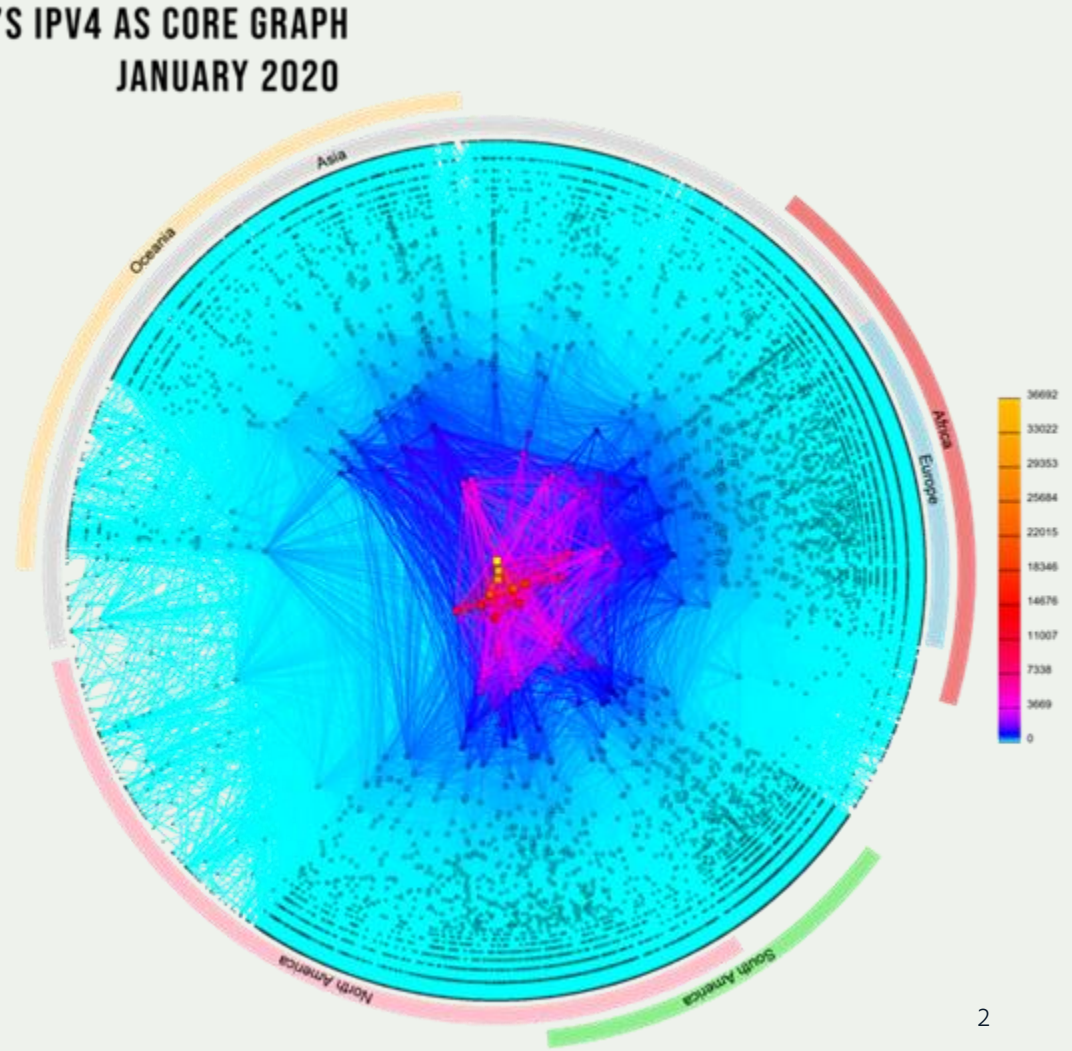
MANRS:
10 years of improving routing security

Pablo López-Aguilar <plopezaguilar@globalcyberalliance.org>

GLOBAL CYBER ALLIANCE

Today’s Internet routing system

- About **77,500*** Autonomous Systems (AS) that together make up the Internet.
- Each AS builds its own roadmap of the Internet using a language called **Border Gateway Protocol, or BGP.**
- There are more than **1.1M*** advertised IP prefixes (routes).
- BGP is a fundamental underpinning of the Internet.



*as of March 2025

What is the challenge of routing security?

