BGP Watch : Collaborative BGP Routing Analysis, Monitoring, and Incident Response Platform

Platform Overview & Importance for South Asia

A Collaborative Global BGP Routing Analyzing and Diagnosing Platform developed in partnership with 38 global institutions across 27 economies.

Presenter: NREN

Reference Document: https://bgpwatch.cgtf.net/#/document

APNIC FOUNDATION

APAN

Tsinghua University

NREN

Project's Background

01 Initiative
June 2020 – May 2023

Previous Project:

- Joint Research on IPv6 Network Management: Research Development and Demonstration
- Funded by National Key Research and Development Program of China

02 Improvement
Feb. 2022 – Aug. 2023

Previous Project:

- Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform
- Co-founded by APNIC Foundation and Tsinghua University

03 Enhancement
Dec. 2023 – June. 2025

Previous Project:

- An Extension of the Ongoing Project "Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform"
- Co-founded by APNIC Foundation and Tsinghua University

04 Innovation
Dec. 2025 – Nov. 2026

Current Project:

- Learning fine-grained interdomain routing policy in BGP through AI
- Co-founded by Tsinghua University, APNIC Foundation and APAN Grant

DragonLab | BGPWatch

Current Project Partners

What is BGP Watch?

Global Monitoring System

BGPWatch is a major cyberspace security initiative led by Tsinghua University. It acts as an open governance diagnostic sandbox, monitoring prefix hijacking, route leaks, and source IP spoofing on a global scale.

Recognized in 2025 as an Outstanding Case at the World Internet Conference.

Unified Diagnostic Pillars

Designed with four core modules: Anomaly Detection (tracking hijacks & leaks), AS Dashboard (comprehensive ASN registries), Routing Path (multi-angle topology maps), and Subscriptions (proactive automated warning alerts via email).

Co-funded by the National Key R&D Program of China and the APNIC Foundation.

Free Access & Open Source

BGP Watch provides free public access to global BGP routing security data and is built on an open-source model. It enables researchers, network operators, and the Internet community to collaboratively detect, analyze, and mitigate malicious routing manipulation worldwide.

