

MANRS: 10 years of improving routing security

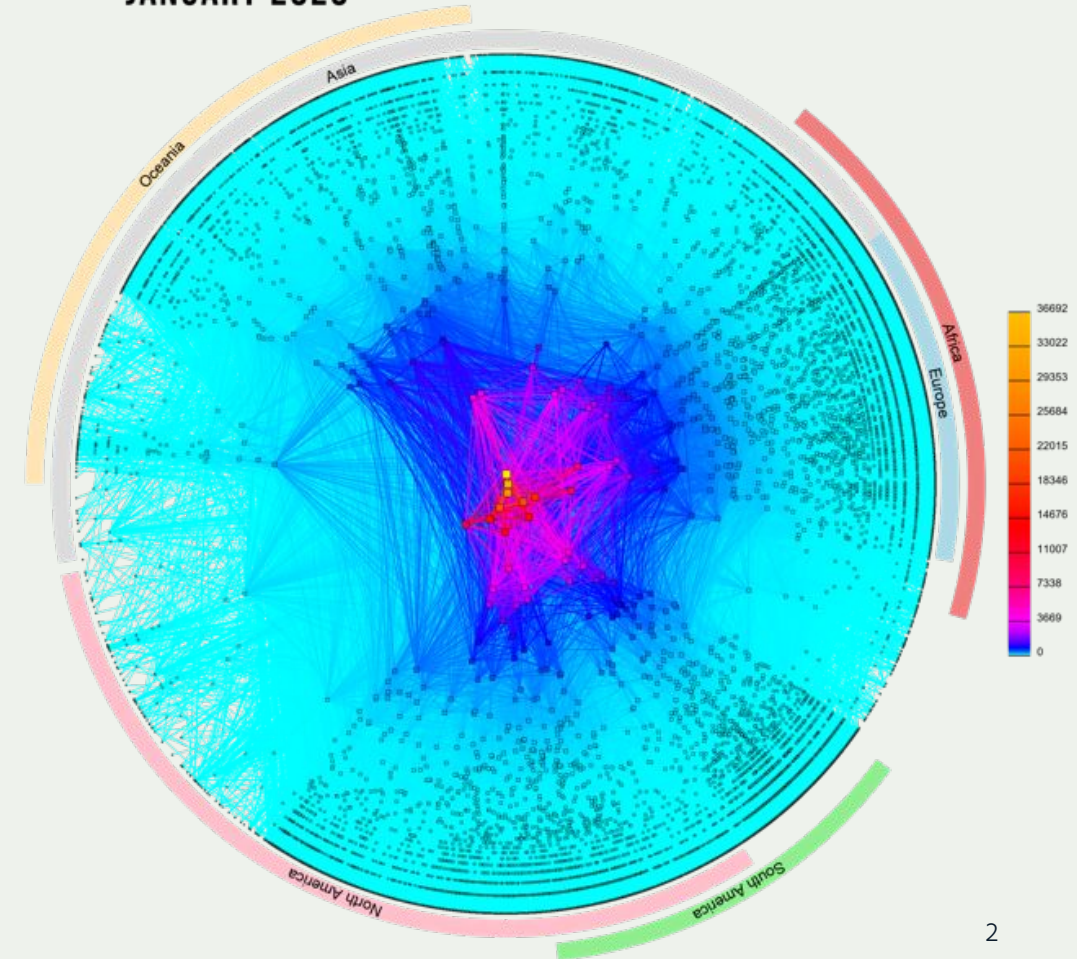
Arturo Servin <arturo.servin@google.com>
MANRS Steering Committee



Today's Internet routing system

- About **76,000*** 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 **970,000*** advertised IP prefixes (routes).
- BGP is a fundamental underpinning of the Internet.

CAIDA'S IPV4 AS CORE GRAPH
JANUARY 2020



*as of July 2024

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.	<i>The 2008 YouTube hijack April 2018 Amazon Route 53 hijack February 2022 KLAYswap hijack</i>
Route Leak	A network operator with multiple upstream providers (often due to accidental misconfiguration) announces to one upstream provider that it has a route to a destination through the other upstream provider.	Can be used for a MITM, including traffic inspection, modification and reconnaissance.	<i>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.</i>
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	<i>March 1, 2018. Memcached 1.3Tb/s reflection-amplification attack reported by Akamai</i>

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 Network Operators Program

Launched in 2014 by a group of network operators with the following goals:

- Raise awareness of routing security problems and encourage the implementation of actions that can address them.
- Promote a culture of collective responsibility toward the security and resilience of the Internet's global routing system.
- Demonstrate the ability of the Internet industry to address routing security problems.
- Provide a framework for network operators to better understand and address issues relating to the security and resilience of the Internet's global routing system.



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



MANRS IXP Program

Internet Exchange Points (IXPs) are a collaborative focal point to discuss and promote the importance of routing security.

Launched in 2018, the IXP Program addresses the unique needs and concerns of IXPs with a separate set of MANRS actions.

