIF 3) در بیشکک، قرقیزستان در تاریخ 24-25 سپتامبر 2024 برگزار می‌شود. این رویداد متخصصان از آسیای مرکزی، ایران و مناطق همسایه را برای تقویت زیرساخت اینترنت منطقه و حمایت از توسعه دیجیتالی آن گرد هم خواهد آورد. در این مقاله، ما به بررسی حوزه‌های کلیدی در زمینه فناوری‌های اینترنتی پرداختیم که می‌توانند به شکل قابل توجهی بر امنیت، مقیاس‌پذیری و آمادگی شبکه‌های اینترنتی کشورهای آسیای مرکزی در مواجهه با چالش‌های آینده تأثیر بگذارند. در این راستا، ما دو فناوری مهم را برجسته کرده‌ایم: زیرساخت کلیدهای عمومی منابع (RPKI) و پروتکل اینترنت نسخه 6 (IPv6).

آسیای مرکزی منطقه‌ای با تاریخ مشترک غنی و بدون دسترسی به دریا است و جمعیتی نزدیک به 80 میلیون نفر (بر اساس آمار 2024) دارد. در سال‌های اخیر، این منطقه رشد اقتصادی و اجتماعی قابل توجهی را تجربه کرده است، که طبق پیش‌بینی‌های بانک اروپایی برای بازسازی و توسعه (EBRD) تا پایان سال 2024 از 5 درصد بیشتر خواهد شد. علاوه بر این، این منطقه شاهد دیجیتالی شدن سریع است و بیش از 65 میلیون کاربر اینترنتی در سال 2023 در آن ثبت شده است. با این حال، دسترسی به اینترنت و اتصال آن همچنان چالش‌برانگیز است.

در این مقاله، ما به تحلیل پذیرش RPKI و گذار به IPv6 در آسیای مرکزی پرداخته‌ایم و به فرصت‌های تقویت زیرساخت‌های اینترنتی منطقه و پشتیبانی از رشد دیجیتالی آن اشاره کرده‌ایم.

در بررسی بازار اینترنت هر یک از کشورهای آسیای مرکزی، روند کلی تمرکز بازار مشاهده می‌شود. هرچند این امر ممکن است رقابت را محدود کند، اما فرصتی منحصر به فرد برای پیشرفت فناوری فراهم می‌آورد. به طور متوسط، چهار سیستم مستقل بزرگ (AS) در هر کشور منطقه حدود 80 درصد از جمعیت را پوشش می‌دهند، به این معنی که چند بازیگر اصلی می‌توانند تحولات چشمگیری در پذیرش فناوری‌های اینترنتی مهم در سراسر منطقه ایجاد کنند.

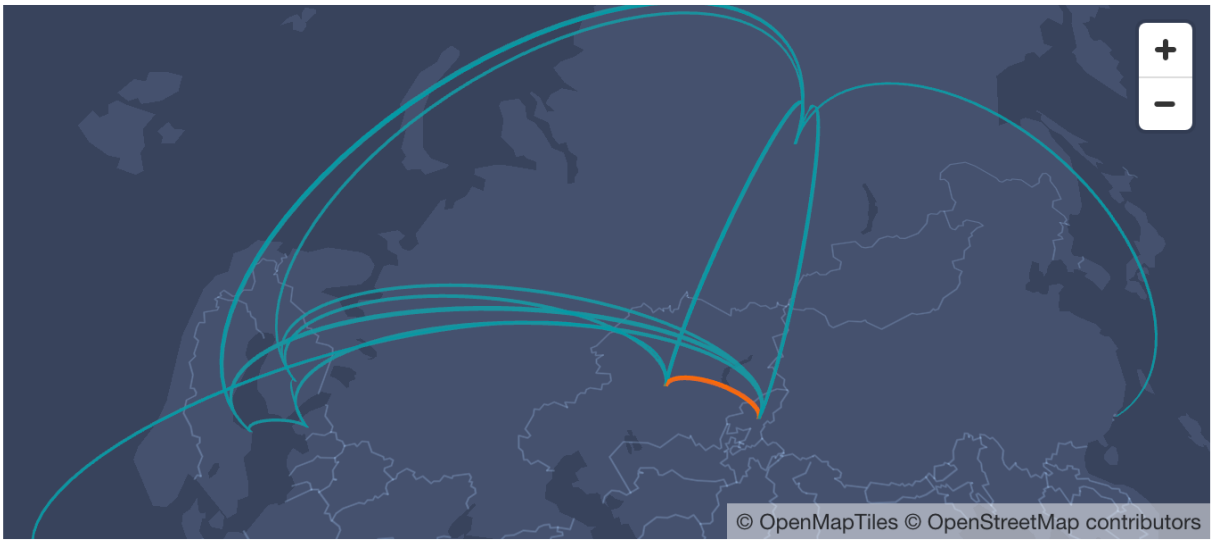


ارتباطات بین شبکه‌ای در آسیای مرکزی

با افزایش همکاری‌های درون‌منطقه‌ای در آسیای مرکزی، از جمله رشد تجارت، سرمایه‌گذاری و گردشگری، ما به بررسی شبکه‌های منطقه‌ای از منظر مسیریابی پرداخته‌ایم، با استفاده از داده‌های RIPE Atlas. تمام نقاط RIPE Atlas در کشورهای آسیای مرکزی به‌عنوان مبدا و مقصد مورد استفاده قرار گرفتند. در ترکمنستان، که هیچ نقطه متصل ندارد، میزبان‌های اضافی استفاده شدند. این پژوهش دو سال پیش انجام شد و در CAPIF 1 ارائه شد، بنابراین این بار توانستیم تغییرات از سال ۲۰۲۲ را ببینیم.