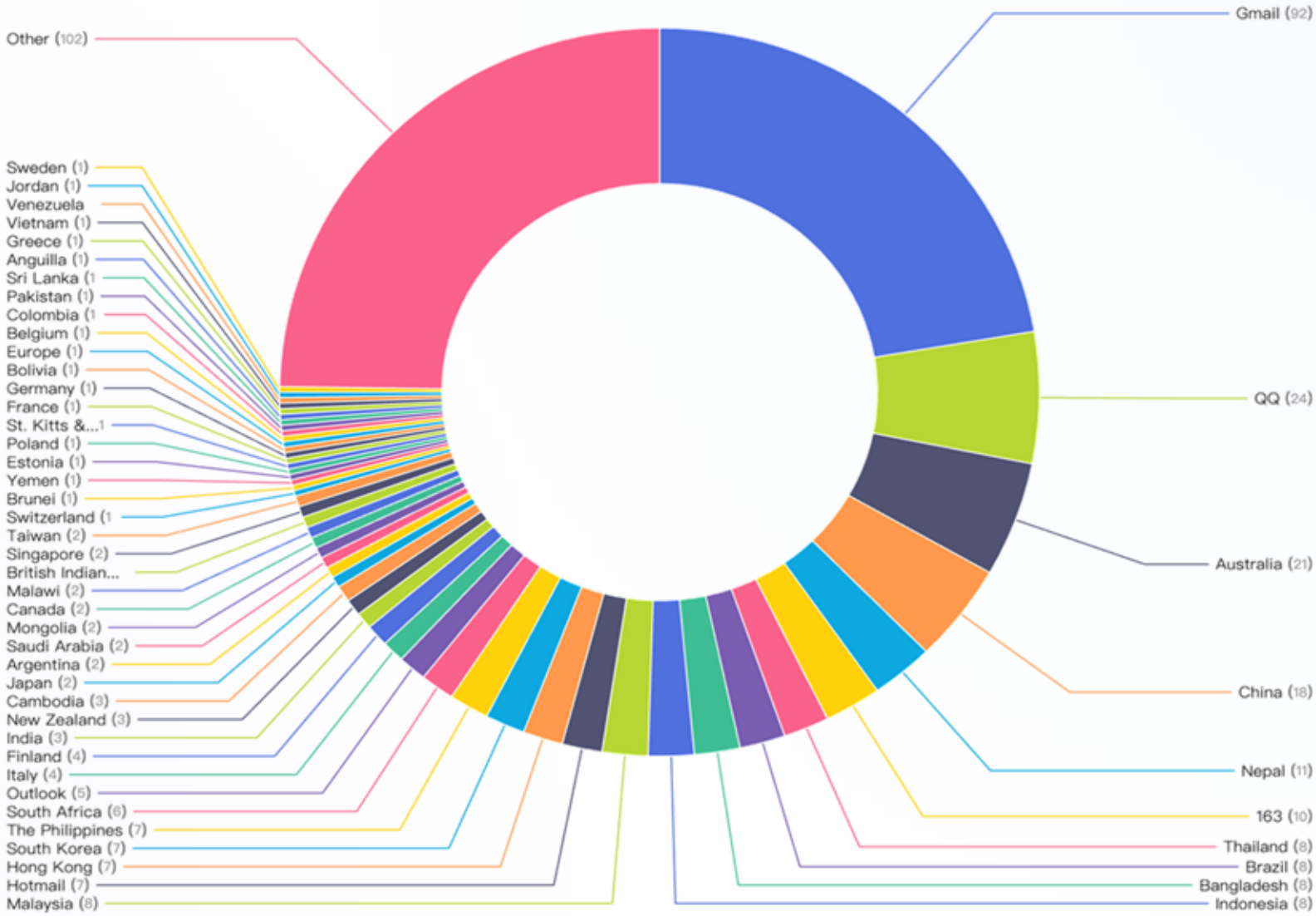
Common Good Mapping database

Designed to Integrates data from PeeringDB and other public Internet infrastructure sources to provide an open, community-driven mapping of global networks. Supports free access to network topology information for research, routing analysis, and Internet resilience.

Current BGP Watch User Distribution

According to the email information, grouped by economy and email provider

Totally 412 users, from 46 economies



Four Pillars of BGP Watch

Anomaly Detection

Auto-scans and classifies prefix hijacks, sub prefix hijacks, and unauthorized route leaks across global routing updates.

UI Dashboard

Aggregates ASN statistics, RPKI ROA status, daily bogon metrics, and peer connectivity graphs.

Routing Path

Provides forward, reverse, and bidirectional path tracing alongside active route instability/jitter monitoring.

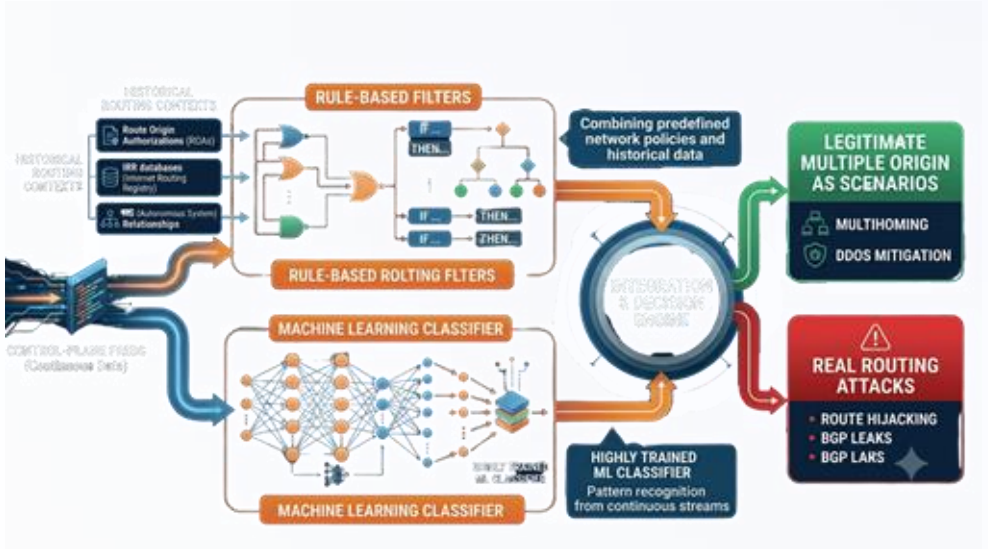
PeeringDB

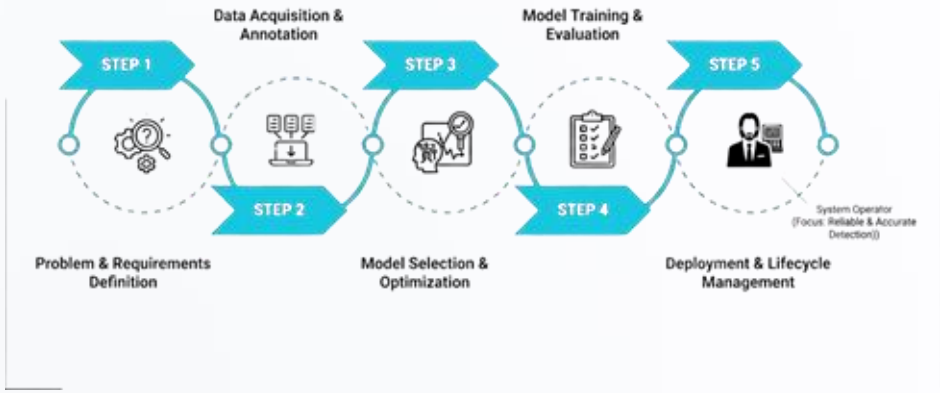
Offers alerts for prefix changes, peer fluctuations, and weekly reports triggered immediately upon discovery.