IXPs can implement actions that demonstrate their commitment to routing security and bring significant improvement to the resilience and security of their peering relationships.



MANRS Actions for Internet Exchange Points

Action 1

Prevent propagation of incorrect routing information

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

Action 2

Promote MANRS to the IXP membership

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

Facilitate global operational communication and coordination

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

Action 5

Provide monitoring and debugging tools to the members.

Provide a looking glass for IXP members.



MANRS CDN and Cloud Program

Launched in 2020, the CDN and Cloud Provider Programme helps by requiring egress routing controls so networks can prevent incidents from happening. Leveraging CDNs' and cloud providers' peering power can have significant positive spillover effect on the routing hygiene of networks they peer with.

Goals include:

- Create a secure network peering environment
- Encourage better routing hygiene from peering partners
- Demonstrate responsible behavior
- Improve operational efficiency for peering interconnections, minimizing incidents and providing more granular insight for troubleshooting



MANRS Actions for CDNs & Cloud Providers

Action 1

Prevent propagation of incorrect routing information

Ensure correctness of own announcements and of their peers (non-transit) by implementing explicit (whitelist) filtering with prefix granularity.



Action 2

Prevent traffic with illegitimate source IP addresses

Implement anti-spoofing controls to prevent packets with illegitimate source IP address from leaving the network (egress filters).

Action 3

Facilitate global operational communication and coordination

Maintain globally accessible, up-to-date contact information in PeeringDB and relevant RIR databases.

Action 4

Facilitate validation of routing information on a global scale

Publicly document ASNs and prefixes that are intended to be advertised to external parties (IRR and/or RPKI)

Action 5

Encourage MANRS adoption

Actively encourage MANRS adoption among the peers.

Action 6

Provide monitoring and debugging tools to the peering partners

Provide a mechanism to inform peering partners if announcements did not meet the requirements of the peering policy.

Equipment Vendor Program

Networks can only implement good routing security if the equipment they use, like routers and switches, has the right features and support.

Launched in 2021, the Equipment Vendor Program goals include:

- Articulate common baseline requirements for routing security features
- Influence network engineers through vendor training programs and technical content
- Facilitate good collaboration between network operators and equipment vendors



MANRS Actions for Equipment Vendors

Action 1

Provide solutions to implement MANRS Actions

Offer relevant features in network equipment to help participants join MANRS

Action 2

Promote MANRS through training and technical content

Provide encouragement or assistance for customers to implement MANRS actions.

Intention:

Participation in ongoing activities

Become part of the MANRS community by engaging in advisory, development, and promotional opportunities



MANRS Actions



Filtering

Ensure the correctness of your own announcements and of announcements from your customers to adjacent networks with prefix and AS-path granularity



Anti-Spoofing

Enable source address validation for at least single-homed stub customer networks, your own end-users, and infrastructure