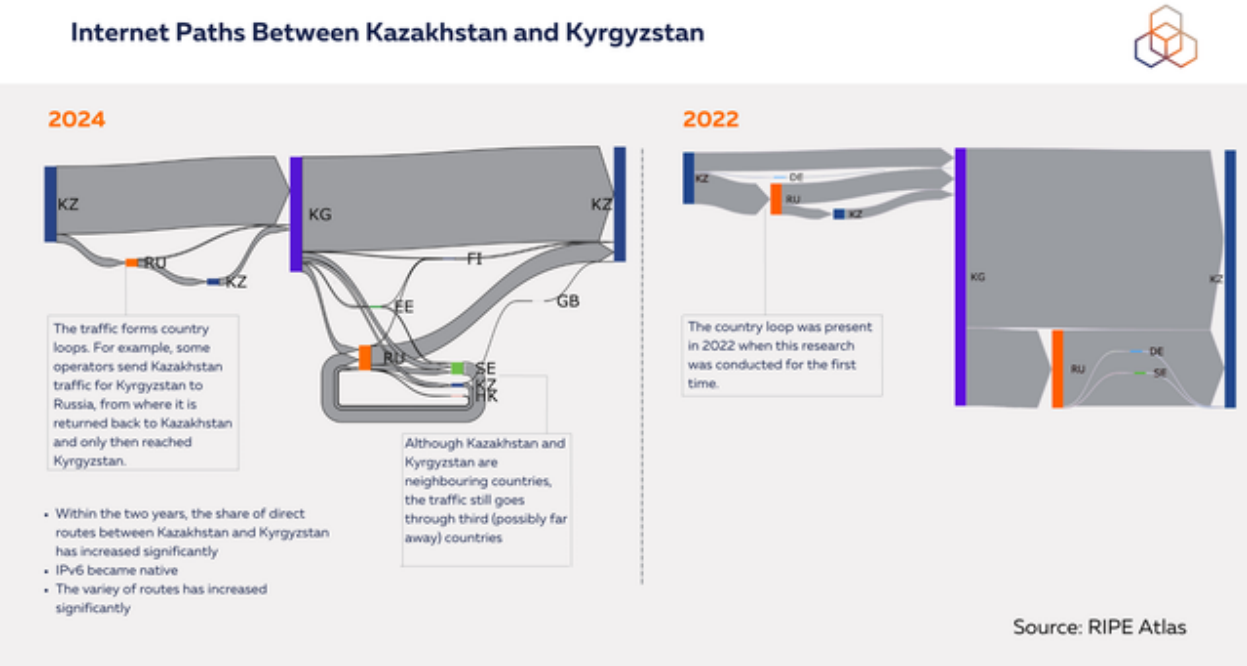
در این نقشه، جریان‌های داده ترافیک اینترنتی بین قزاقستان و قرقیزستان، و همچنین بین قزاقستان و تاجیکستان نشان داده شده است که از طریق چندین کشور عبور می‌کند. اگرچه مسیر مستقیم بین کاربران اینترنت در این کشورها بهینه‌تر است، ترافیک به دلیل نبود پیرینگ مستقیم، اغلب از مسیرهای کم‌بازده‌تر عبور می‌کند.

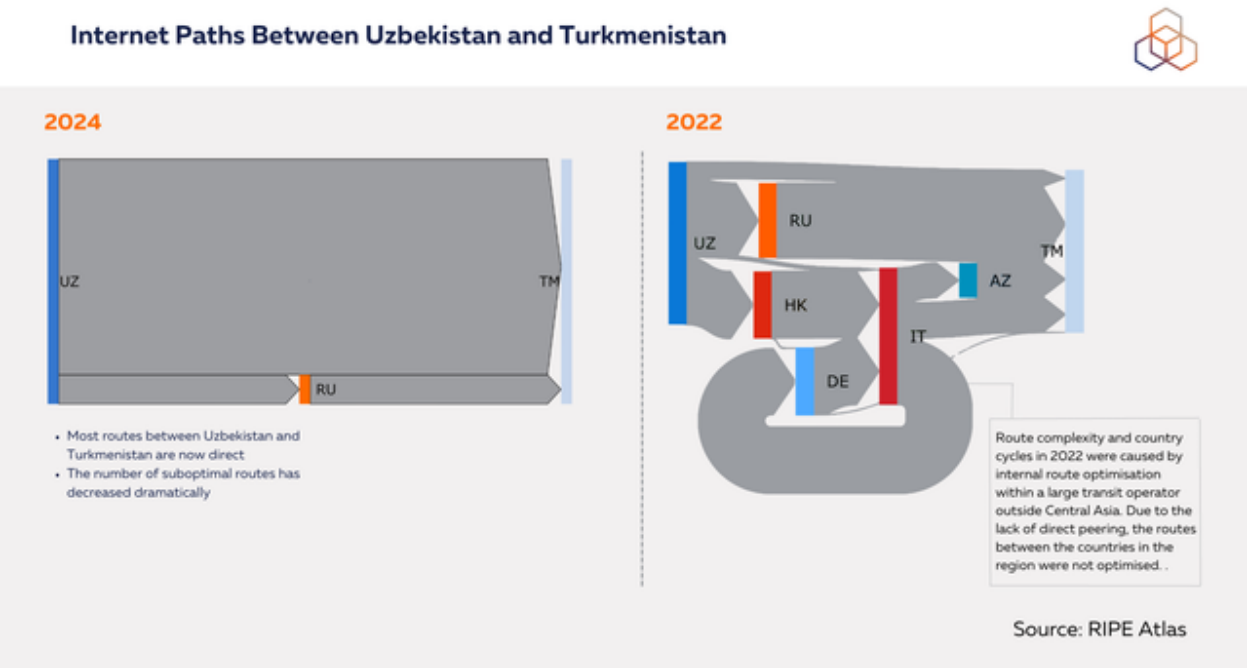
The map below illustrates the flow of Internet traffic between Kazakhstan and Kyrgyzstan, passing through multiple countries, including Russia, the UK, Finland, and others. While the most direct route between Internet users in these two countries is always preferable, traffic often takes less efficient paths due to a lack of direct peering between networks. This map highlights the routing paths and reveals the number of data flows involved in the exchange between Kazakhstan and Kyrgyzstan.



Source: RIPE Atlas • We have used a logarithmic scale to present the data

در مقایسه با سال ۲۰۲۲، بهبودهای قابل توجهی در مسیرهای بین ازبکستان و ترکمنستان رخ داده است، در حالی که مسیرهای اصلی بین قزاقستان و قرقیزستان هنوز نیاز به بهبود دارند (نمودارهای زیر را ببینید).





(عکس: نمودارهای نشان‌دهنده بهبود مسیرهای اینترنتی بین کشورهای آسیای مرکزی)

به‌طور کلی، پیشرفت‌هایی در بومی‌سازی ترافیک در منطقه و تنوع مسیرها بین کشورهای مختلف دیده می‌شود. با این حال، مسیرهای ناکارآمد در عبور ترافیک هنوز در منطقه وجود دارند. پیاده‌سازی سیاست‌ها و توافق‌های پیرینگ موثرتر می‌تواند گامی مهم در جهت بهبود ارتباطات بین شبکه‌ای در منطقه باشد.

CAPIF 3 فرصتی برای تقویت و ایجاد روابط پیرینگ جدید با شرکت‌کنندگان در این رویداد فراهم می‌کند. در طول CAPIF 3، یک ساعت برای برگزاری جلسات دوطرفه پیرینگ در نظر گرفته شده است. برای برنامه‌ریزی جلسات خود در این رویداد، می‌توانید به این صفحه مراجعه کنید.