Proactive Detection Mechanisms

Hybrid ML and Rule-Based System

To differentiate between legitimate Multiple Origin AS scenarios (like multihoming or DDoS mitigation) and real attacks, BGP Watch combines rule-based filters with a highly trained Machine Learning classifier.
Historical routing contexts such as Route Origin Authorizations (ROAs), IRR databases, and AS relationships are integrated directly into control-plane feeds for continuous classification.





Auto-Detecting AI Stream Analysis

Standard Static Databases Fail: Static lists of unallocated or private IP blocks (Bogon lists) quickly go stale in high-speed global tables.

The AI Solution: BGPWatch utilizes an **auto-detecting AI engine** that continuously parses incoming real-time BGP streams. It dynamically detects when reserved or unassigned address space leaks into public tables.
This allows BGPWatch to flag leaks without requiring manual lookup rules for every newly allocated prefix block.

Dynamic Data Plane Validation

≥0.7

Correlation Coefficient

Probing and Reachability Verification

When a suspicious routing manipulation is flagged, BGPWatch deploys data-plane probes from Viewpoints to calculate a correlation coefficient between hijack events and server reachability:

$$\text{Correlation} \geq 0.7 \rightarrow \text{High Possible Hijack}$$

Results are dynamically bucketed into 5 states: Not Done, No Result, High Possible, Low Possible, or Not Hijack.

Unified Routing Path Integration

Forward Routing

Traces the forward route to a destination from select NRENs, highlighting ISP transits and R&E pathways.

Reverse Routing

Provides topology mapping on geographic coordinates to verify how incoming traffic targets your networks.

Bi-Directional Path

Highlights asymmetry by showing both paths side-by-side, helping identify path optimization problems.

Jitter Monitoring

Identifies active prefixes and peers with extreme update frequencies to isolate unstable networks.

Areas & Cybemap Topology

Multi-Dimensional Coordinate Mapping

The Areas path hijacking algorithm renders complex global BGP connection trees into interactive Cybermap coordinate layers.

The system splits the canvas into a 4x4 grid spanning 16 ASN ranges.

Suspect links flash in red, affected links are highlighted in orange, and victim ASNs show as blue nodes.

The Instant Probe Trigger (10)

No Manual Path Edits: BGP routing paths are entirely auto-scanned in real time from public collectors (RouteViews, RIPE RIS, CGTF RIS). Operators cannot manually inject or alter paths.

Instant Action: The second BGPWatch's AI detects a suspicious path transition, it automatically triggers a batch of **10 or more targeted data-plane probes** from anchor Viewpoints.

This 10-probe batch instantly tests hop integrity and confirms if traffic is actively being intercepted or dropped.

Section Dashboard - Peering Relationships

IPv4/IPv6 Peer Visualization

The Areas path hijacking algorithm renders complex global BGP connection trees into interactive Cybermap coordinate layers.

Network Topology Graph

Provider relationship
Peer relationship
Customer relationship
Unknown relationships

Top 10 Rankings

By Providers
By Peers
By Customers
By Peer Economy

Quantitative Metrics

Export prefix count
Import prefix count
AS Customer Cone calculation

Interactive Actions

Hover for prefix exchange details
Click ASN for dashboard redirect
Filter by relationship type

Realworld Incidents

1. Facebook’s Global Disappearance (October 2021)

During routine maintenance, Facebook engineers accidentally sent a command that severed all BGP route announcements to their data centers.

- The Impact: Facebook, Instagram, WhatsApp, and Messenger vanished from the global internet routing table for roughly six hours.
- The Chaos: Because physical badge readers and internal communication networks relied on the same DNS and network infrastructure, technicians were physically locked out of server rooms while trying to fix the routing issue.

2. Vodafone’s 34,000-Route Leak (April 2021)

Indian ISP Vodafone Idea (AS55410) mistakenly announced over 34,000 networks that did not belong to it.

- The Impact: Inbound traffic to Vodafone Idea spiked to 13 times its normal volume, overloading their routers and swallowing user traffic into a massive internet "black hole".
- Affected Targets: Major services including Google, Akamai, Deutsche Telekom, Orange, and Telefónica suffered widespread regional outages affecting over 3,500 companies globally.