Photo by charlesdeluvio on Unsplash

- BGP was created in 1989, before Internet security was a concern.
- BGP assumes all networks are trustworthy. Any network can announce it has a path to any other network, even if it does not.
- There is no built-in security mechanism to check if this info is legitimate or not.
- On today's Internet, this is a problem.
- BGP is vulnerable to both malicious attacks and human mistakes.

Routing security matters

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* *February 2022 KLAYswap 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.* *June 2019. Allegheny leaked routes from another provider to Verizon, causing significant outage.*
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*

Why is Routing Security Hard?

Every network has a responsibility to implement basic routing security practices to mitigate threats. Otherwise - they are part of the problem.

But implementing best practices does not bring many immediate benefits. It costs time and money, and you probably can’t charge extra for it.

A secure routing system benefits all. But even if you do everything right, your security is still in the hands of other networks.

This is a collective action problem.

Solving the collective action problem

Regulation doesn’t really help

- Global span and dependencies
- Fragmented solutions

Making good practices a norm

- Widely accepted
- Not exactly a least common denominator, but not too high either
- Visible and Measurable

A collaborative approach:

Mutually Agreed Norms for Routing Security (MANRS)

Provides crucial fixes to reduce the most important routing threats

Two pillars

An undisputed minimum security baseline – the norm.

- Defined through MANRS Actions

Demonstrated commitment by the participants

- Measured by the Observatory and published on https://www.manrs.org

MANRS Programs

- Network Operators (2014)
- Internet Exchange Points (2018)
- Content Delivery Networks (CDNs) and Cloud Providers (2020)
- Network Equipment Vendors (2021)

MANRS Actions for Network Operators

Action 1

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

Action 2

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

Action 3

Coordination

Facilitate global operational communication and coordination between network operators

Maintain globally accessible, up-to-date contact information in common routing databases

Action 4

Routing Information

Facilitate validation of routing announcements on a global scale

Publish your data so others can validate

Blue shading = Mandatory Action

MANRS Actions for IXPs

Action 1

Filtering

Implement filtering of route announcements at the Route Server based on routing information data (IRR and/or RPKI).

Action 2

Promotion

Provide encouragement or assistance for IXP members to implement MANRS actions.

Action 3

Protect the peering platform

Have a published policy of traffic not allowed on the peering fabric and perform filtering of such traffic.

Action 4

Coordination

Facilitate communication among members by providing necessary mailing lists and member directories.

Action 5

Tools

Provide monitoring and debugging tools to IXP members.

Blue shading = Mandatory Action

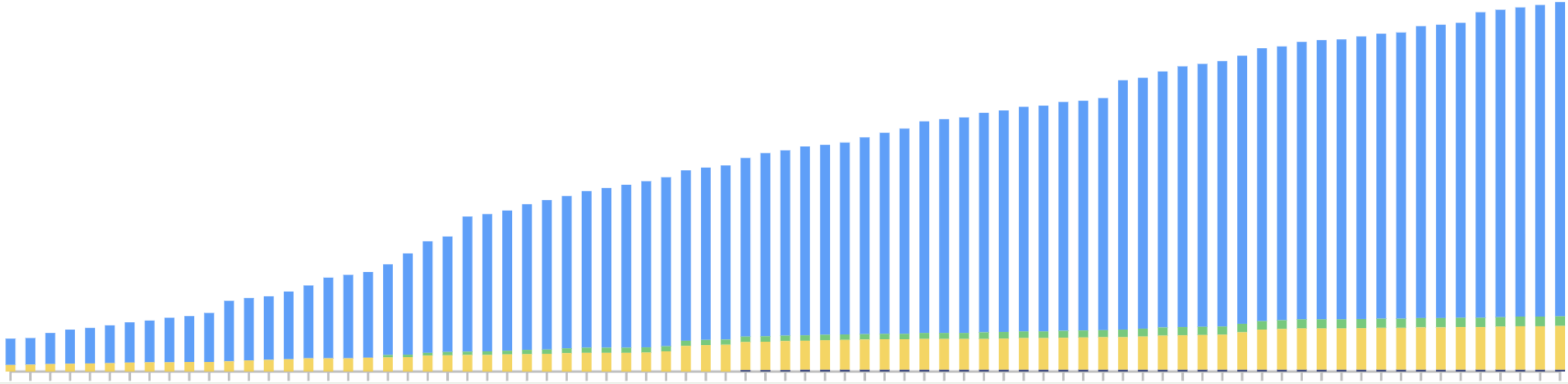
The MANRS Community

1042 Network Operators

146 IXPs

32 CDN & Clouds providers

6 Vendors*



*As of February 2025

A global effort

Why to join MANRS?

