MANRS – improving routing security together

APRICOT, FIRST TC

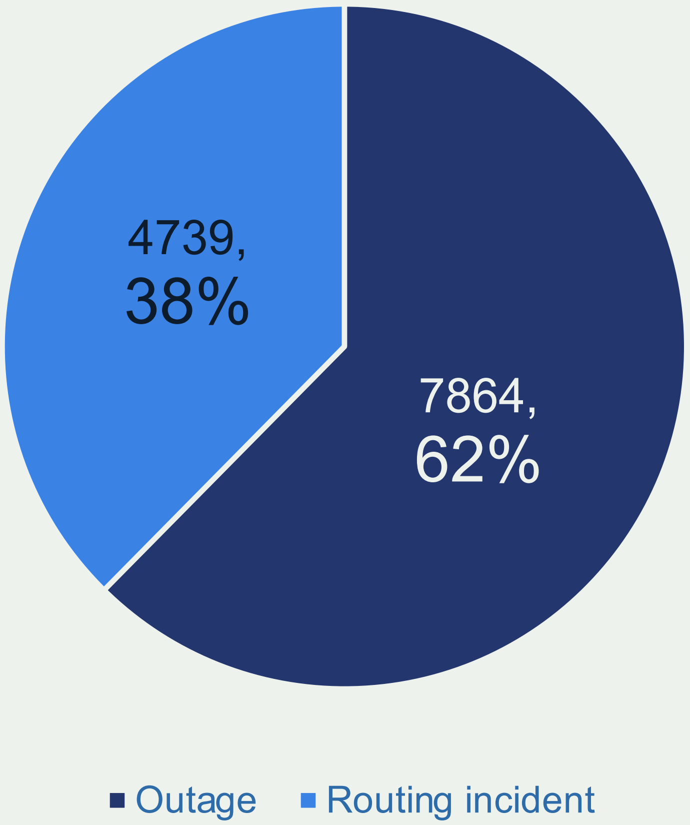
Andrei Robachevsky

robachevsky@isoc.org

There is a problem

- 12,600 total incidents (either outages or attacks, like route leaks and hijacks)
- About 4.4% of all Autonomous Systems on the Internet were affected
- 2,737 Autonomous Systems were a victim of at least one routing incident
- 1,294 networks were responsible for 4739 routing incidents

Twelve months of routing incidents (2018)



Source: https://www.bgpstream.com/

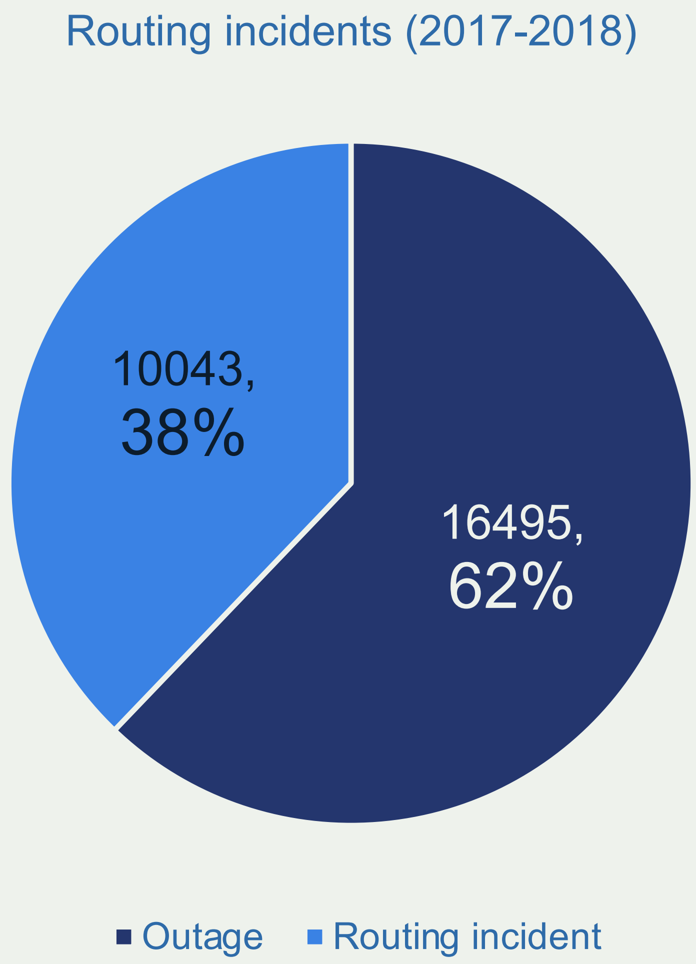
There is a problem (comp. 2017)

- 12,600 (↓9.6%) total incidents (either outages or attacks, like route leaks and hijacks)