Coordination

Maintain globally accessible up-to-date contact information



Routing Information

Publish your data, so others can validate routing information on a global scale



Tools

Provide monitoring and debugging tools to help others



Promotion

Actively encourage MANRS adoption among peers, customers, and partners



The MANRS Community

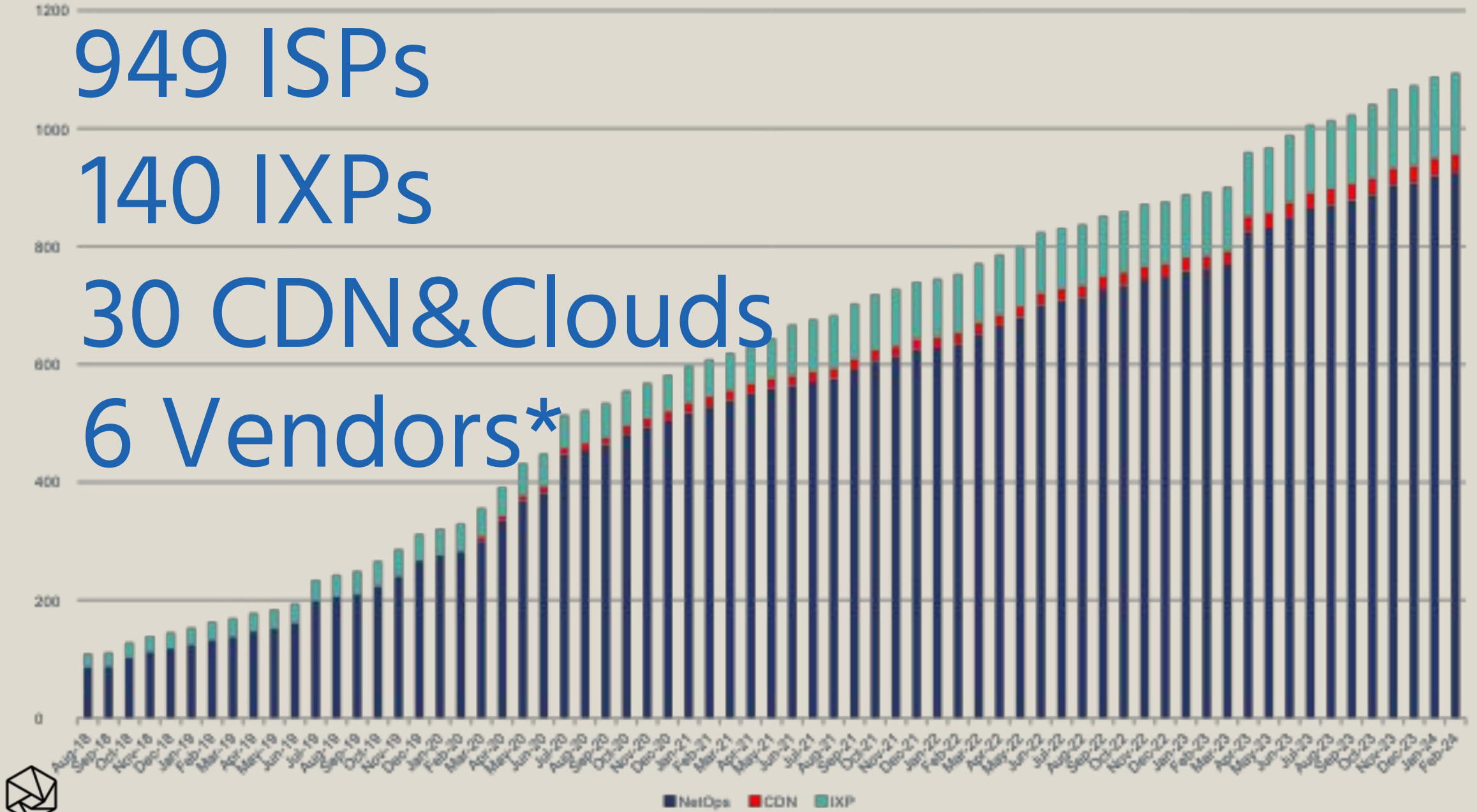


949 ISPs

140 IXPs

30 CDN&Clouds

6 Vendors*



*As of June 2024


A global effort



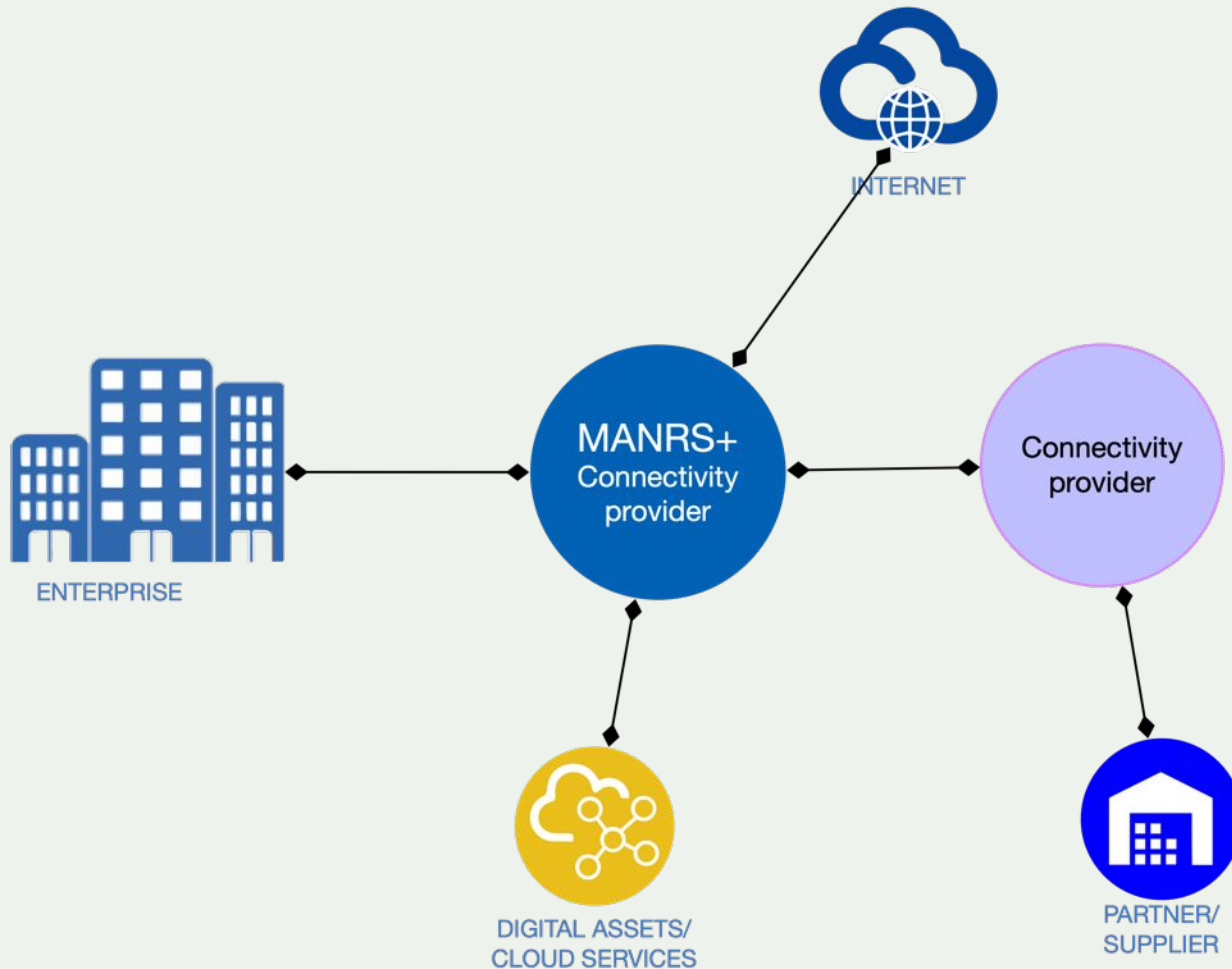
MANRS+: The Business Case for Routing Security



