Improving routing security through concerted action

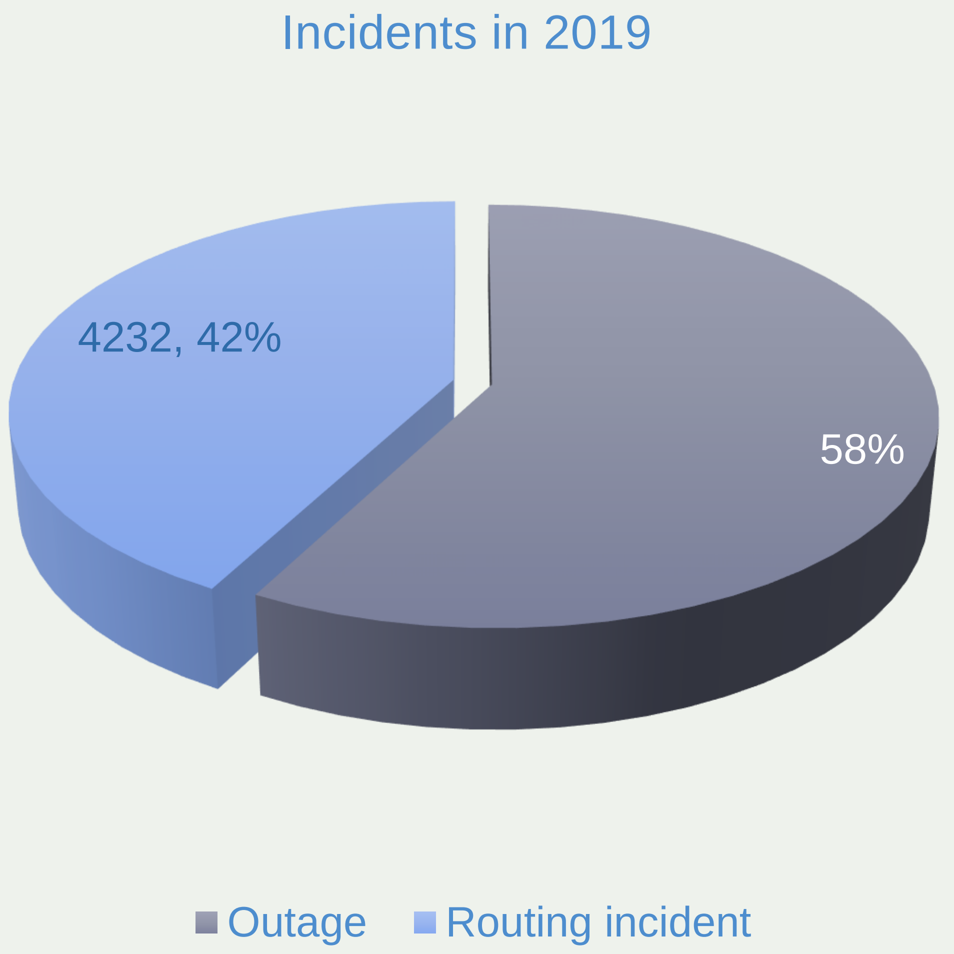
RIPE 80, May 12, 2020

Andrei Robachevsky

robachevsky@isoc.org

There is a problem (2019)

- 10,036 total incidents - either outages or attacks, like route leaks and hijacks
- 2.5% of all networks were affected by an outage
- 3.8% of all networks were affected by a routing incident
- 2% of all networks were responsible for 4232 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.* *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	The root cause of reflection DDoS attacks	*March 1, 2018. Memcached 1.3Tb/s reflection-amplification attack reported by Akamai*

Why routing security is so hard?

- Each player can contribute to routing security
  - And be the cause of an incident
- Most of them would like to have a more secure routing system
  - Routing incidents are hard to debug and fix
- Most of them have little incentive
  - One’s network security is in the hands of others

We have a typical collective action problem

We Are In This Together

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

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

Security of your network depends on measures taken by other operators.

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

Can this problem be solved without regulation?

Norms may provide a solution in some cases

- Need to agree on **values**. And **behaviors** that support these values

Common Value

- Resilient and secure global routing system

Behaviors

- Do not accept and propagate others mistakes (Validate what you accept from the neighbors)
- Protect your neighbors from your own mistakes (avoid policy violations)
  - Do not hijack
  - Do not leak
- Enable others to validate