- About 4.4% (↓1%) of all Autonomous Systems on the Internet were affected

- 2,737 (↓12%) Autonomous Systems were a victim of at least one routing incident

- 1,294 (↓17%) networks were responsible for 4739 routing incidents

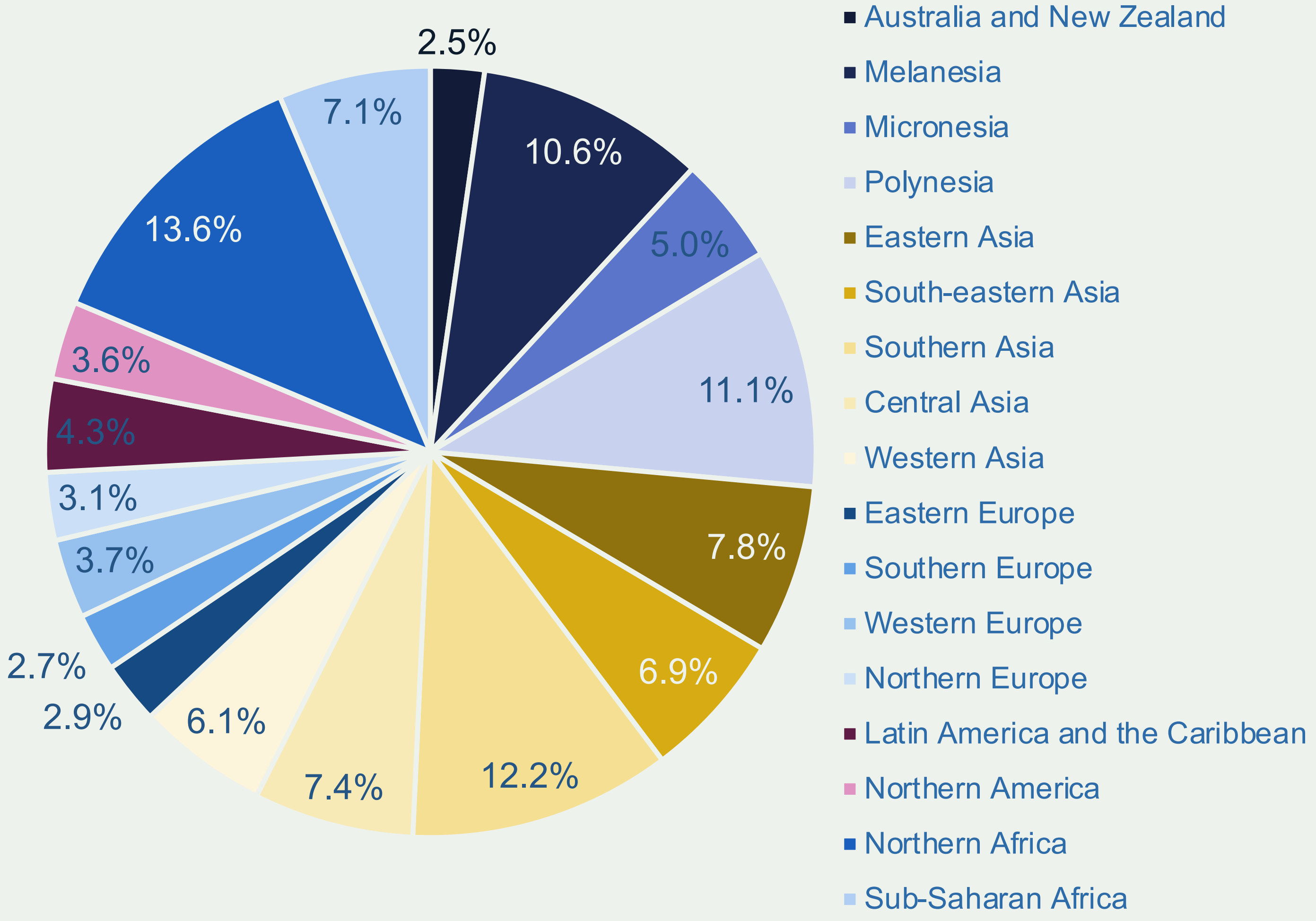


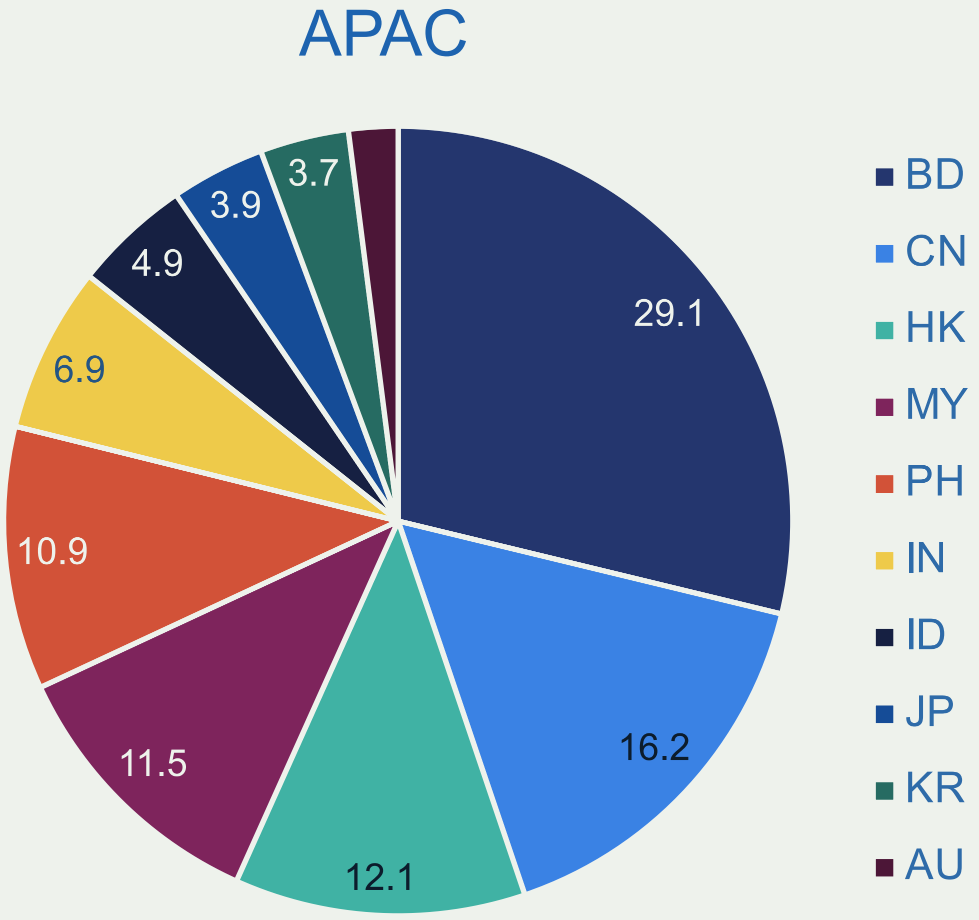
Source: https://www.bgpstream.com/

Routing Incidents Cause Real World Problems

Event	Explanation	Repercussions	Example
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, and can cause Denial of Service (DoS) attacks or traffic interception.	*The 2008 YouTube hijack* *April 2018 Amazon Route 53 hijack*
Route Leak	A network operator with multiple upstream providers (often due to accidental misconfiguration) announces to one upstream provider that is has a route to a destination through the other upstream provider.	Can be used for a MITM, including traffic inspection, modification and reconnaissance.	*November 2018. Google faced a major outage in many parts of the world thanks to a BGP leak. This incident that was caused by a Nigerian ISP MainOne due to a configuration mistake.*
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	*March 1, 2018. Memcached 1.3Tb/s reflection-amplification attack reported by Akamai*

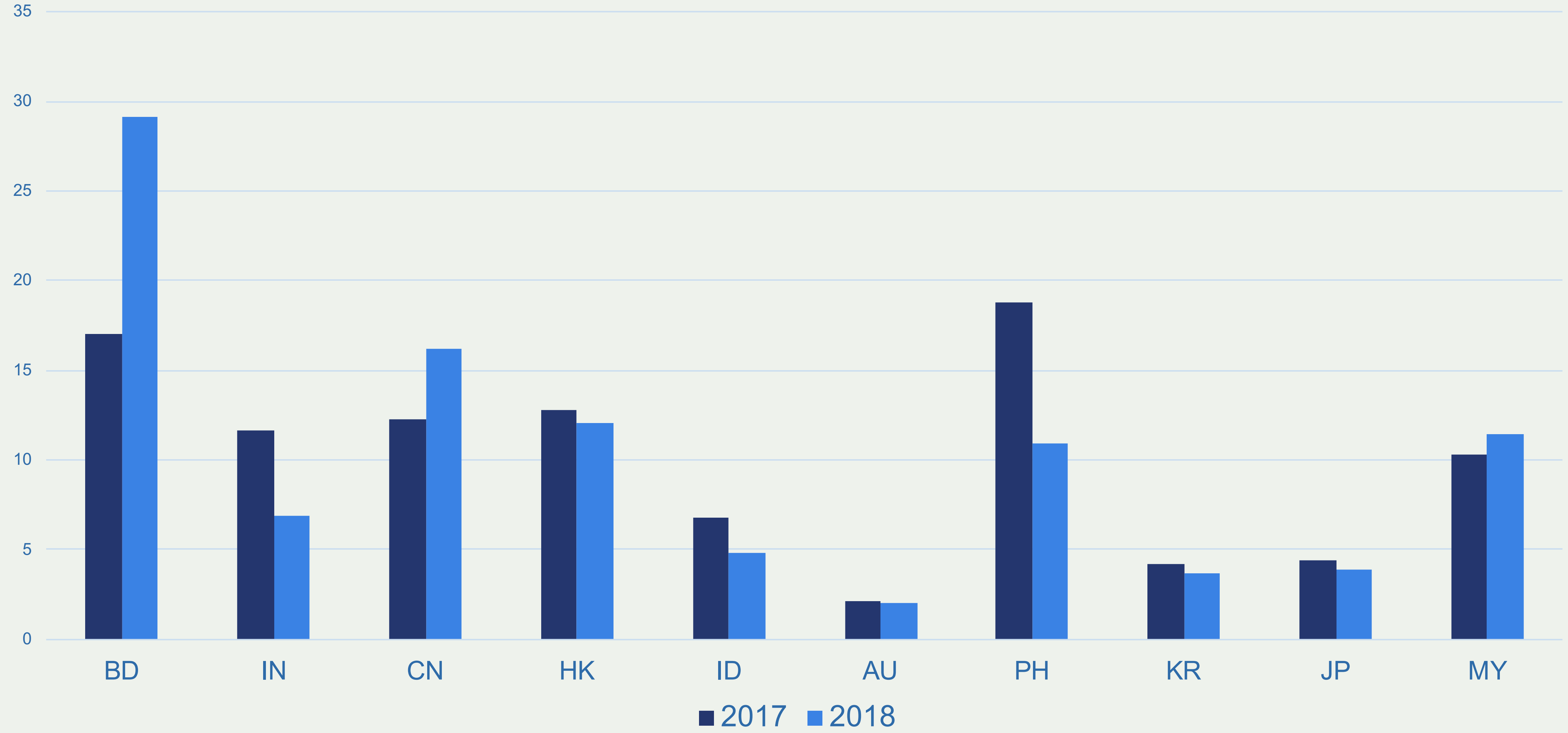
Potential victims (percent of networks affected by an incident)