لطفاً توجه داشته باشید که این داده‌ها بر اساس نمونه‌های RIPE Atlas است و ما هنوز نیاز به افزایش تعداد نمونه‌ها در این منطقه داریم. اگر مایلید یک نمونه فیزیکی یا مجازی (نرم‌افزاری) از RIPE Atlas در منطقه خود قرار دهید، با تیم RIPE Atlas تماس بگیرید.

امنیت مسیریابی در آسیای مرکزی

امنیت مسیریابی (Routing Security) یکی از جنبه‌های اساسی امنیت شبکه است که تضمین‌کننده تمامیت و پایداری ترافیک اینترنت جهانی می‌باشد. با پیچیده‌تر شدن شبکه‌ها، خطراتی نظیر حملات به مسیرها، نشت پیشوندها، و اشتباهات در تنظیمات پروتکل BGP افزایش می‌یابد. این حوادث می‌توانند منجر به اختلالات جدی، رهگیری داده‌ها و حتی مشکلات بزرگ‌مقیاس در سرویس‌های اینترنتی شوند.

برای مقابله با این مشکلات، زیرساخت کلید عمومی منابع (RPKI) توسعه داده شد، که به یک سیستم امنیتی حیاتی تبدیل شده است و به اپراتورهای شبکه کمک می‌کند تا تصمیمات مسیریابی خود را با اطمینان بیشتری انجام دهند. با استفاده از بررسی رمزنگاری مشروعیت اعلان‌های مسیریابی، RPKI به مدیران شبکه اجازه می‌دهد تا از وقوع اشتباهات یا حملات مخرب در مسیریابی جلوگیری کنند، که این امر امنیت و پایداری عملیاتی زیرساخت اینترنت را افزایش می‌دهد.

دو مؤلفه اصلی RPKI عبارتند از:

- مجوزدهی منبع مسیریابی (ROA): یک سند الکترونیکی امضاشده است که مشخص می‌کند کدام سیستم‌های خودمختار (AS) مجاز به اعلان پیشوندهای IP خاص هستند. ROA به عنوان یک مرجع اعتماد عمل می‌کند و به اپراتورهای شبکه اجازه می‌دهد تا منبع اطلاعات مسیریابی را بررسی کنند.

- اعتبارسنجی منبع مسیریابی (ROV): فرآیندی است که با استفاده از ROA برای بررسی اعتبار اعلان‌های مسیریابی انجام می‌شود. این فرآیند مسیرهای BGP را به سه حالت دسته‌بندی می‌کند: «معتبر»، «نامعتبر» یا «یافت‌نشده» که بسته به وجود و محتوای ROA تعیین می‌شود.

تأثیر RPKI بر امنیت اینترنت

پیش از پیاده‌سازی RPKI، سیستم مسیریابی اینترنت به‌ویژه در برابر اشتباهات تصادفی در تنظیمات و حملات مخرب آسیب‌پذیر بود. یکی از رویدادهای برجسته در سال ۲۰۰۸ اتفاق افتاد، زمانی که شرکت Pakistan Telecom (PTCL) به‌صورت اشتباهی آدرس‌های IP متعلق به YouTube را گرفت و باعث اختلال جهانی در این پلتفرم ویدئویی به مدت نزدیک به دو ساعت شد. این حادثه نشان‌دهنده آسیب‌پذیری سیستم مسیریابی جهانی بود و نیاز به تدابیر امنیتی قوی‌تر را برجسته کرد. در سال‌های بعد، حوادث دیگری که شامل شرکت‌های بزرگ مخابراتی و فناوری می‌شد، ضرورت رفع آسیب‌پذیری‌های پروتکل BGP را نشان دادند.

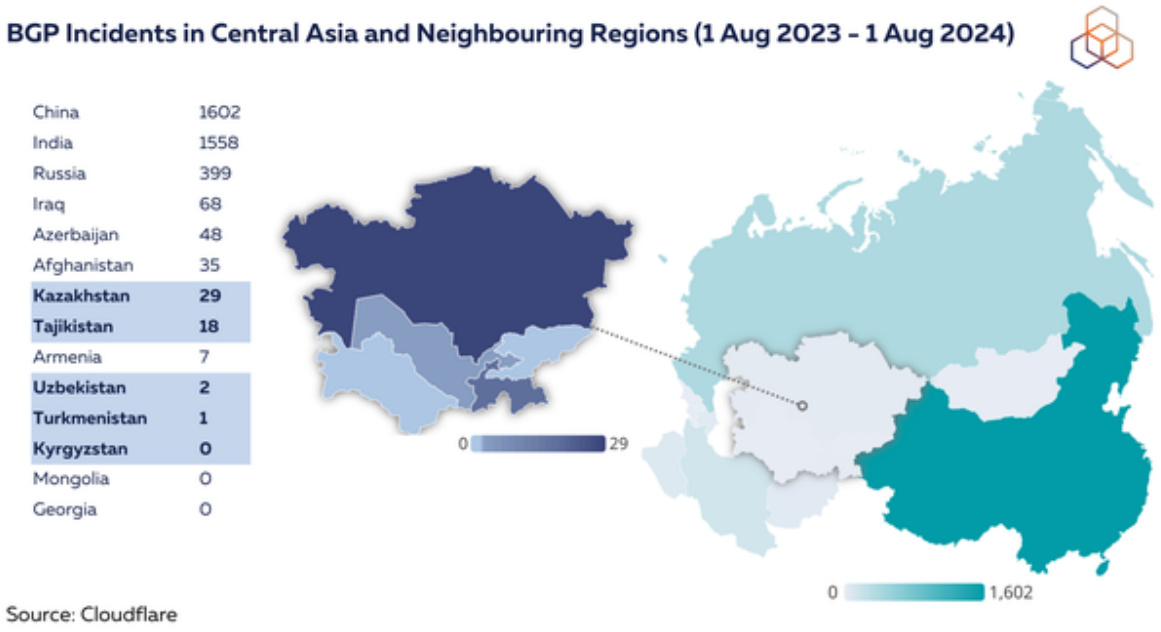
پس از پیاده‌سازی RPKI، اگرچه حوادث مسیریابی همچنان رخ می‌دهند، اما تأثیرات آن‌ها به طور قابل توجهی کاهش یافته است. برای مثال، حادثه‌ای که در تاریخ ۲۷ ژوئن ۲۰۲۴ برای Cloudflare 1.1.1.1 رخ داد، ناشی از مسیریابی نادرست بود که منجر به اختلال در خدمات شد. اعتبارسنجی منبع مسیریابی (ROV) می‌توانست از انتشار این مسیر نادرست جلوگیری کند و بدین ترتیب، عواقب این حادثه را کاهش دهد.