Implementing MANRS Actions

Signals an organization's security-forward posture and can eliminate SLA violations that reduce profitability or cost customer relationships.

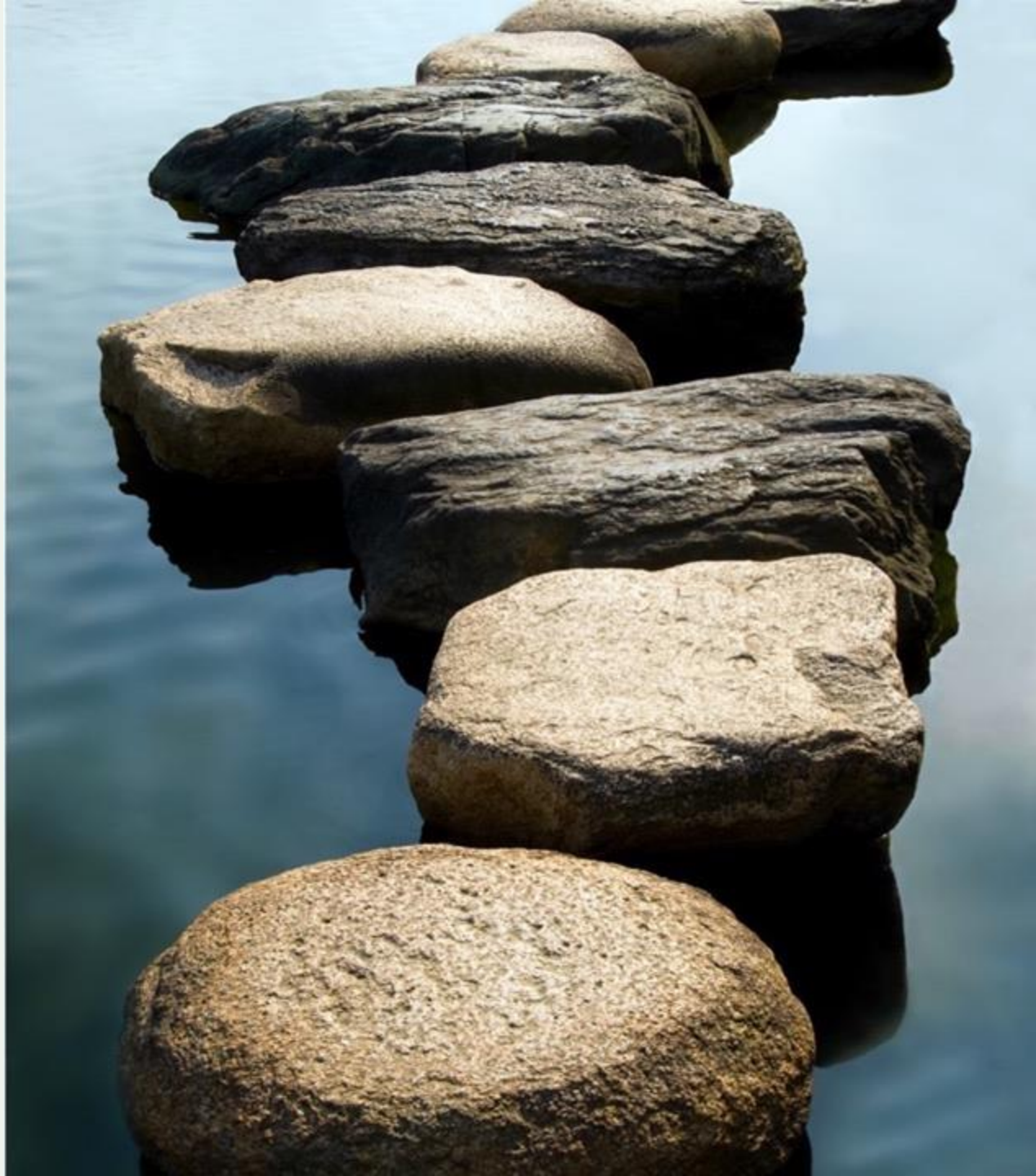
Reduces routing incidents, helping networks readily identify and address problems with customers or peers.