The MANRS (and routing security) business case

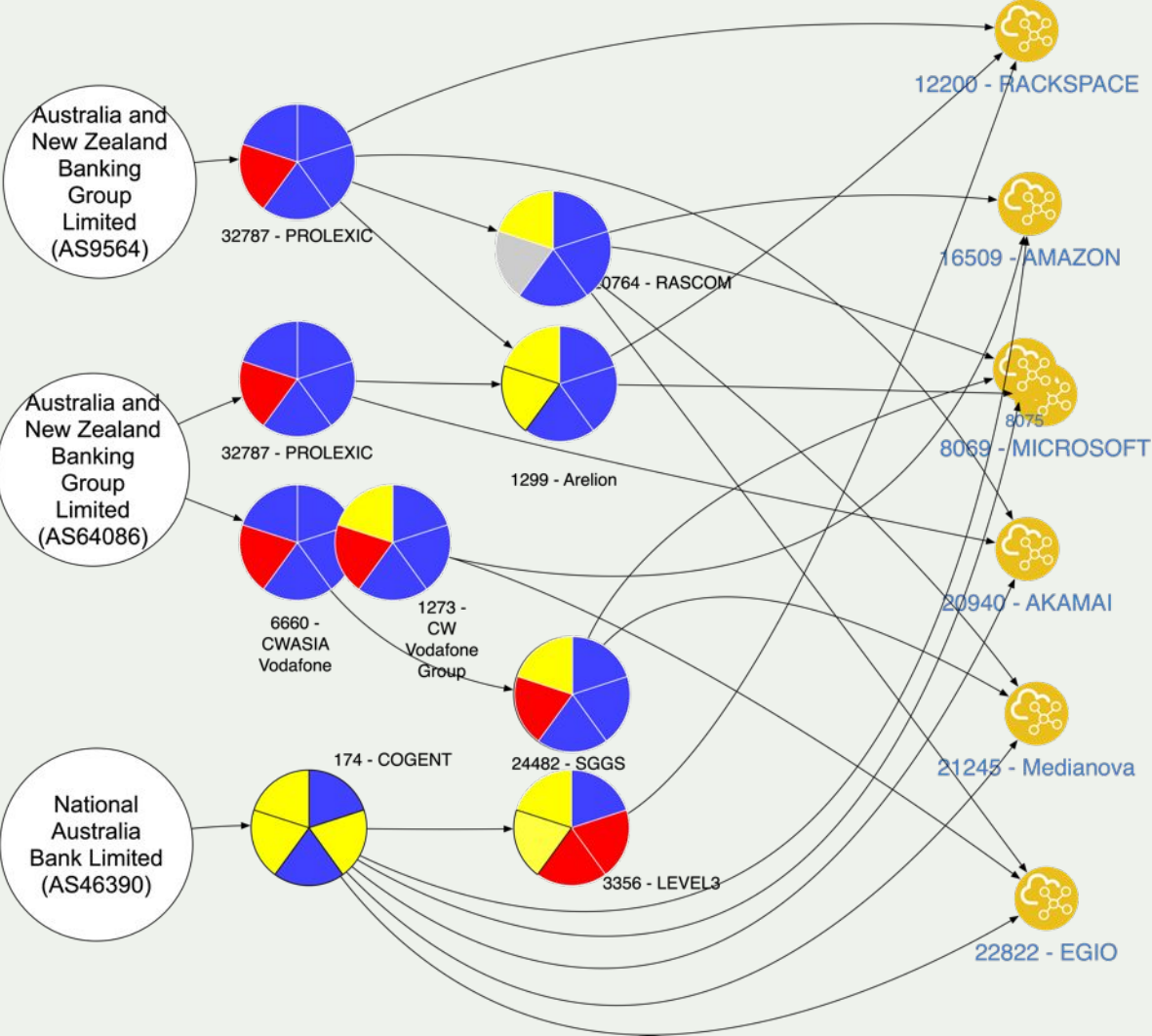
- **Protecting own network** by improving security processes and deploying essential controls
- **Improving security of the global routing system** (overcoming the collective action problem), because
 - routing security is a sum of all contributions
 - this is a way to promote a new baseline
 - a community has gravity to attract others
-  **Gaining competitive advantage** by responding to **customer demands?**

Traffic security for enterprises – a smaller Internet



- Enterprise's connectivity provider is the first line of defense against routing incidents.
- Enterprise can reduce risk by implementing the MANRS actions.
- A strong and reliable tie with the connectivity provider(s) can achieve much more – secure the company supply chain.