در یک مثال واقعی دیگر، ROV در سال ۲۰۲۳ زمانی که دولت عراق سعی در مسدود کردن برنامه تلگرام داشت، «موفق شد.» اعلام نادرست مسیر BGP باعث شد بخش بزرگی از ترافیک اینترنت جهانی مسدود شود. شبکه‌هایی که از ROV استفاده می‌کردند، این مسیرهای نادرست را رد کردند و دسترسی کاربران خود به اینترنت حفظ شد. تلگرام برای مسیرهای خود ROA ایجاد کرد، که باعث شد سیستم‌های خودمختار (AS) خارج از عراق به‌صورت خودکار تلاش‌های سرقت مسیر را رد کنند.

این مثال‌ها اهمیت پیاده‌سازی RPKI برای جلوگیری از خطاهای تصادفی و عمدی در مسیریابی و تضمین دسترسی بی‌وقفه به اینترنت را برجسته می‌کنند.

حوادث پروتکل BGP در آسیای مرکزی

حوادث مربوط به پروتکل دروازه مرزی (BGP)، به‌ویژه سرقت مسیرها، در آسیای مرکزی و مناطق همجوار به ثبت رسیده است. این حوادث می‌توانند در نتیجه اشتباهات پیکربندی یا اقدامات مخرب رخ دهند که به‌طور بالقوه منجر به تغییر مسیر ترافیک اینترنت می‌شود. تحلیل داده‌های Cloudflare در مورد حوادث BGP نشان می‌دهد که الگوهای جالبی در این منطقه وجود دارد. داده‌های ارائه‌شده شامل اطلاعاتی در مورد پیشوندهای دزدیده‌شده، تعداد عاملان حمله و تعداد کل حوادث است.



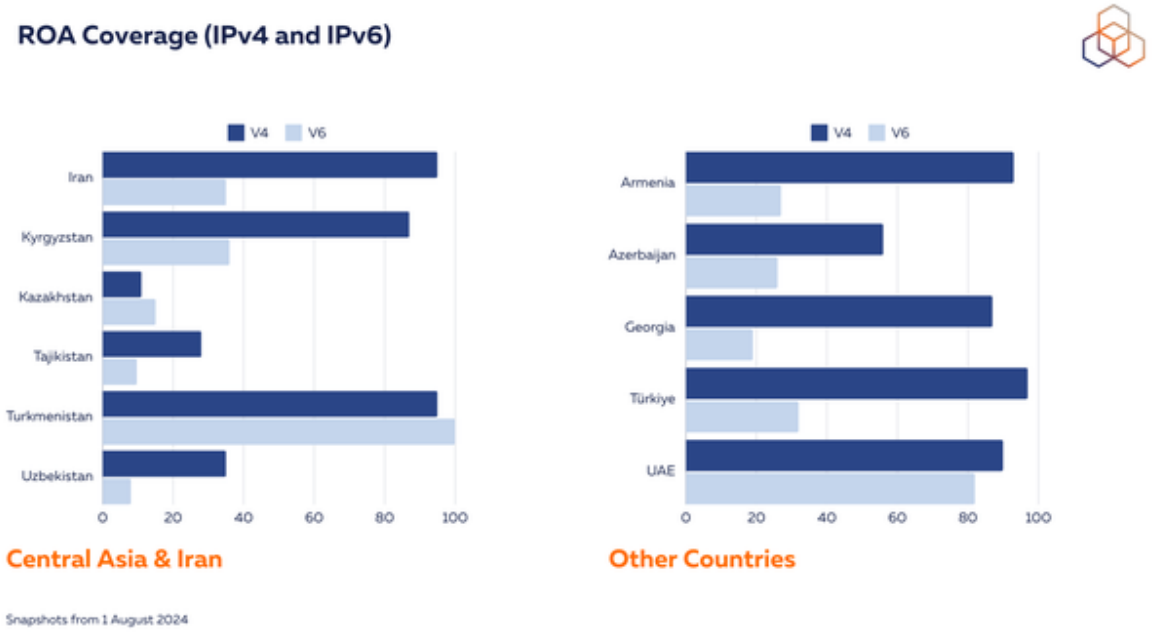
در نقشه‌ی زیر می‌توان مشاهده کرد که در کشورهایی مانند چین و هند، تعداد زیادی از این حوادث گزارش شده‌اند، در حالی که تعداد آن‌ها در کشورهای آسیای مرکزی نسبتاً کم است. هرچند تعداد حوادث BGP در این منطقه کمتر است، اما حتی یک مورد سرقت پیشوند، چه به دلیل اشتباهات پیکربندی یا اقدامات مخرب، می‌تواند منجر به اختلالات شدید یا قطع ارتباطات شود.

ماهیت جهانی و متصل مسیریابی اینترنت اهمیت تقویت امنیت BGP را نشان می‌دهد. اقدامات پیشگیرانه برای حفاظت از اشتباهات محلی و کاهش تأثیرات احتمالی حوادث در مناطق همجوار با سطح بالاتر از وقوع حادثه ضروری است. برای درک بهتر وضعیت امنیت مسیریابی در منطقه، ما به تحلیل پوشش شبکه‌های ROA و سپس پیاده‌سازی ROV در آسیای مرکزی پرداختیم.