Improves network's operations by establishing better and cleaner peering communication pathways, while also providing granular insight for troubleshooting.

Addresses many concerns of security-focused enterprises and other customers.

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 a network should consider, with low risk and cost-effective actions.
- MANRS is not a one-stop solution to all the Internet's routing goes, but it is an important step toward a globally robust and secure routing infrastructure.



Measuring MANRS

MANRS Observatory
https://observatory.manrs.org

MANRS Observatory

Provides a factual state of security and resilience of the Internet routing system and individual networks, and tracks it over time

Measurements are:

- **Transparent** – using publicly accessible data
- **Passive** – no cooperation from networks required
- **Evolving** – MANRS community decides what gets measured and how

MONTH (PARTIAL) March 2025

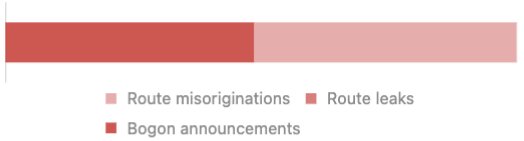
Overview

State of Routing Security

Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

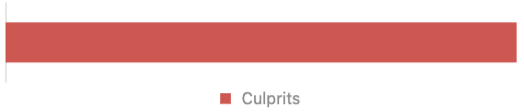
Incidents

Route misoriginations	168
Route leaks	0
Bogon announcements	159
Total	327



Culprits

Culprits	262

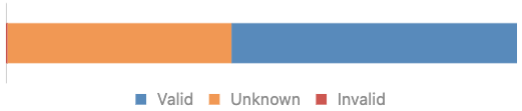


Routing Information (IRR)

Unregistered	113,932	9.1%
Registered	1,138,708	90.9%

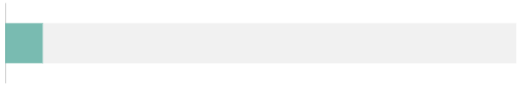
Routing Information (RPKI)