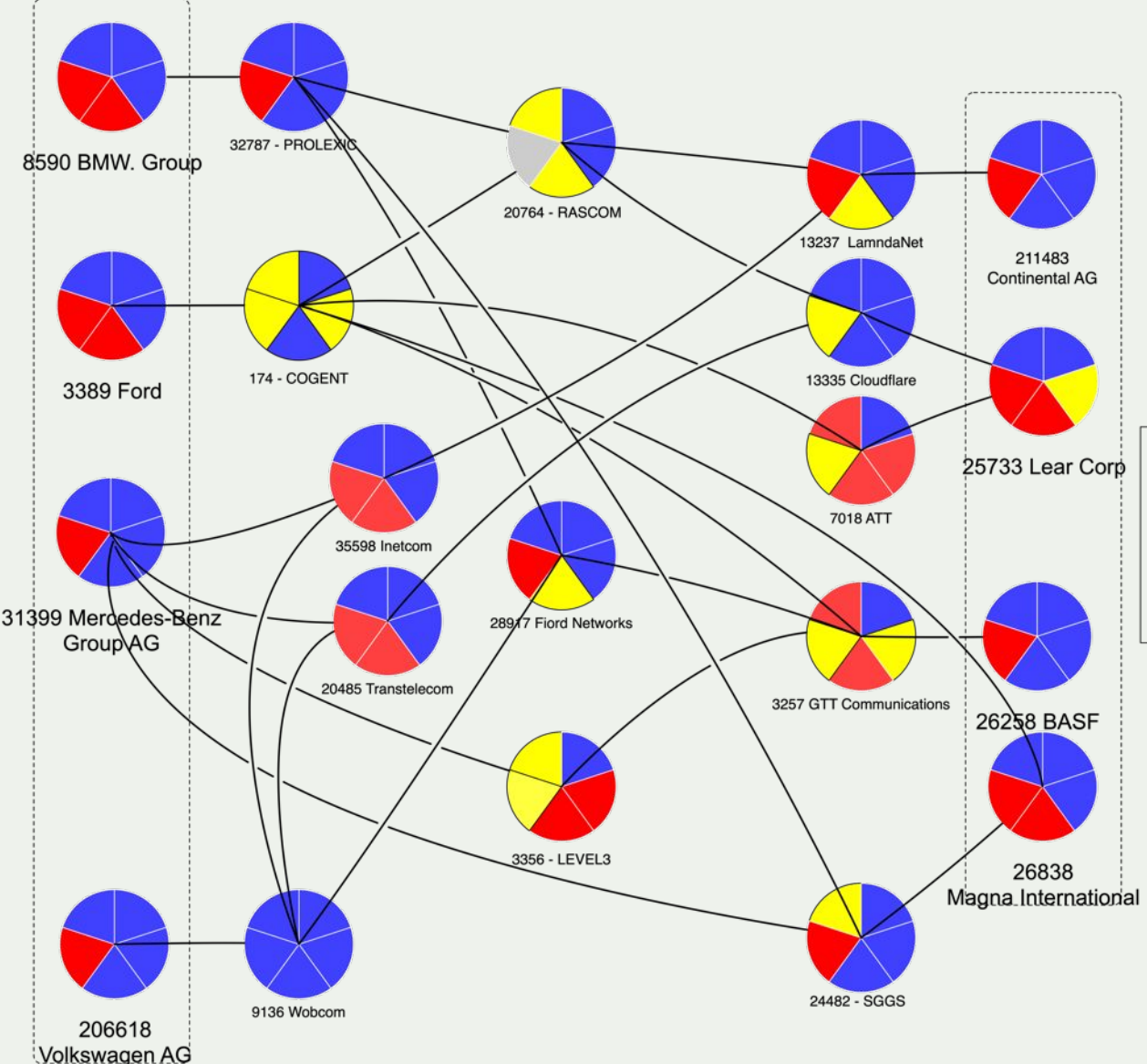
Supply chain: AU banking: 1 intermediary



F - filtering
 C - Coordination
 IRR - Routing information RPKI
 RPKI - Routing Information RPKI
 ROV - ROV