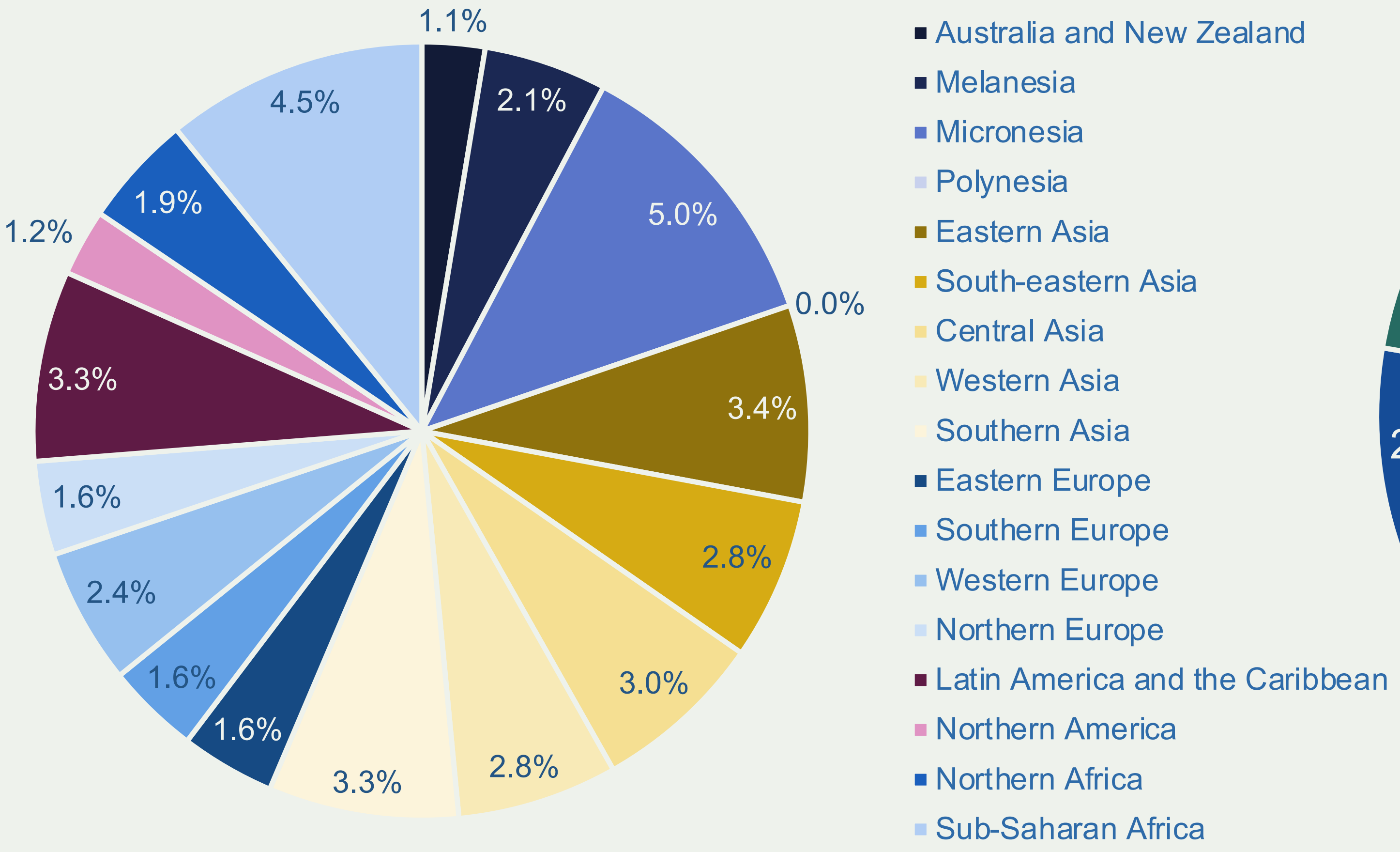


Source: https://www.bgpstream.com/

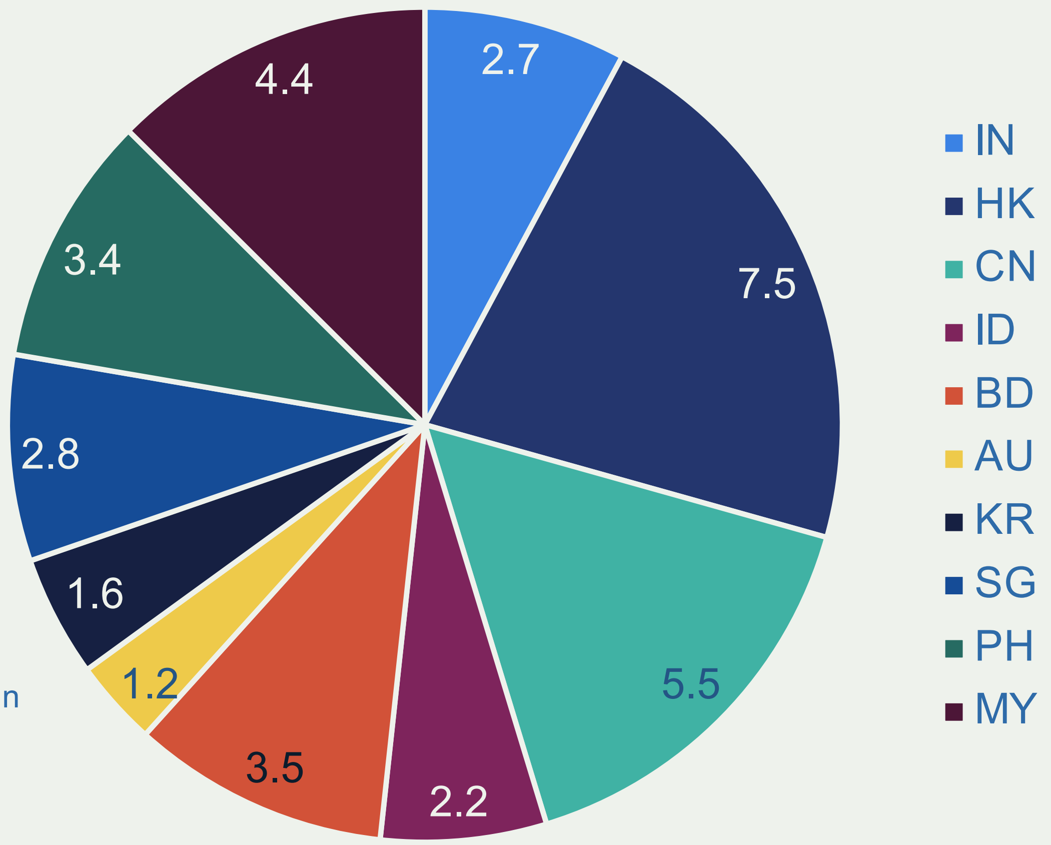
Potential victims: 2017 ➡ 2018



Potential culprits (percent of networks responsible for an incident)