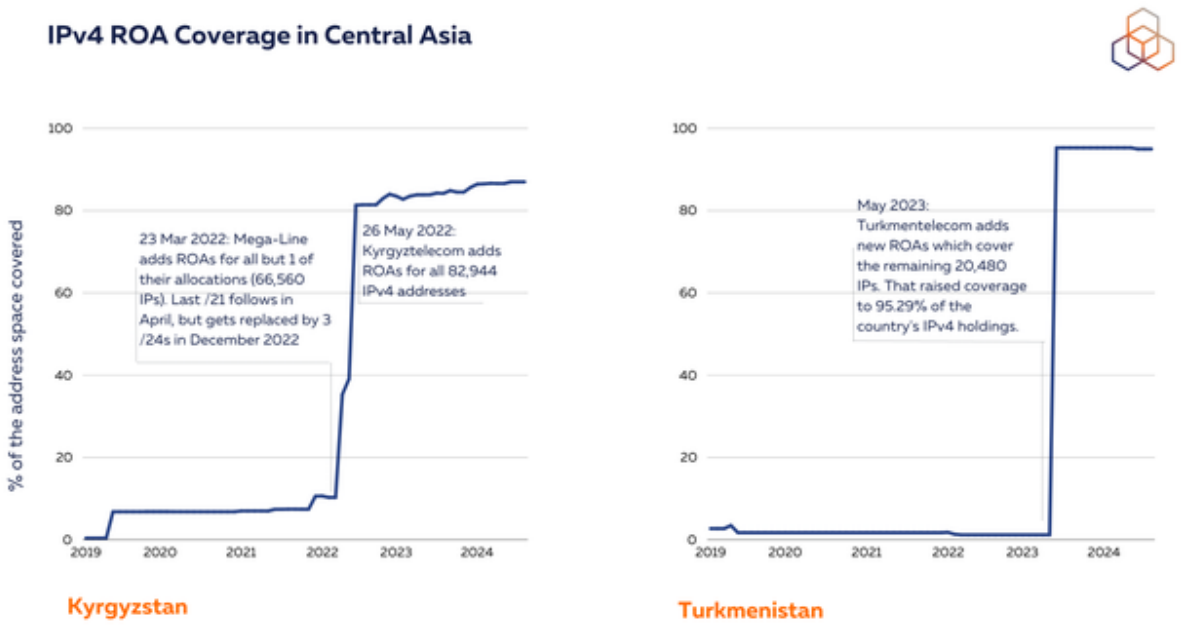
سطح پیاده‌سازی مجوزدهی منبع مسیریابی (ROA Coverage) در آسیای مرکزی

پیاده‌سازی ROA در سراسر جهان به طور قابل‌توجهی در حال گسترش است. اخیراً جامعه جهانی اینترنت به یک نقطه عطف مهم دست یافته است: طبق داده‌های NIST RPKI Monitor، بیش از ۵۰ درصد از فضای آدرس جهانی IPv4 اکنون تحت پوشش ROA قرار دارد. این یک نقطه عطف در تلاش‌ها برای بهبود امنیت جهانی مسیریابی است و نشان‌دهنده آگاهی روزافزون اپراتورهای شبکه از اهمیت RPKI در جلوگیری از سرقت مسیرهای BGP و خطاهای پیکربندی است.

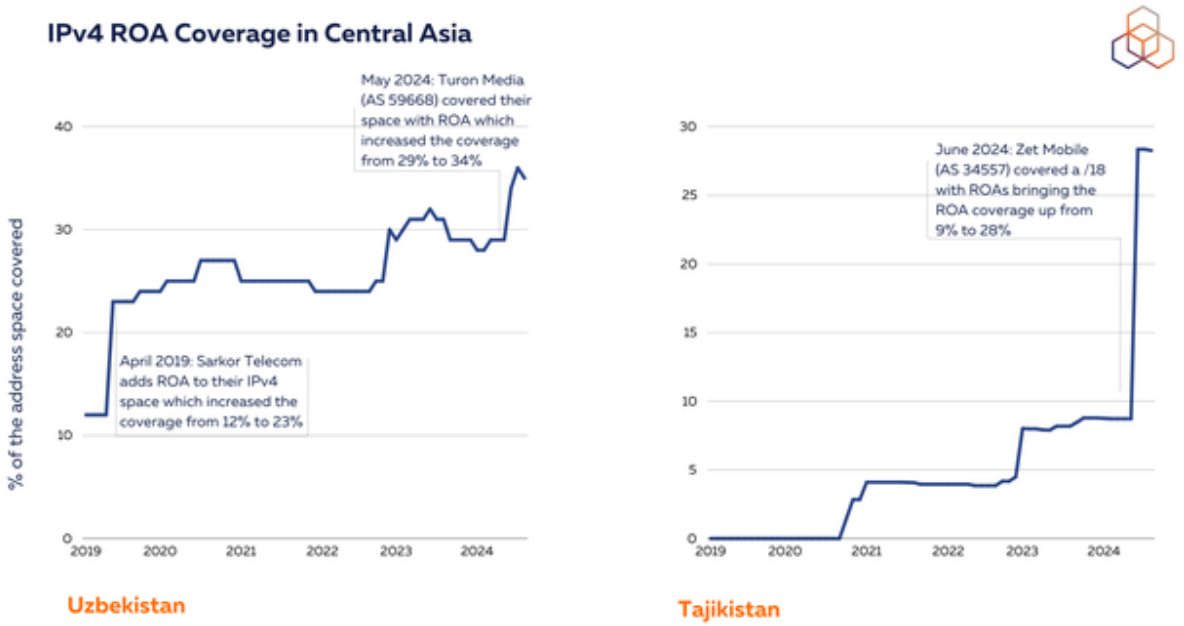
در حوضه آسیای مرکزی، پوشش ROA تصویری ناهماهنگ را نشان می‌دهد. سطح پیاده‌سازی در کشورهای منطقه از ۱۰ درصد تا نزدیک به ۱۰۰ درصد برای فضاهای آدرس IPv4 و IPv6 متغیر است. این تفاوت بزرگ نشان می‌دهد که در حالی که برخی از شبکه‌های آسیای مرکزی در خط مقدم پیاده‌سازی این اقدامات امنیتی هستند، دیگران هنوز در مراحل ابتدایی اجرای آن قرار دارند.



بخش بزرگی از پیشرفت‌ها که در قرقیزستان و ترکمنستان مشاهده می‌شود، طی دو سال اخیر به دست آمده است. در قرقیزستان، شرکت Mega-line در مارس و دسامبر ۲۰۲۲ ROA را در فضای IPv4 خود پیاده‌سازی کرد و Kyrgyztelecom نیز در مه همان سال پیاده‌سازی خود را تکمیل کرد. در ترکمنستان، Turkmentelecom در مه ۲۰۲۳ فضای آدرس‌های پوشش‌نیافته خود را با ROA تکمیل کرد که به تقریباً ۱۰۰ درصد پوشش IPv4 منجر شد (به نمودار مراجعه کنید).