From Behaviors to Norms

Widely accepted as a good practice

Not exactly a least common denominator, but not too high either

Visible and Measurable

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

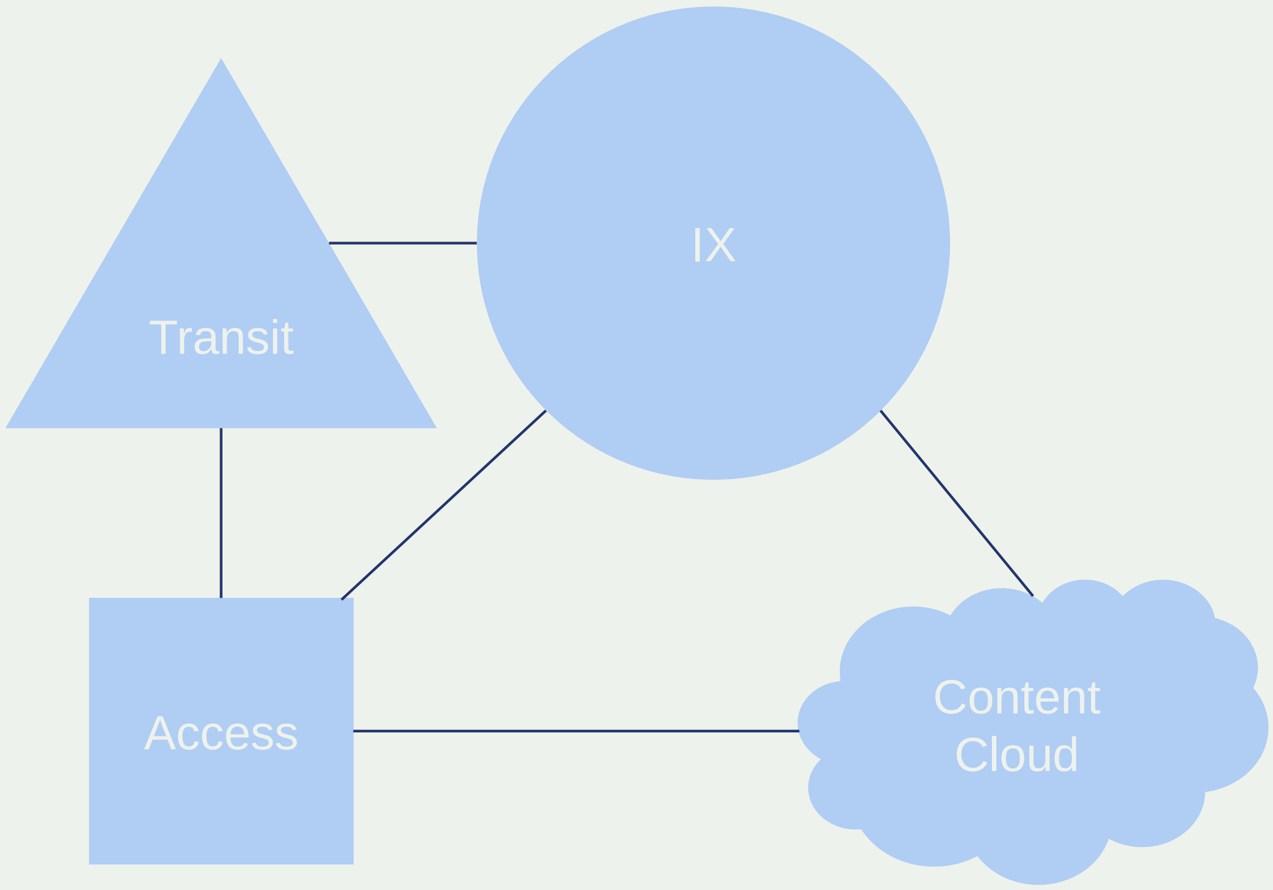
- Social acceptance and peer pressure

MANRS

MANRS – increasing adoption

Action – who can make an impact?

- Enterprise and access networks
- Transit providers
- IXPs
- CDNs and Cloud providers



Network operators – MANRS launch, November 2014

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 databases (RIR whois, IRR, PeeringDB)

Global Validation

Facilitate validation of routing information on a global scale

Publish your data, so others can validate

MANRS IXP Programme

There is synergy between MANRS and IXPs

- IXPs form communities 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 commitment of an IXP and bring significant improvement to the resilience and security of the peering relationships

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.