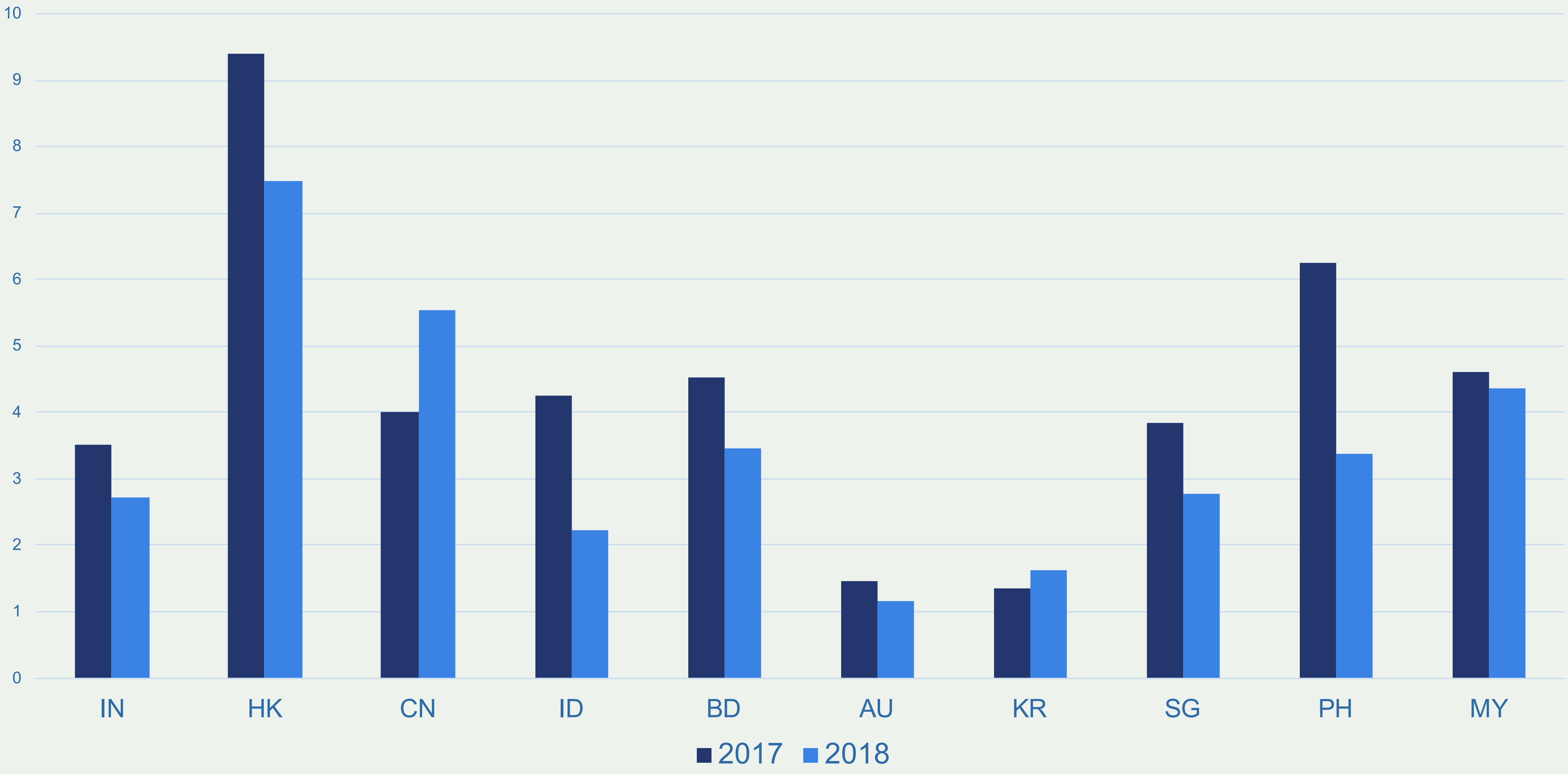


APAC



Source: https://www.bgpstream.com/

Positive dynamics



Tools to Help

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

But…

- Not enough deployment
- Lack of reliable data

We need a systemic approach to improving routing security

We Are In This Together

Network operators have a responsibility to ensure a globally robust and secure routing infrastructure.

Your network's safety depends on a routing infrastructure that weeds out bad actors and accidental misconfigurations that wreak havoc on the Internet.

The more network operators work together, the fewer incidents there will be, and the less damage they can do.

Mutually Agreed Norms for Routing Security (MANRS)

Provides crucial fixes to reduce the most common routing threats

Mutually Agreed Norms for Routing Security

MANRS provides baseline recommendations in the form of Actions

- Distilled from common behaviors – BCPs, optimized for low cost and low risk of deployment
- With high potential of becoming norms

MANRS builds a visible community of security minded operators

- Social acceptance and peer pressure

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

MANRS is an Important Step

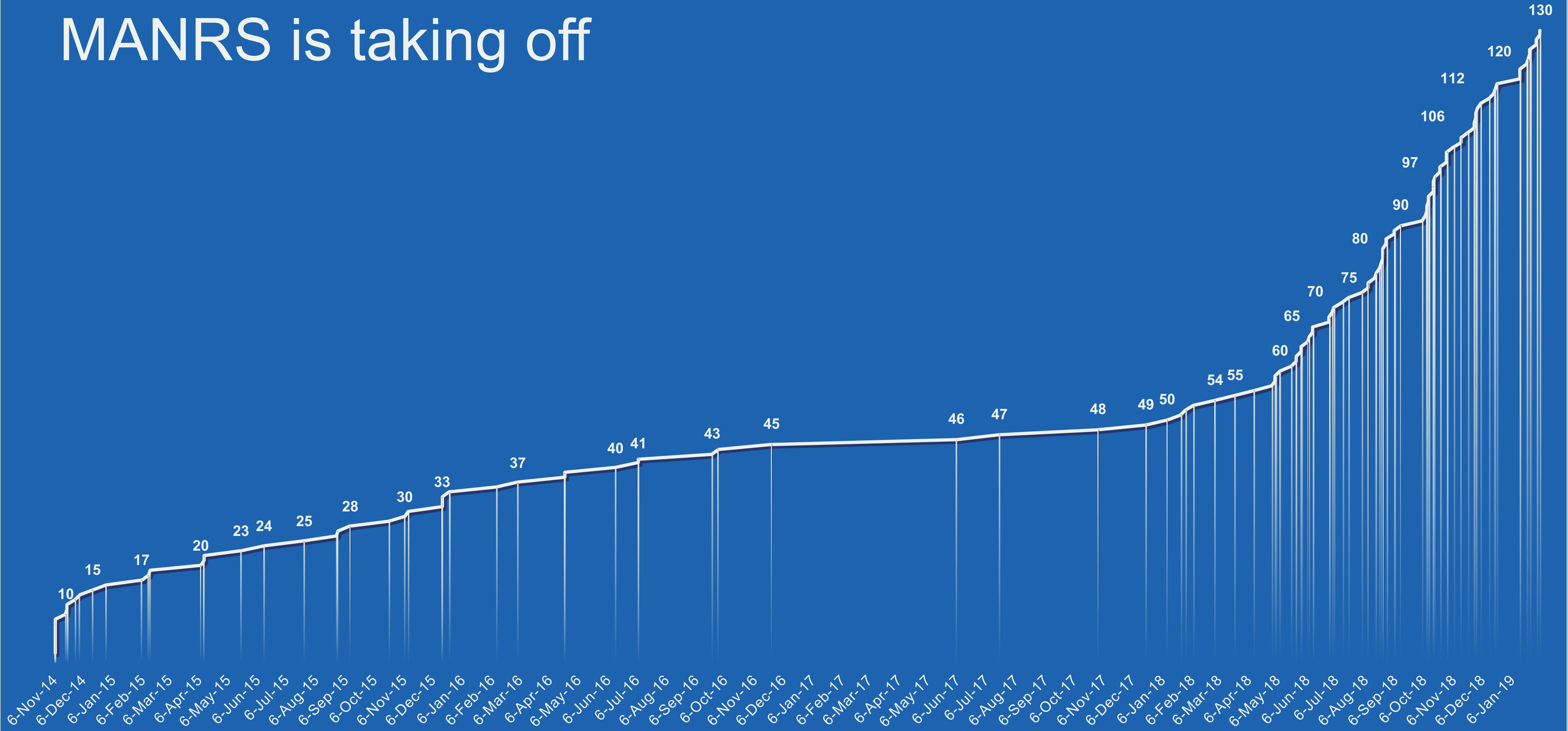
Security is a process, not a state. MANRS provides a structure and a consistent approach to solving security issues facing the Internet.

MANRS is the minimum an operator should consider, with low risk and cost-effective actions.

MANRS is not a one-stop solution to all of the Internet's routing woes, but it is an important step toward a globally robust and secure routing infrastructure.