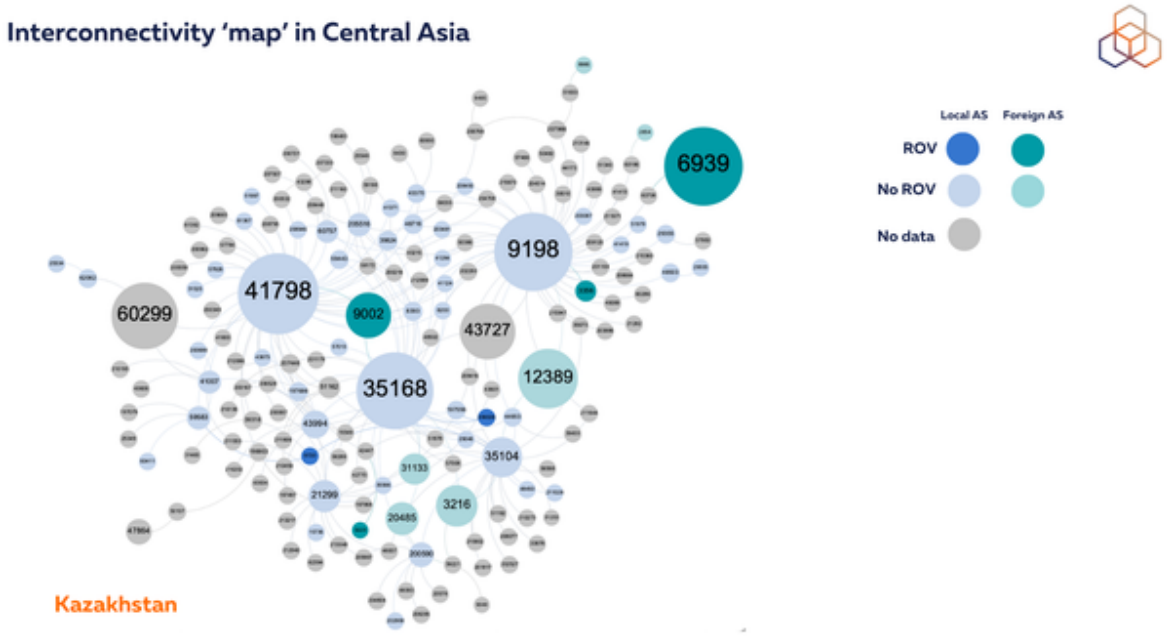
در ازبکستان، سطح پوشش ROA در آوریل ۲۰۱۹ افزایش یافت، زمانی که شرکت Sarkor Telecom اقدام به پیاده‌سازی ROA کرد. افزایش بعدی در ماه مه ۲۰۲۴ رخ داد، هنگامی که شرکت Turon Media نیز ROA را پیاده‌سازی کرد. در تاجیکستان، سطح پیاده‌سازی ۱۰ درصد افزایش یافت، زمانی که شرکت Zet Mobile (که قبلاً با نام Tacom شناخته می‌شد) ROA را به فضای آدرس‌های IP خود اضافه کرد.

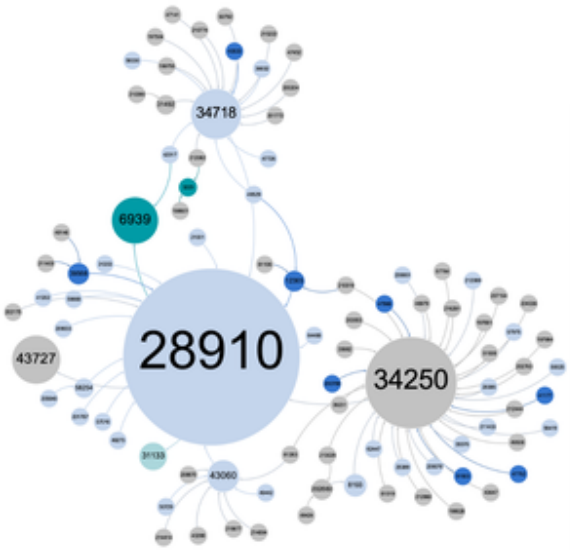


اعتبارسنجی منبع مسیریابی (ROV) و ارتباط سامانه‌های مستقل

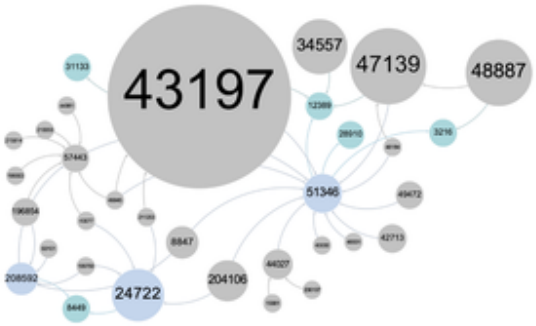
به‌عنوان «گام دوم» در تضمین امنیت مسیریابی از طریق سیستم RPKI، اعتبارسنجی منبع مسیریابی (ROV) بررسی می‌کند که آیا اعلان‌های مسیریابی با مجوزهای ذکرشده در ROA همخوانی دارند یا خیر.

ما پیاده‌سازی ROV را در منطقه با استفاده از ابزار RoVISTA که ارزیابی‌هایی بر اساس تعداد پیشوندهای نامعتبر RPKI که یک سامانه مستقل (AS) می‌تواند به آن‌ها دسترسی داشته باشد، تجزیه و تحلیل کردیم.

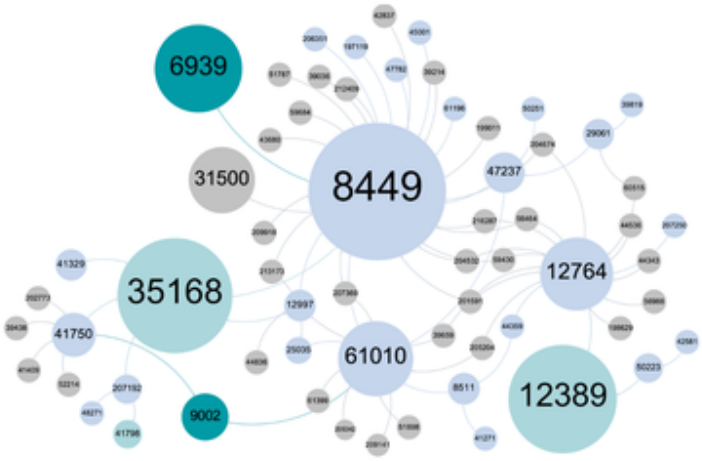




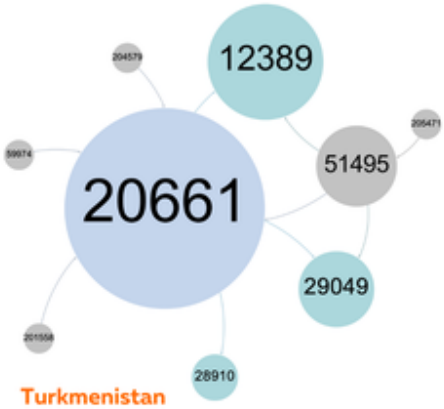
Uzbekistan



Tajikistan



Kyrgyzstan



Turkmenistan

نتایج به گونه‌ای مصور شده است که اندازه هر سامانه مستقل (AS) نشان می‌دهد که این شبکه چه نقشی در مسیریابی اینترنتی ایفا می‌کند. در نمودارهای زیر می‌توان دید که گروه نسبتاً کوچکی از سامانه‌های مستقل (AS) در منطقه نقش بسیار مهمی در چشم‌انداز مسیریابی ایفا می‌کنند.