Valid	700,384	55.9%
Unknown	548,734	43.8%
Invalid	3,522	0.3%

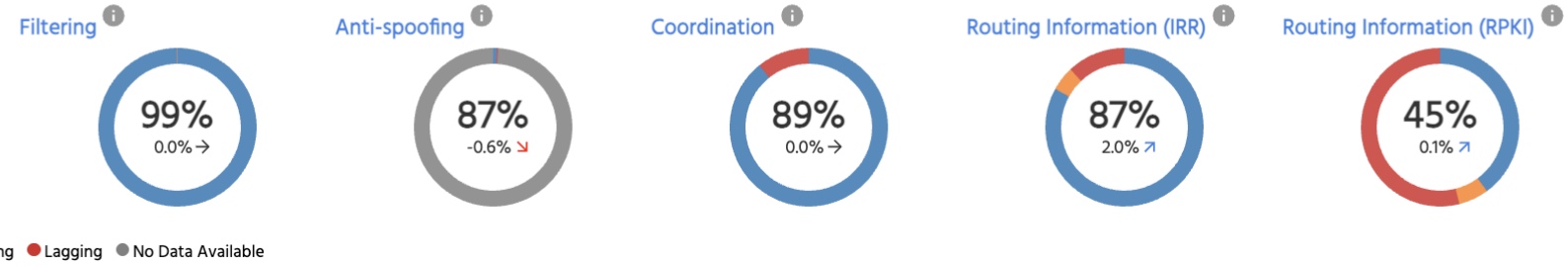


Route Origin Validation

ROV-based Filtering Rate (%)	7.4%



MANRS Readiness



MONTH (PARTIAL) March 2025 COUNTRY Myanmar

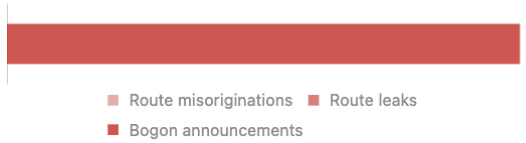
Overview

State of Routing Security

Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

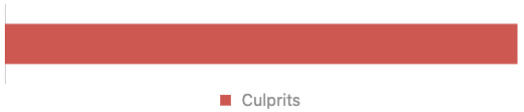
Incidents

Route misoriginations	0
Route leaks	0
Bogon announcements	3
Total	3



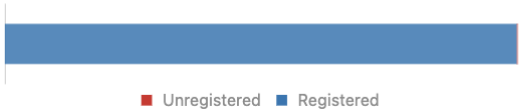
Culprits

Culprits	3



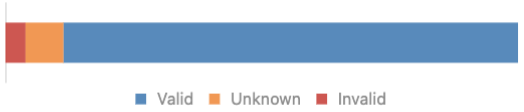
Routing Information (IRR)

Unregistered	3	0.2%
Registered	1,295	99.8%



Routing Information (RPKI)

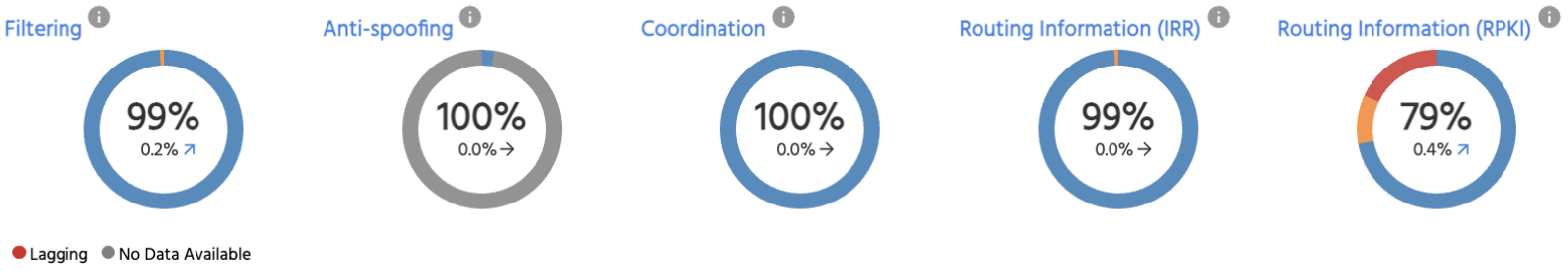
Valid	1,152	88.7%
Unknown	96	7.4%
Invalid	50	3.9%



Route Origin Validation

ROV-based Filtering Rate (%)	48.0%

MANRS Readiness



A more detailed overview

MONTH (PARTIAL) March 2025 COUNTRY Myanmar

Details

Download data Copy to clipboard

Severity: All | Ready | Aspiring | Lagging | No Data Available

Scope: All | Filtering | Anti-spoofing | Coordination | Routing Information (IRR) | Routing Information (RPKI)

Result Limit: 100 | All

Total 122 Previous 1 2 Next

Overview

ASN	Holder	Country	UN Regions	UN Sub-Regions	RIR Regions	Filtering	Anti-spoofing	Coordination	Routing Information (IRR)	Routing Information (RPKI)
		MM	Asia	South-eastern Asia	APNIC	100%	100%	100%	100%	97%
		MM	Asia	South-eastern Asia	APNIC	100%	-	100%	100%	100%
		MM	Asia	South-eastern Asia	APNIC	100%	-	100%	100%	100%
		MM	Asia	South-eastern Asia	APNIC	100%	-	100%	100%	99%
		MM	Asia	South-eastern Asia	APNIC	100%	-	100%	71%	71%
		MM	Asia	South-eastern Asia	APNIC	100%	-	100%	100%	100%
		MM	Asia	South-eastern Asia	APNIC	100%	-	100%	100%	100%
		MM	Asia	South-eastern Asia	APNIC	100%	-	100%	100%	100%
		MM	Asia	South-eastern Asia	APNIC	100%	-	100%	100%	100%
		MM	Asia	South-eastern Asia	APNIC	100%	-	100%	100%	100%
		MM	Asia	South-eastern Asia	APNIC	100%	-	100%	100%	100%
		MM	Asia	South-eastern Asia	APNIC	100%	-	100%	100%	90%
		MM	Asia	South-eastern Asia	APNIC	100%	-	100%	100%	100%
		MM	Asia	South-eastern Asia	APNIC	100%	-	100%	100%	100%
		MM	Asia	South-eastern Asia	APNIC	100%	-	100%	100%	100%
		MM	Asia	South-eastern Asia	APNIC	100%	-	100%	100%	100%

MANRS is turning 10 years old this year

10 years of community action

Key achievements:

- Uptake: with more than 1,200 participants from across the globe
- Diversity: from one original program to four
- Dissemination: with training resources and activities that play at global scale
- Impact: an industry-driven reference for operators and policy-makers
- Objectivity: compliance can be effectively tracked through the MANRS Observatory

The Internet Society launched the MANRS project in 2014. After nine years of providing the MANRS secretariat, they partnered with the Global Cyber Alliance to take on that role as of January 2024.