MANRS – increasing adoption

MANRS is taking off



MANRS IXP Programme

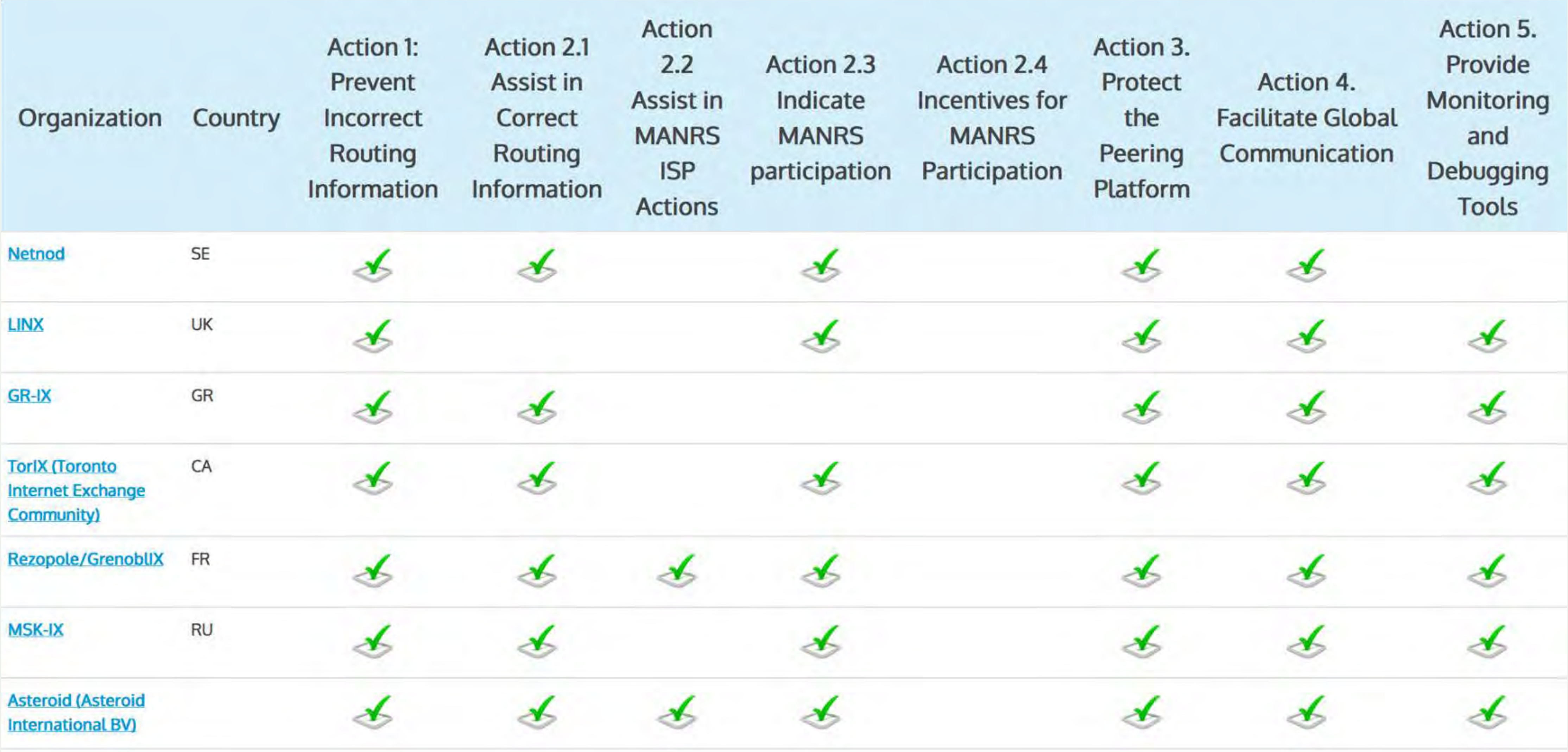
There is synergy between MANRS and IXPs

- IXPs form a community with a common operational objective
- MANRS is a reference point with a global presence – useful for building a “safe neighborhood”

How can IXPs contribute?

- Implement a set of Actions that demonstrate the IXP commitment and also bring significant improvement to the resilience and security of the routing system

MANRS IXP Program – launched in April 2018



Organization	Country	Action 1: Prevent Incorrect Routing Information	Action 2.1 Assist in Correct Routing Information	Action 2.2 Assist in MANRS ISP Actions	Action 2.3 Indicate MANRS participation	Action 2.4 Incentives for MANRS Participation	Action 3. Protect the Peering Platform	Action 4. Facilitate Global Communication	Action 5. Provide Monitoring and Debugging Tools
Netnod	SE	✓	✓		✓		✓	✓	
LINX	UK	✓			✓		✓	✓	✓
GR-IX	GR	✓	✓				✓	✓	✓
TorIX (Toronto Internet Exchange Community)	CA	✓	✓		✓		✓	✓	✓
Rezopole/GrenoblIX	FR	✓	✓	✓	✓		✓	✓	✓
MSK-IX	RU	✓	✓		✓		✓	✓	✓
Asteroid (Asteroid International BV)		✓	✓	✓	✓		✓	✓	✓

MANRS IXP Actions

Action 1

Prevent propagation of incorrect routing information

This mandatory action requires IXPs to implement filtering of route announcements at the Route Server based on routing information data (IRR and/or RPKI).

Action 2

Promote MANRS to the IXP membership

IXPs joining MANRS are expected to provide encouragement or assistance for their members to implement MANRS actions.

Action 3

Protect the peering platform

This action requires that the IXP has a published policy of traffic not allowed on the peering fabric and performs filtering of such traffic.

Action 4

Facilitate global operational communication and coordination

The IXP facilitates communication among members by providing necessary mailing lists and member directories.

Action 5

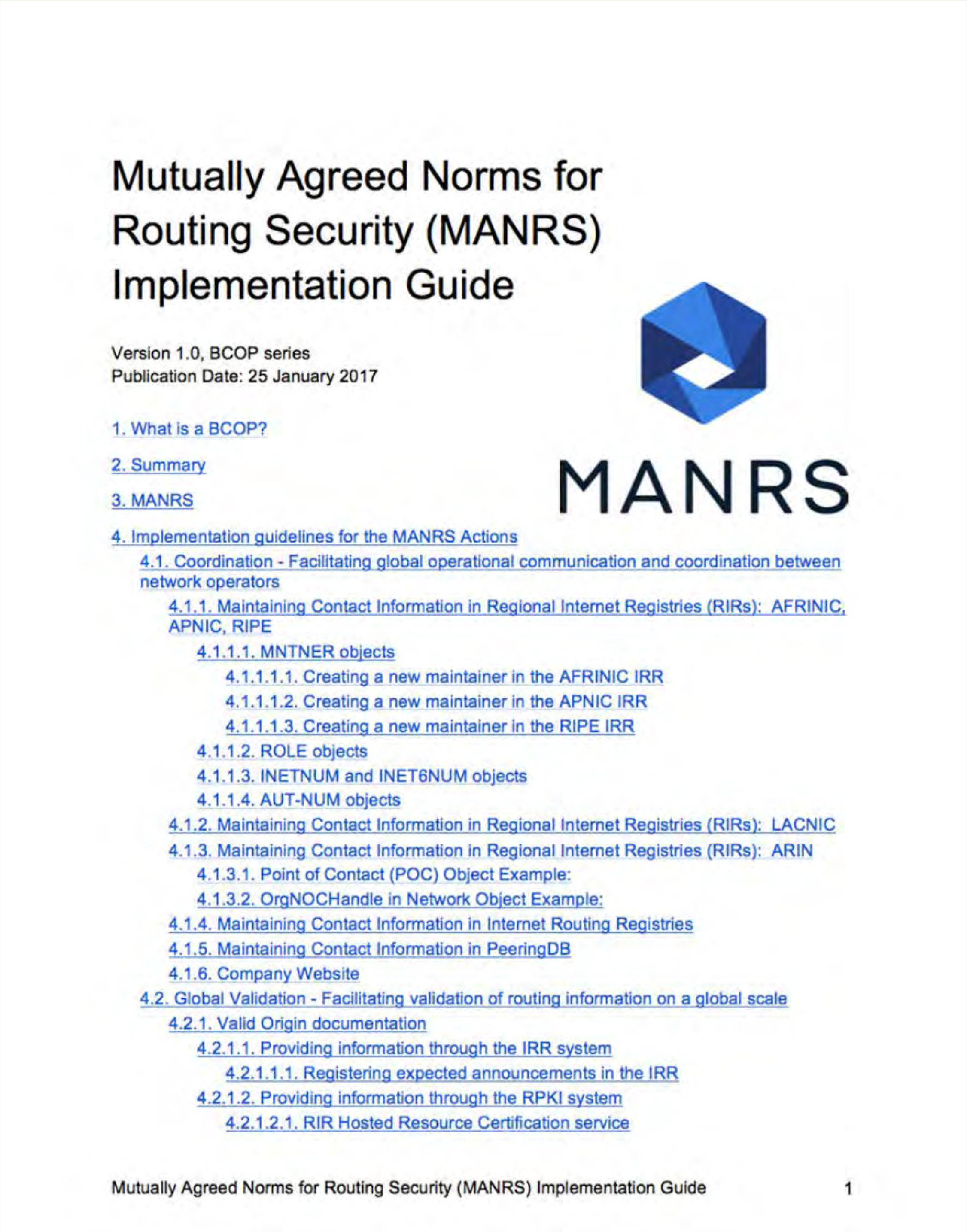
Provide monitoring and debugging tools to the members.

The IXP provides a looking glass for its members.

MANRS Implementation Guide

A resource to help Operators implement MANRS Actions.