Ready
 Aspiring
 Lagging

Supply chain: Automotive (B2B): 2 intermediaries



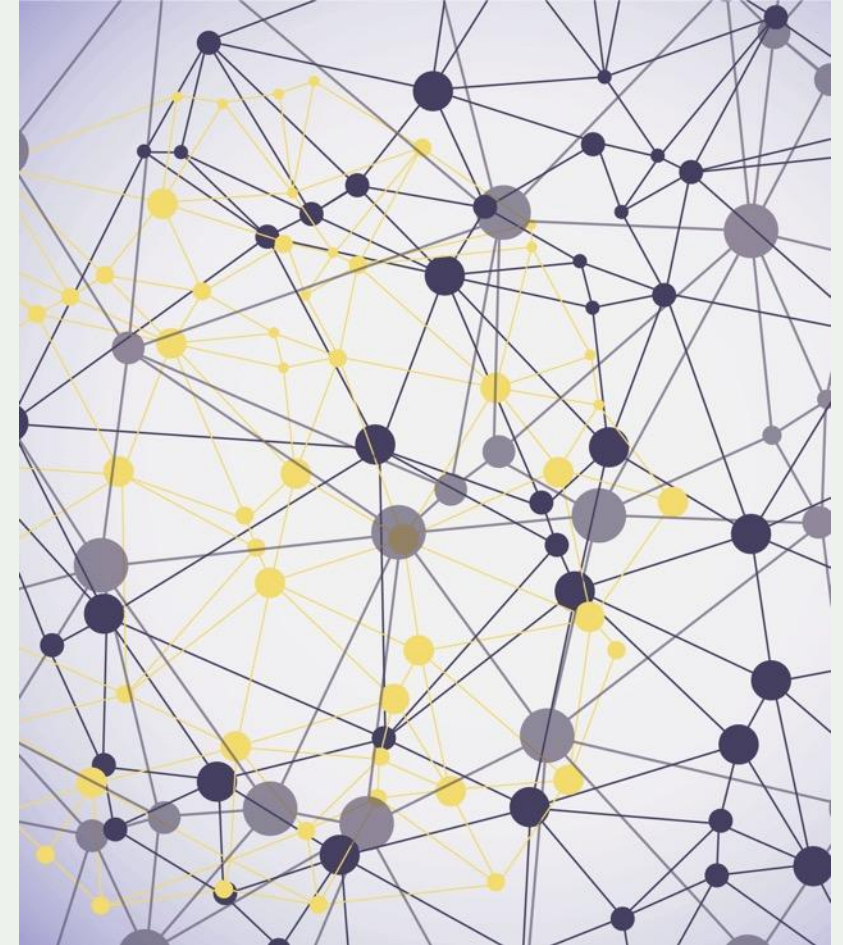
Routing security as part of supply chain security

85% of all ASes are origin-only networks. They fully depend on their connectivity provider for accessing their external digital assets and the Internet.

However, origin-only networks, mostly “enterprises” can contribute to a better routing security by:

1. Enterprises **implementing** routing security best practices in their network infrastructure.
2. Enterprises **demanding** proper routing security controls from their connectivity and cloud providers.

Is your connectivity or cloud provider the first line of defense, or the weakest link?



MANRS+

- A framework for routing security, essential part of supply chain security
- Focus on the demands of enterprise customers in various industry sectors
 - *Extended set of requirements, covering a broader set of risks related to routing and traffic security*
- Conditioned to be included in/referenced from common infosec frameworks
 - *Stronger and more detailed requirements enforcing best practices in traffic security*
 - *High level of assurance of conformance. This includes more profound technical audit and process audit.*
 - *Developed in an transparent and inclusive manner – Standard Development Process*



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 decide what gets measured and how



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 ⁱ

Route misoriginations	262
Route leaks	0
Bogon announcements	123
Total	385



Culprits ⁱ

Culprits	295
----------	-----



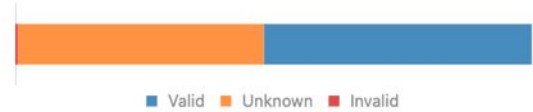
Routing Information (IRR) ⁱ

Unregistered	114,311	9.4%
Registered	1,104,864	90.6%



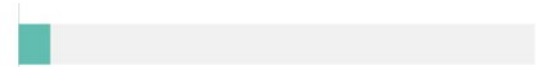
Routing Information (RPKI) ⁱ

Valid	632,645	51.9%
Unknown	580,388	47.6%
Invalid	6,142	0.5%



Route Origin Validation ⁱ

ROV-based Filtering Rate (%)	6.2%
------------------------------	------



MANRS Readiness ⁱ

Filtering ⁱ



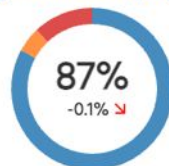
Anti-spoofing ⁱ



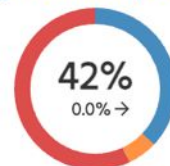
Coordination ⁱ



Routing Information (IRR) ⁱ



Routing Information (RPKI) ⁱ



A more detailed overview

MONTH (PARTIAL)