Who is the Global Cyber Alliance (GCA)?

INTERNET INTEGRITY

AIDE, Domain Trust, MANRS, OSS.

Solutions at the systemic or infrastructure level, with the potential to scale worldwide.

CAPACITY & RESILIENCE

Cybersecurity Toolkit, ACT, DMARC.

Empowering communities by improving their cyber capacity and enhancing their resilience to cyber risk.

COLLABORATIVE CYBERSECURITY

NonProfit Cyber, Cyber Civil Defense, Common Good Cyber.

GCA as a central player —and a guide— in the universe of collaborative efforts for a safer Internet

GCA'S MISSION

A THURSTWORTHY INTERNET FOR ALL

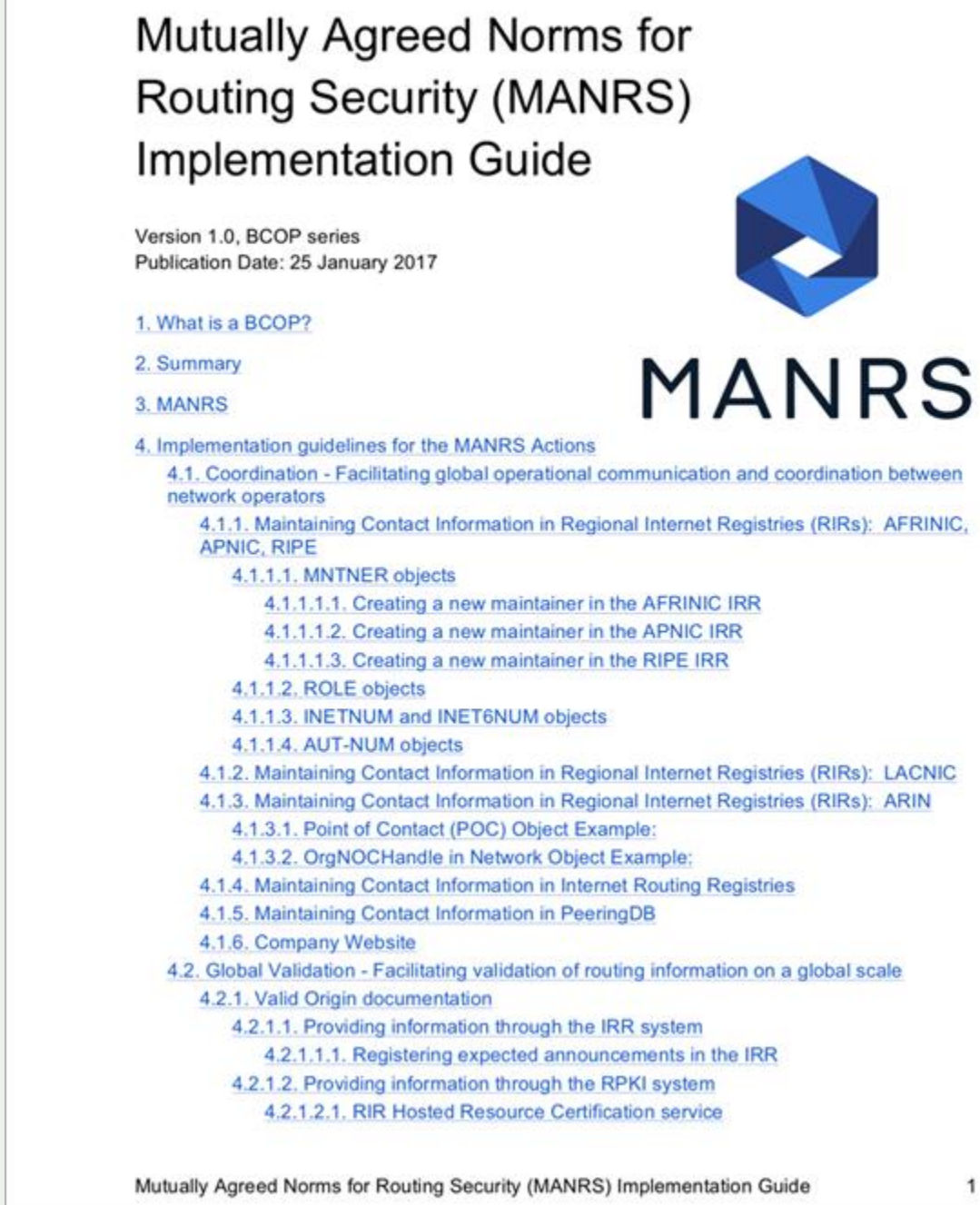
GLOBAL CYBER ALLIANCE

Learn More and Join Us

MANRS Implementation Guide for Network Operators

If you're not ready to join yet, implementation guidance is available to help you.

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



Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide

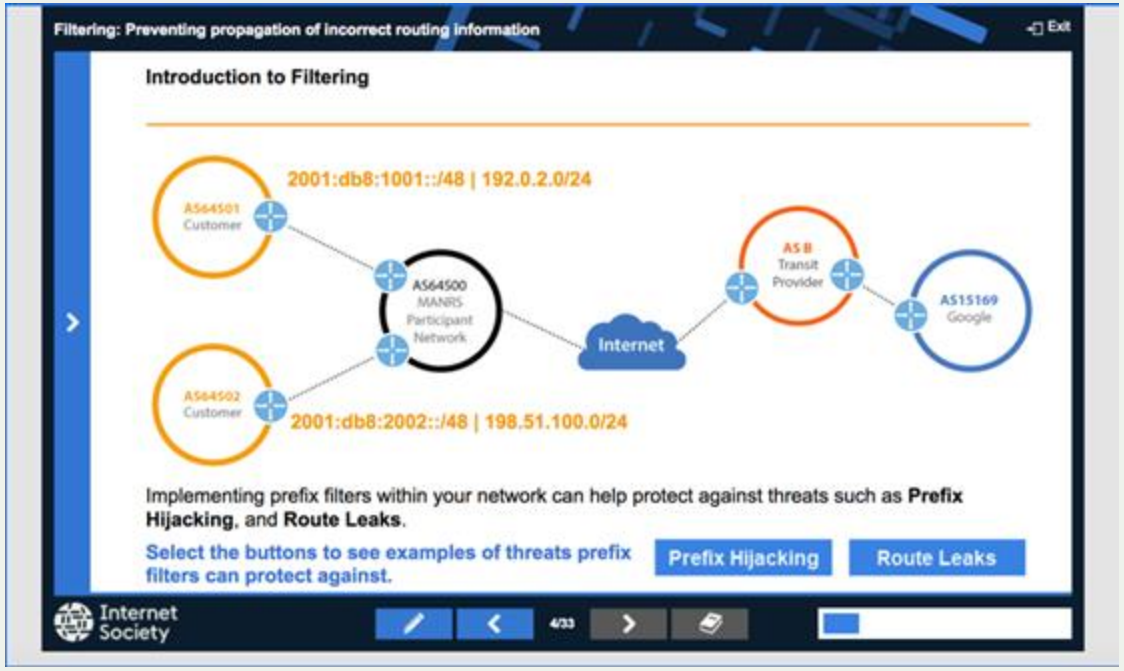
Version 1.0, BCOP series
Publication Date: 25 January 2017

MANRS

MANRS Tutorials

- Tutorials based on information in the Implementation Guide
- Walks through the tutorial with a test at the end of each module
- Working with and looking for partners that are interested in integrating it in their curricula

https://www.manrs.org/tutorials



Why join MANRS?

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

Join Us

Visit https://www.manrs.org/join/

- Fill out the form with as much detail as possible.
- We will guide you through the process, ask questions and run tests

Contact us:

- contact@manrs.org
- https://manrs.org/about/contact/
- We will be happy to help you!

LEARN MORE:

https://www.manrs.org

https://globalcyberalliance.org/

FOLLOW US:

/RoutingMANRS