- Based on Best Current Operational Practices deployed by network operators around the world
- https://www.manrs.org/bcop/
- Has received recognition from the RIPE community by being published as RIPE-706

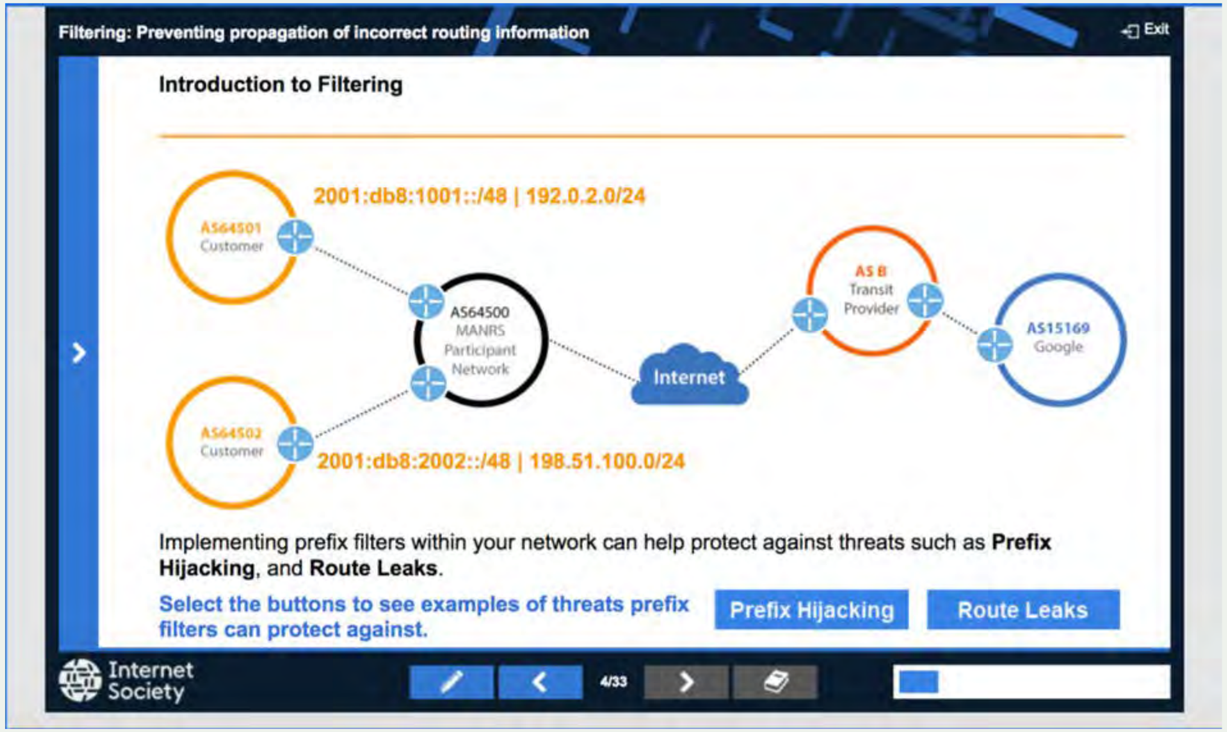


Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide

Version 1.0, BCOP series
Publication Date: 25 January 2017

MANRS Training Tutorials

6 training tutorials based on information in the Implementation Guide. A test at the end of each tutorial.
https://www.manrs.org/tutorials



Filtering: Preventing propagation of incorrect routing information

Introduction to Filtering

Implementing prefix filters within your network can help protect against threats such as **Prefix Hijacking**, and **Route Leaks**.

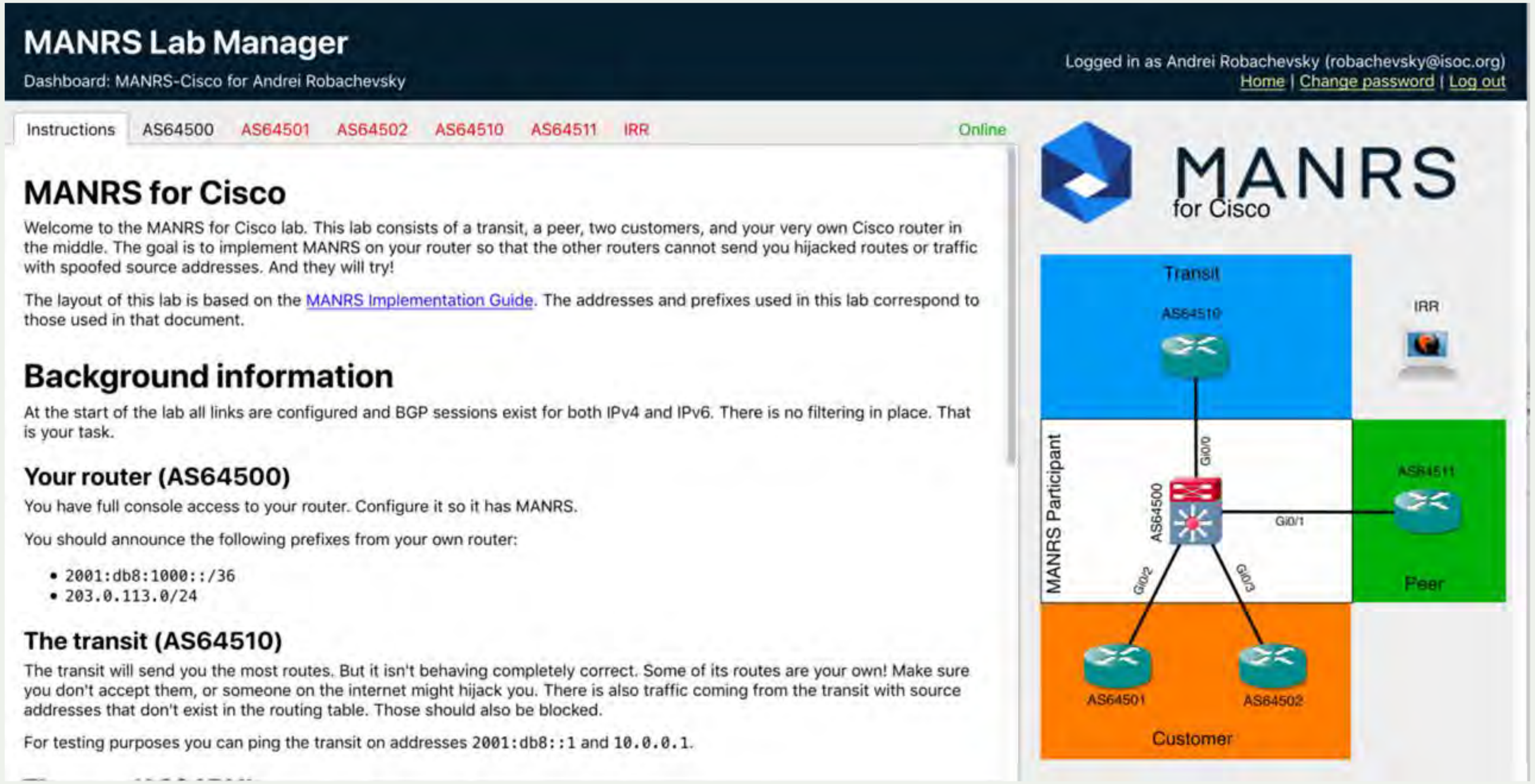
Select the buttons to see examples of threats prefix filters can protect against.

MANRS Hands-on Lab

The prototype lab is ready, finalizing the production version.

- Cisco
- Juniper
- Mikrotik

Can be used as a standalone lab or as an end-exam



MANRS Lab Manager

Dashboard: MANRS-Cisco for Andrei Robachevsky

Logged in as Andrei Robachevsky (robachevsky@isoc.org)
Home | Change password | Log out

MANRS for Cisco

Welcome to the MANRS for Cisco lab. This lab consists of a transit, a peer, two customers, and your very own Cisco router in the middle. The goal is to implement MANRS on your router so that the other routers cannot send you hijacked routes or traffic with spoofed source addresses. And they will try!

The layout of this lab is based on the MANRS Implementation Guide. The addresses and prefixes used in this lab correspond to those used in that document.

Background information

At the start of the lab all links are configured and BGP sessions exist for both IPv4 and IPv6. There is no filtering in place. That is your task.

Your router (AS64500)

You have full console access to your router. Configure it so it has MANRS.

You should announce the following prefixes from your own router:

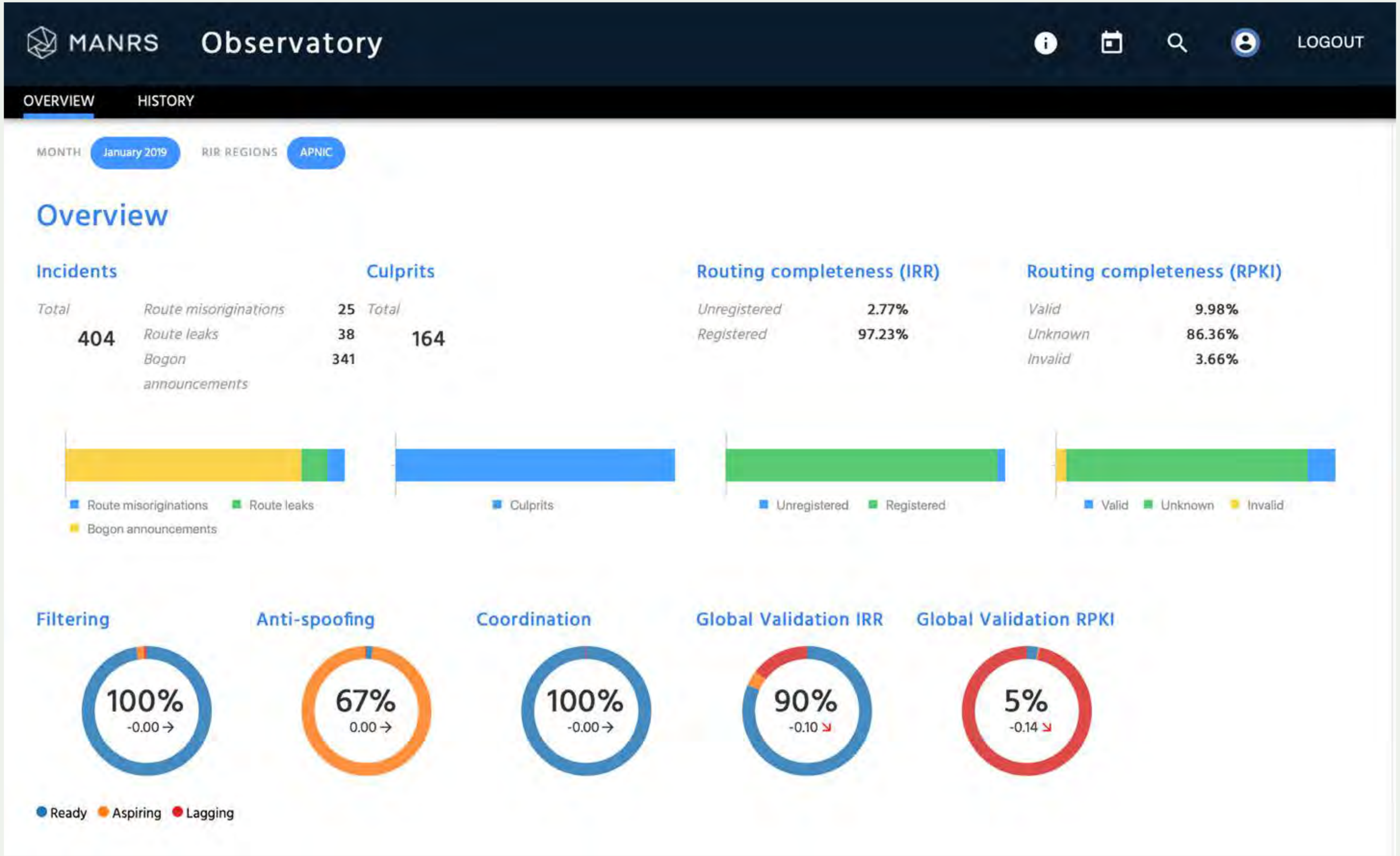
- `2001:db8:1000::/36`
- `203.0.113.0/24`

The transit (AS64510)

The transit will send you the most routes. But it isn't behaving completely correct. Some of its routes are your own! Make sure you don't accept them, or someone on the internet might hijack you. There is also traffic coming from the transit with source addresses that don't exist in the routing table. Those should also be blocked.

For testing purposes you can ping the transit on addresses `2001:db8::1` and `10.0.0.1`.

State of routing security: APNIC region, Jan 2019



MONTH January 2019 RIR REGIONS APNIC

Overview

Incidents

Total		
404	Route misoriginations	25
	Route leaks	38
	Bogon announcements	341

Culprits

Total

164

Routing completeness (IRR)

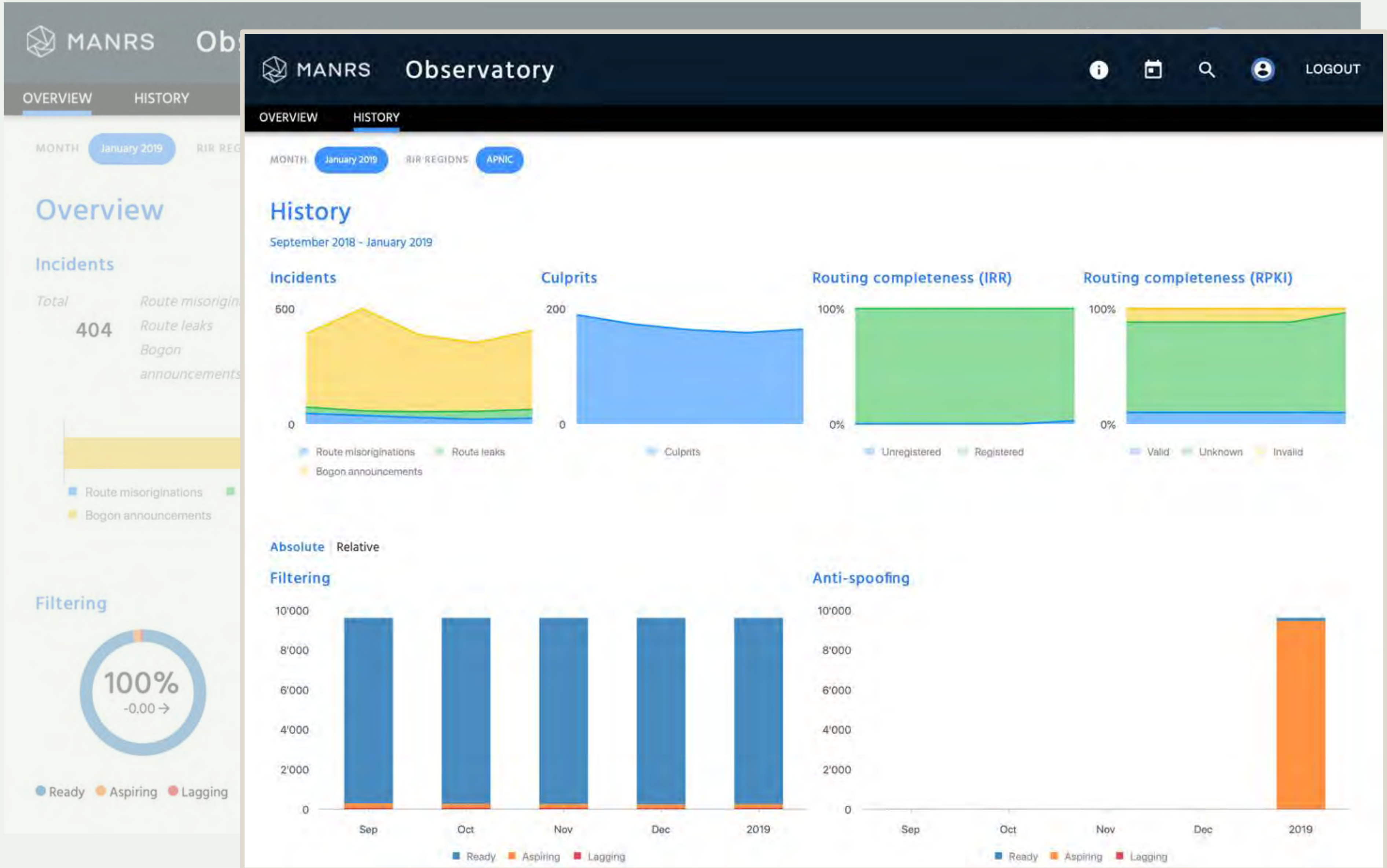
Unregistered	2.77%
Registered	97.23%

Routing completeness (RPKI)

Valid	9.98%
Unknown	86.36%
Invalid	3.66%

Filtering	Anti-spoofing	Coordination	Global Validation IRR	Global Validation RPKI
100% -0.00 →	67% 0.00 →	100% -0.00 →	90% -0.10 ↘	5% -0.14 ↘