October 2024

UN REGIONS

Europe

Details

Download data

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

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

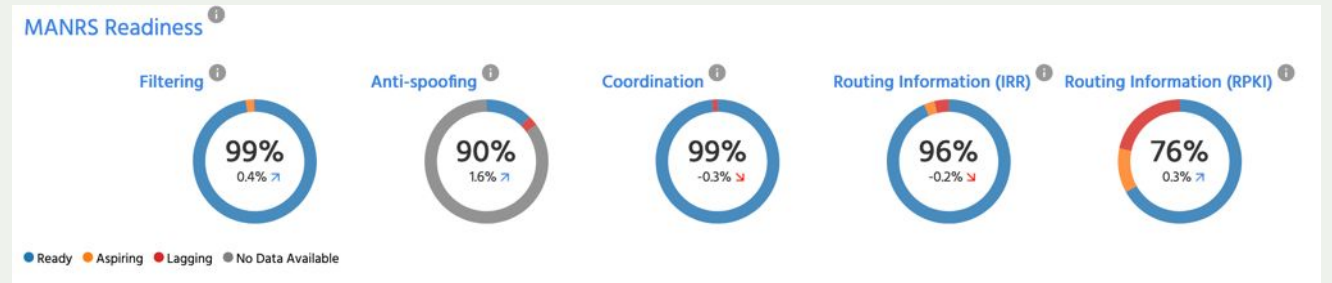
Result Limit: **100** | 200 | 500 | 1000

Total 26,421 Previous **1** 2 3 4 5 ... 265 Next

Overview

ASN	Holder	Country	UN Regions	UN Sub-Regions	RIR Regions	Filtering	Anti-spoofing	Coordination	Routing Information (IRR)	Routing Information (RPKI)
AS13	AS13 TELECOM ITALIA SPA	IT	Europe	-	RIPE NCC	100%	-	100%	94%	0%
AS133	AS133 TELECOM ITALIA SPA	IT	Europe	Southern Europe	RIPE NCC	100%	100%	100%	100%	80%
AS134	AS134 TELECOM ITALIA SPA	IT	Europe	Northern Europe	RIPE NCC	100%	100%	100%	100%	0%
AS135	AS135 TELECOM ITALIA SPA	IT	Europe	-	RIPE NCC	98%	-	100%	100%	0%
AS136	AS136 TELECOM ITALIA SPA	IT	Europe	-	RIPE NCC	100%	-	100%	100%	0%
AS137	AS137 TELECOM ITALIA SPA	IT	Europe	Western Europe	RIPE NCC	100%	-	100%	100%	0%
AS138	AS138 TELECOM ITALIA SPA	IT	Europe	Northern Europe	RIPE NCC	100%	-	100%	100%	100%
AS139	AS139 TELECOM ITALIA SPA	IT	Europe	Western Europe	RIPE NCC	100%	-	100%	100%	100%
AS140	AS140 TELECOM ITALIA SPA	IT	Europe	Western Europe	RIPE NCC	100%	100%	100%	100%	86%

MANRS Readiness



Organization Name	Date Approved	Areas Served	ASNs	Action 1 Filtering	Action 2 Anti-Spoofing	Action 3 Coordination	Action 4 Routing Information	
							IRR	RPKI
.pt	15th Oct 2018	PT	199993	✓	No data	100%	100%	100%
1-Grid	24th Oct 2023	ZA	36943	✓		100%	100%	100%
10110770 Manitoba O/A Vulpine Networks	19th Jun 2022	CA, US	400442	✓		100%	100%	100%
2012 Limited	26th Apr 2023	HK	4658	✓		100%	100%	94%
3D TELECOMUNICACOES LTDA	20th Nov 2023	SC	52706	✓	100%	100%	100%	100%
3WACCES	31st Mar 2020	BR	269053	✓	49%	100%	100%	100%
76 Telecom Telecomunicações Ltda	7th Jul 2020	BR	262760, 262363	✓		50%	100%	0%

MANRS is turning 10 years old this year



10 years of community action

Key achievements:

- Uptake: with more than 1,100 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



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

[1. What is a BCOP?](#)

[2. Summary](#)

[3. MANRS](#)

[4. Implementation guidelines for the MANRS Actions](#)

[4.1. Coordination - Facilitating global operational communication and coordination between network operators](#)

[4.1.1. Maintaining Contact Information in Regional Internet Registries \(RIRs\): AFRINIC, APNIC, RIPE](#)

[4.1.1.1. MNTNER objects](#)

[4.1.1.1.1. Creating a new maintainer in the AFRINIC IRR](#)

[4.1.1.1.2. Creating a new maintainer in the APNIC IRR](#)

[4.1.1.1.3. Creating a new maintainer in the RIPE IRR](#)

[4.1.1.2. ROLE objects](#)

[4.1.1.3. INETNUM and INET6NUM objects](#)

[4.1.1.4. AUT-NUM objects](#)

[4.1.2. Maintaining Contact Information in Regional Internet Registries \(RIRs\): LACNIC](#)

[4.1.3. Maintaining Contact Information in Regional Internet Registries \(RIRs\): ARIN](#)

[4.1.3.1. Point of Contact \(POC\) Object Example:](#)