پیاده‌سازی ROV به‌ویژه برای چنین شبکه‌هایی اهمیت دارد. این سیستم نه‌تنها به حفاظت از مشتریان خودشان کمک می‌کند، بلکه هنگامی که سامانه‌های مستقل بزرگ ROV را پیاده‌سازی می‌کنند، به طور خودکار از شبکه‌های کوچک‌تری که مستقیماً به آن‌ها متصل هستند نیز در برابر تهدیدات مسیریابی محافظت می‌کنند. این اثر جانبی اهمیت پیاده‌سازی ROV توسط اپراتورهای بزرگ شبکه را برای بهبود اکوسیستم امنیتی تعاملات بین شبکه‌ای برجسته می‌کند.

با این حال، نمودارها نشان می‌دهند که اکثر شبکه‌های مرکزی در آسیای مرکزی هنوز ROV را پیاده‌سازی نکرده‌اند، حتی در کشورهایی که سطح پیاده‌سازی ROA نسبتاً بالاست. این ممکن است به دلیل کمبود دانش در مورد پیاده‌سازی ROV باشد، همان‌طور که پاسخ‌دهندگان آخرین نظرسنجی RIPE NCC (که در سال ۲۰۲۳ بین اعضای RIPE NCC در اروپا، خاورمیانه و آسیای مرکزی انجام شد) به آن اشاره کردند.

ابتکارات دولتی برای پیاده‌سازی RPKI

پذیرش RPKI، از جمله اجرای ROA و ROV، به طور فزاینده‌ای نه تنها توسط مهندسان شبکه بلکه در سطوح دولتی نیز به عنوان یک اقدام حیاتی شناخته می‌شود. سیاست‌های دولتی نقش مهمی در تسریع پیاده‌سازی این اقدامات امنیتی و تقویت تاب‌آوری کلی زیرساخت اینترنت ایفا می‌کنند.

به عنوان مثال، در ایالات متحده، کاخ سفید نقشه راهی را منتشر کرد که در آن RPKI به عنوان راه‌حلی بالغ برای رفع آسیب‌پذیری‌های BGP در نظر گرفته شده است. این برنامه جامع اقداماتی را برای تمام ارائه‌دهندگان خدمات شبکه شامل می‌شود، از جمله آن‌هایی که شبکه‌های سازمانی را مدیریت می‌کنند یا مالک منابع IP هستند.

علاوه بر این، کمیسیون فدرال ارتباطات ایالات متحده (FCC) پیش‌تر به ارائه‌دهندگان خدمات اینترنتی توصیه کرده بود که نقشه راهی برای مدیریت ریسک‌های مرتبط با امنیت BGP تدوین کرده و هر ساله آن را به‌روز کنند. این نقشه‌ها باید شامل استراتژی‌هایی برای پیاده‌سازی ROA و ROV باشند.

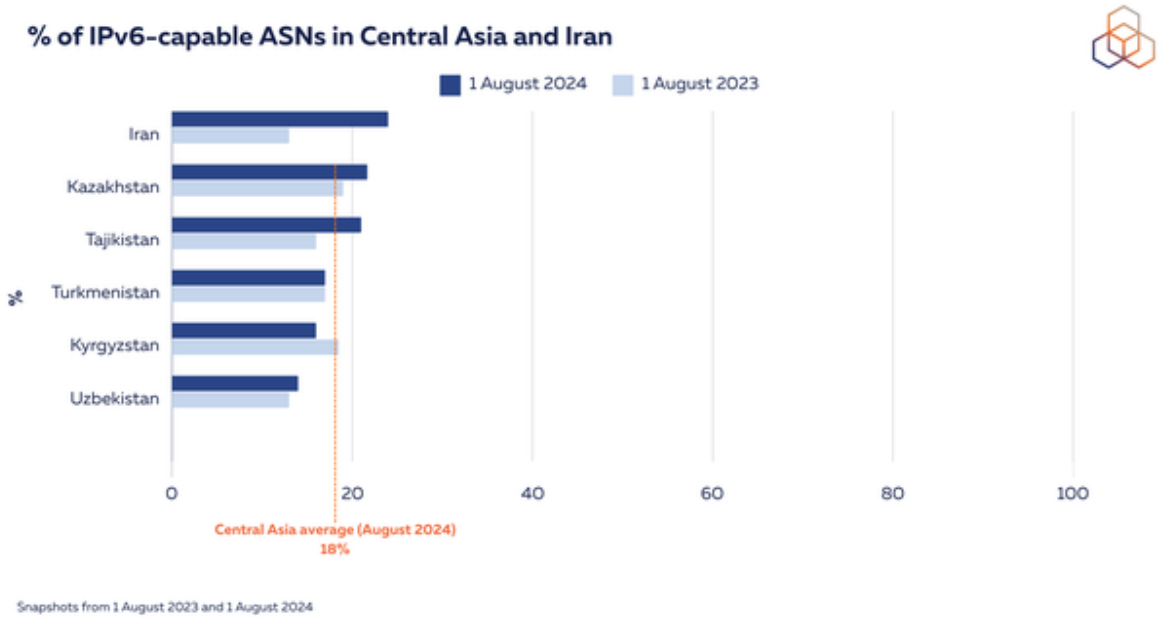
این اقدامات بر نقش دولت‌ها در تقویت امنیت مسیریابی تأکید دارد. دولت‌های منطقه آسیای مرکزی می‌توانند اقدامات مشابهی را اتخاذ کنند، مانند تعیین دستورالعمل‌های مشخص و تعیین ضرب‌الاجل برای پذیرش RPKI توسط ارائه‌دهندگان خدمات اینترنتی و دیگر اپراتورهای شبکه.

توسعه IPv6 در منطقه

با رشد سریع اقتصادی در آسیای مرکزی، برای اپراتورها مهم است که در راه‌حل‌های آینده‌نگر سرمایه‌گذاری کنند. علاوه بر استراتژی‌های امنیتی، باید ظرفیت‌های لازم برای پشتیبانی از تعداد بیشتری از کاربران توسعه یابد، که در اینجا IPv6 نقش کلیدی دارد. گذار به IPv6 راه‌حلی برای رشد بلندمدت اینترنت است، به ویژه با توجه به محدودیت منابع IPv4.