Evolution: APNIC region, September 2018 - Jan 2019



MONTH January 2019

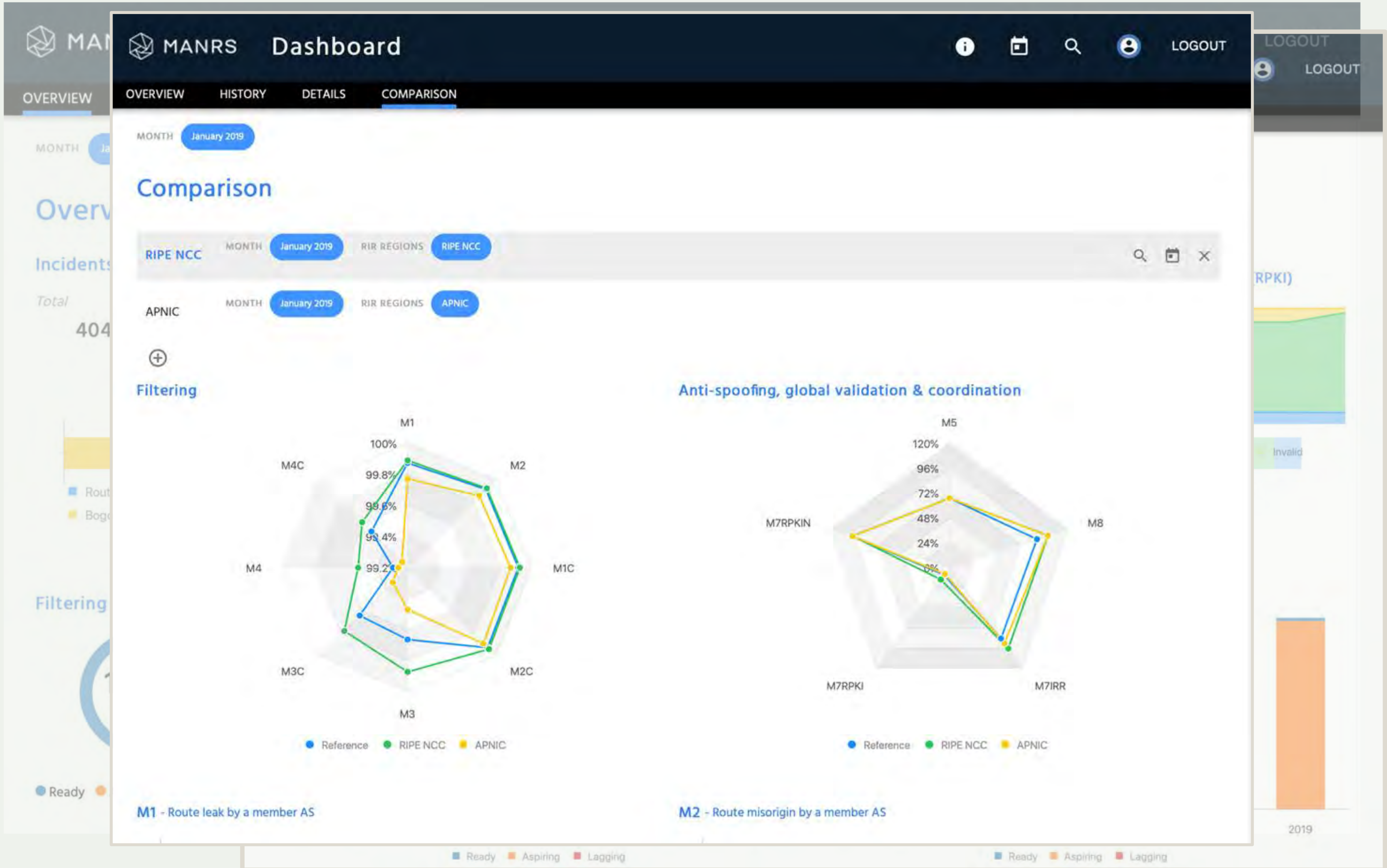
RIR REGIONS APNIC

History

September 2018 - January 2019

Absolute | Relative

Comparison on regional level



MONTH January 2019

Comparison

RIPE NCC MONTH January 2019 RIR REGIONS RIPE NCC

APNIC MONTH January 2019 RIR REGIONS APNIC

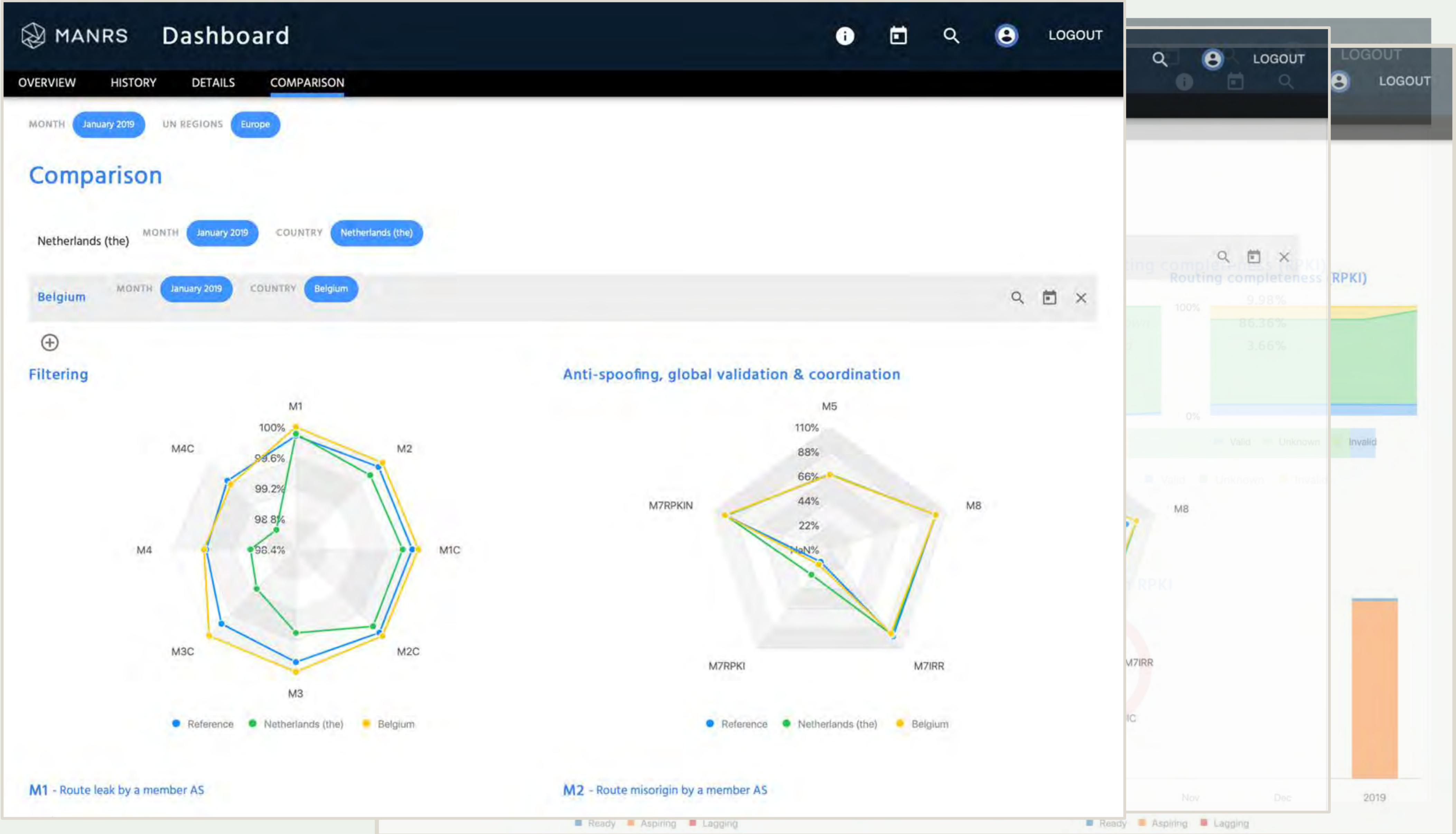
Filtering

Anti-spoofing, global validation & coordination

M1 - Route leak by a member AS

M2 - Route misorigin by a member AS

Comparison on country level



MANRS Dashboard

LOGOUT

OVERVIEW HISTORY DETAILS COMPARISON

MONTH January 2019 UN REGIONS Europe

Comparison

Netherlands (the) MONTH January 2019 COUNTRY Netherlands (the)

Belgium MONTH January 2019 COUNTRY Belgium

Filtering

Anti-spoofing, global validation & coordination

M1 - Route leak by a member AS

M2 - Route misorigin by a member AS

Why join MANRS?

- Improve your security posture and reduce the number and impact of routing incidents
- Demonstrate that these practices are reality
- Join a community of security-minded operators working together to make the Internet better
- Use MANRS as a competitive differentiator

Why should CSIRTs get involved?

- You have a role in risk analysis, threat mitigation, and education/training
  - Ensure network operators, network admins, and technical management are aware of routing security issues
  - MANRS is looking to partner with training providers to include routing security in curriculum

- To demonstrate security proficiency and commitment to your constituency
  - Promote MANRS compliance to security-focused customers

- To help solve global network problems
  - Lead by example, encourage good operational practices, and help weed out bad actors
  - Being part of the MANRS community can strengthen enterprise security credentials

- Potential collaboration regarding MANRS Observatory
  - Information sharing

manrs.org

#ProtectTheCore

https://www.youtube.com/c/RoutingMANRS

MANRS Video:
https://www.youtube.com/embed/nJINk5p-HEE