[4.1.3.2. OrgNOCHandle in Network Object Example:](#)

[4.1.4. Maintaining Contact Information in Internet Routing Registries](#)

[4.1.5. Maintaining Contact Information in PeeringDB](#)

[4.1.6. Company Website](#)

[4.2. Global Validation - Facilitating validation of routing information on a global scale](#)

[4.2.1. Valid Origin documentation](#)

[4.2.1.1. Providing information through the IRR system](#)

[4.2.1.1.1. Registering expected announcements in the IRR](#)

[4.2.1.2. Providing information through the RPKI system](#)

[4.2.1.2.1. RIR Hosted Resource Certification service](#)

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>

Filtering: Preventing propagation of incorrect routing information

Introduction to Filtering

AS64501 Customer: 2001:db8:1001::/48 | 192.0.2.0/24

AS64502 Customer: 2001:db8:2002::/48 | 198.51.100.0/24

AS64500 MANRS Participant Network

Internet

AS B Transit Provider

AS15169 Google

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.

Prefix Hijacking Route Leaks

Internet Society

4/33

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**



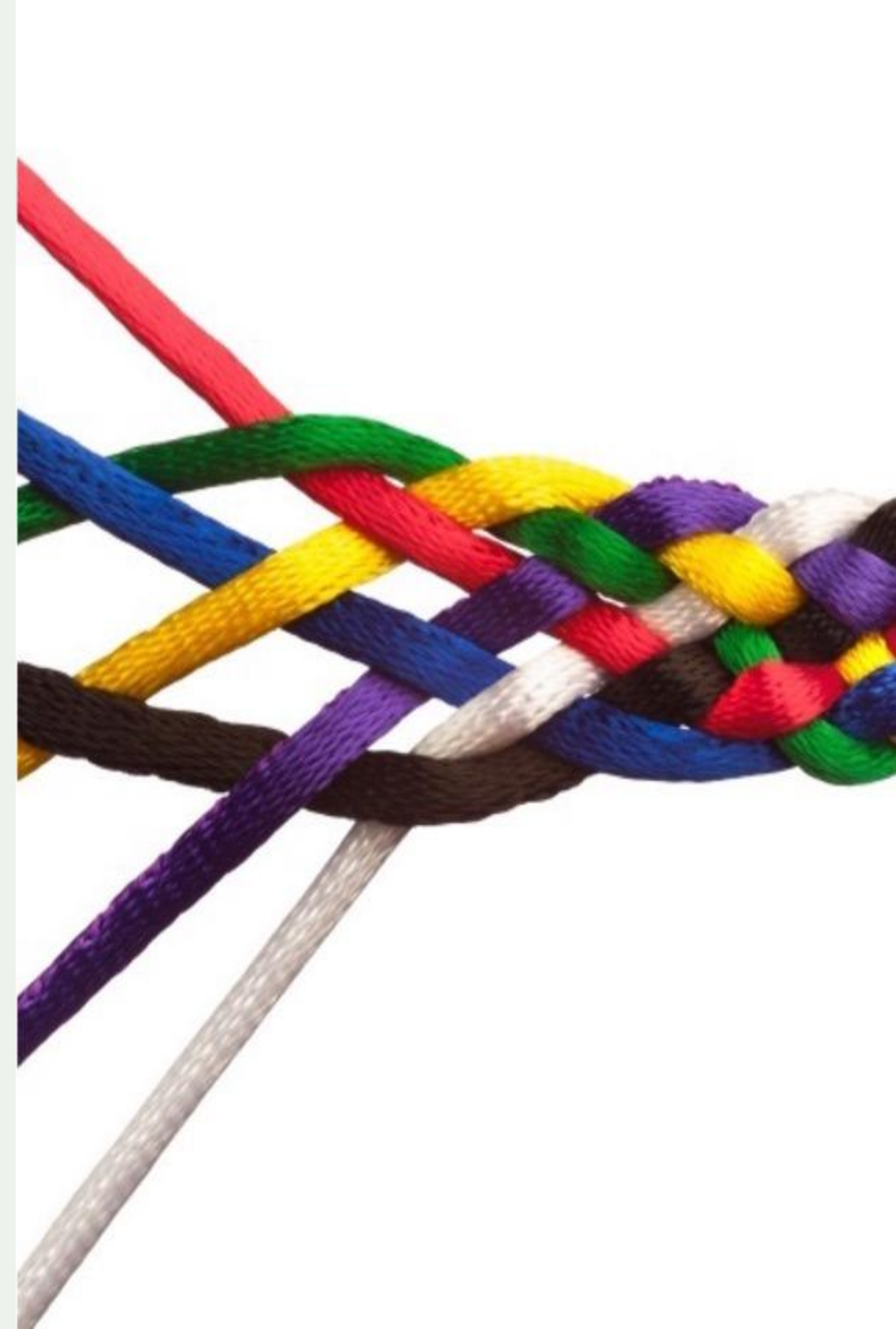
Join Us

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