3. The Allegheny/Verizon/Cloudflare Traffic Jam (June 2019)

A regional steel company in Pennsylvania (Allegheny Technologies) and a small local ISP accidentally leaked thousands of optimized BGP routes to Verizon.

- The Impact: Verizon blindly accepted the bogus routes without filtering and re-announced them globally.
- Affected Targets: Traffic bound for major internet platforms—most notably Cloudflare—was funneled through a tiny local ISP pipe entirely incapable

Step-by-Step UI & Navigation Guide

1. Register Account

Access bgp watch.cgtf.net, input username, password, and active email in registration popup.

2. Confirm Activation

Click the secure validation link received in your mailbox sent directly from sec@cgtf.net.

3. Automated Login

Your browser automatically authenticates, logging you directly into the diagnostic dashboard.

4. Search Dashboard

Use the query bar to lookup ASNs or prefixes to generate real-time metrics and charts.

Live UI Demo, Grids & Login Experience

Self-Service Registration

New operators click the **Register** button to trigger the modal interface. Fields include Username, Password, and Email. Duplicate usernames immediately throw a "Duplicate Username" error.

Pro Tip: Check your spam folder if the activation email from sec@cgtf.net does not land within 2 minutes.

Customizable Grids

Once authenticated, the **Basic Grid** becomes fully customizable. Operators click the "Pen" icon to delete, drag, and reorganize metrics blocks, then click the "Checkmark" to exit edit mode.

Additional options like API-KEY Settings and email alert alerts unlock on login.

Highly Customizable Grid

Once authenticated, the main Dashboard becomes fully editable. Operators can click the "Pen" icon to delete, drag, and reorganize metrics panels, then click the "Checkmark" to exit edit mode.

Allows engineers to position their specific peer paths and active bogon charts at the top of the grid.

Advanced Features Opened

A logged-in account opens advanced, non-public modules: Subscription settings (ASN or Prefix alert modes), custom API-KEY setups, and detailed email alert notifications.

Provides access to tools including Cyber map coordinates and automated CSV downloads.

Operators who contribute VPs

Data Ingestion Frequencies

Data Source / Type	Retrieval Cycle	Processing Update Frequency
BGP Routing Feeds (Routeviews, RIPE, CGTF)	Real-Time Streams	Real-Time AI Anomaly Detection updates
RPKI ROA Registries	Real-Time Streams	Immediate matching validation matching
WHOIS, RIR, CAIDA Datasets	UTC Daily Batch	Updates completed daily by UTC
PeeringDB Registry	UTC Daily Batch	Updated within daily AS profiles
Source Spoofing Detection	Periodic Testing	Updated manually every several months

What is a VP (View Point)

What is a Viewpoint (VP)?

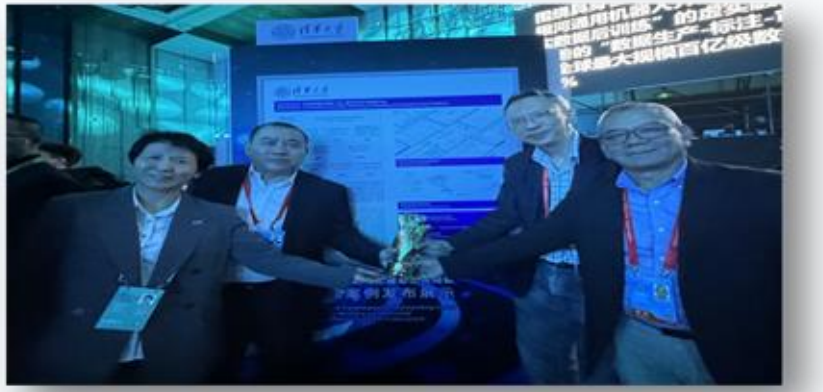
View Points (VPs) are the diagnostic eyes of BGP Watch. They consist of global collector peers and active Looking endpoints hosted by participating networks.
The more VPs connected to BGP Watch, the greater the global routing visibility and the faster the system's AI can isolate network hijackers.

Collector Peering

Peering: Network are make in collaborations with the contributors.

Points: Operators who contribute VPs can set the points in details and set it but there is a default value that needs to be there.

Project's Recognitions



01 **Nov 2025**

- World Internet Conference
- One of the 12 **Outstanding Cases** of the "Practice Cases of Jointly Building a Community with a Shared Future in Cyberspace"

02 **Dec 2025**

- Office of Cyberspace Affairs Commission of Beijing Municipal
- International Cooperative Research and Demonstration of IPv6-based Cyberspace Governance
- **First Prize** of "Excellent Cases of Large-scale Deployment and Application of IPv6"

Questions & Answers

BGP Watch is under continual global development to keep the internet secure and robust.

Join our routing governance community today.

https://bgpwatch.cgtf.net

sec@cgtf.net