ما به بررسی قابلیت و سطح پیاده‌سازی IPv6 در منطقه پرداختیم. به طور متوسط، درصد سامانه‌های مستقل (ASNها) که از IPv6 پشتیبانی می‌کنند (به عنوان درصد ASNهایی که حداقل یک پیشوند IPv6 را مسیریابی می‌کنند) در آسیای مرکزی حدود ۱۸ درصد است. برای مقایسه، در کشورهای اتحادیه اروپا این رقم حدود ۳۹ درصد است که فاصله قابل توجهی در آمادگی برای پذیرش IPv6 را نشان می‌دهد. افزایش کمی در توانایی استفاده از IPv6 در قزاقستان، تاجیکستان و ازبکستان در مقایسه با سال گذشته مشاهده شده است که نشان‌دهنده بهبودهایی در این زمینه است.

اگرچه توانایی استفاده از IPv6 نشان‌دهنده اعلام پیشوندهای IPv6 در جداول مسیریابی جهانی است، پیاده‌سازی IPv6 منعکس‌کننده این است که آیا کاربران واقعاً از IPv6 در شبکه‌های خود استفاده می‌کنند یا خیر. این تفاوت مهم است برای تعیین سطح واقعی پیاده‌سازی IPv6.



داده‌های ارائه‌دهندگان محتوای بزرگ (CDN) سطوح مختلفی از پیاده‌سازی IPv6 را در کشورهای آسیای مرکزی و مناطق همجوار نشان می‌دهند. قزاقستان در این منطقه پیشرو است، با نرخ‌های پیاده‌سازی بین ۱۳٪ (فیس‌بوک) تا ۱۷٪ (Cloudflare و گوگل)، که این اختلافات نشان‌دهنده تفاوت‌های شبکه‌های داخلی کشور است. در قرقیزستان، این رقم حدود ۴٪ و در ازبکستان تقریباً ۳٪ است. هر دو کشور در مقایسه با قزاقستان سطوح پایین‌تری از پیاده‌سازی را نشان می‌دهند.

نکته جالب این است که کشور همسایه ایران، سطوح بسیار بالاتری از پیاده‌سازی IPv6 را نشان می‌دهد، اما نتایج ناهماهنگ دارد: ۷۶٪ (فیس‌بوک)، ۲۲.۶٪ (Cloudflare) و ۱۶٪ (گوگل). این اختلافات بزرگ اهمیت فهم روش‌های اندازه‌گیری استفاده‌شده توسط CDNهای مختلف را نشان می‌دهد. Cloudflare درصد استفاده از IPv6 را به عنوان (درخواست‌های IPv6 / درخواست‌ها برای محتوای دوگانه) محاسبه می‌کند، که معیار خاصی از استفاده IPv6 در میان مشتریانی که هر دو IPv4 و IPv6 را پشتیبانی می‌کنند، ارائه می‌دهد. در مورد گوگل و فیس‌بوک، روش آن‌ها برای محاسبه نرخ‌های پیاده‌سازی کمتر شفاف است، که ممکن است به تفاوت‌های موجود در داده‌های ارائه‌شده کمک کند.

با وجود تفاوت‌های موجود در روش‌های اندازه‌گیری، به طور کلی سطوح پیاده‌سازی IPv6 در آسیای مرکزی پایین است.

چالش‌های پیاده‌سازی IPv6

بر اساس نظرسنجی RIPE NCC در سال ۲۰۲۳، عوامل زیر به عنوان چالش‌های اصلی پیاده‌سازی IPv6 توسط پاسخ‌دهندگان از اروپا، خاورمیانه و آسیای مرکزی ذکر شده است:

- برابری عملکرد بین IPv4 و IPv6: این عامل به‌عنوان اصلی‌ترین مشکل در پیاده‌سازی IPv6 توسط ۴۶٪ از پاسخ‌دهندگان مطرح شد. این رقم در اروپای مرکزی به ۵۴٪ و در اوراسیا به ۵۶٪ افزایش می‌یابد.

- نیاز به تغییر نگرش در مورد :IPv4۴۱٪ از پاسخ‌دهندگان این مسئله را به‌عنوان یک مانع مطرح کرده‌اند، به‌ویژه در آلمان (۵۶٪) و لهستان (۶۱٪).

- کسب دانش در مورد پیاده‌سازی‌های خاص: حدود ۴۰٪ از پاسخ‌دهندگان به این مشکل اشاره کرده‌اند، که نشان‌دهنده نیاز به اطلاعات و آموزش بیشتر است.

این داده‌ها تصویری پیچیده از چالش‌های پیاده‌سازی IPv6 نه تنها در آسیای مرکزی، بلکه در سایر مناطق جهان ارائه می‌دهند. پیاده‌سازی این فناوری نیازمند تلاش‌های هماهنگ از طریق ابتکارات دولتی، سرمایه‌گذاری در زیرساخت‌ها و افزایش آگاهی است.

اگر مایل به افزایش دانش خود در مورد IPv6 و RPKI هستید، می‌توانید به دوره‌های RIPE NCC Academy مراجعه کنید. ما همچنین دوره‌ای در زمینه اصول IPv6 به زبان روسی منتشر کرده‌ایم و آموزش‌های مرتبط با IPv6 را پس از این رویداد در بیشکک ارائه خواهیم داد—در اینجا ثبت‌نام کنید.

نتیجه‌گیری

پیاده‌سازی فناوری‌های کلیدی مانند RPKI و IPv6 گامی مهم در جهت تضمین امنیت و پایداری اینترنت در آسیای مرکزی است. با رشد سریع دیجیتالی منطقه، رسیدگی به مشکلات مسیریابی از طریق ROV و افزایش استفاده از IPv6 به‌عنوان گام‌های ضروری شناخته می‌شوند. اگرچه پیشرفت‌هایی در اجرای ROA به‌ویژه در کشورهایی مانند قرقیزستان و ترکمنستان حاصل شده است، چالش‌هایی مانند کمبود دانش و نگرانی‌های مربوط به ROV همچنان باقی مانده است. با اولویت دادن به این بهبودها، شبکه‌های آسیای مرکزی می‌توانند برای مقابله با تهدیدات مسیریابی آماده‌تر شوند و پایداری دیجیتالی طولانی‌مدت را تضمین کنند.

ما خوشحال می‌شویم که نظر شما را در مورد این پژوهش‌ها بشنویم—با ما در CAPIF 3 در ارتباط باشید. این پژوهش توسط محقق ارشد RIPE NCC، کاسیم لوان، در روز سه‌شنبه، ۲۴ سپتامبر ارائه خواهد شد.