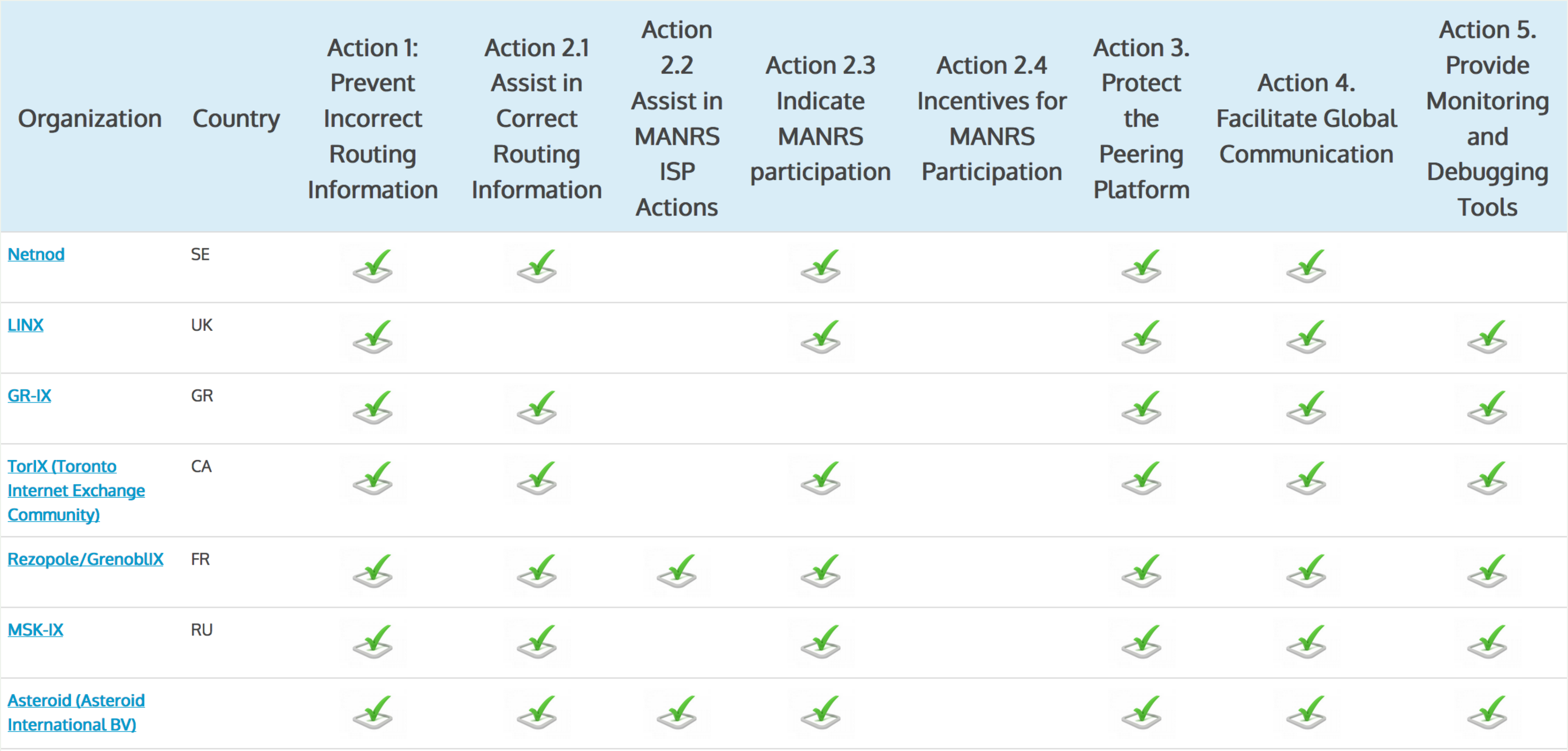
Action 4
Facilitate global operational communication and coordination

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 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)		✓	✓	✓	✓		✓	✓	✓

The CDN and Cloud programme (launched on March 31))

Leverage their peering power, but also bring benefits:

- Create a secure network peering environment, preventing potential attacks at their border
- Encourage better routing hygiene from your peering partners
- Signal organization security-forward posture
- Demonstrate responsible behavior
- Improve operational efficiency for peering interconnections, minimizing incidents and providing more granular insight for troubleshooting

The Task Force

Alejandro Becerra Gonzalez (Telefonica)

Andrei Robachevsky (Internet Society, Editor)

Arturo Servin (Google)

Carlos Asensio (Nexica)

Chris Morrow (Google)

Christian Kaufmann (Akamai)

Daniel Ponticello (Redder)

Gary Ratterree (Microsoft)

Ibrahim Seremet (Verisign)

Jerome Fleury (Cloudflare)

JJ Crawford (Facebook)

Kay Rechthien (Akamai)

Kevin Blumberg (TORIX)

Marcus Grando (Azion)

Martin J. Levy (Cloudflare)

Marty Strong (Facebook)

Rob Spiger (Microsoft)

Rogério Mariano (Azion)

Ronan Mullally (Akamai)

Ray Sliteris (Facebook)

Steve Peters (Facebook)

Tale Lawrence (Oracle)

Tony Tauber (Comcast)

Yong Kim (Verisign)

MANRS Actions for CDN&Cloud

Action 1

Prevent propagation of incorrect routing information

Egress filtering

Ingress filtering – non-transit peers, explicit whitelists

Action 2

Prevent traffic with illegitimate source IP addresses

Anti-spoofing controls to prevent packets with illegitimate source IP address

Action 3

Facilitate global operational communication and coordination

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.

Action 5

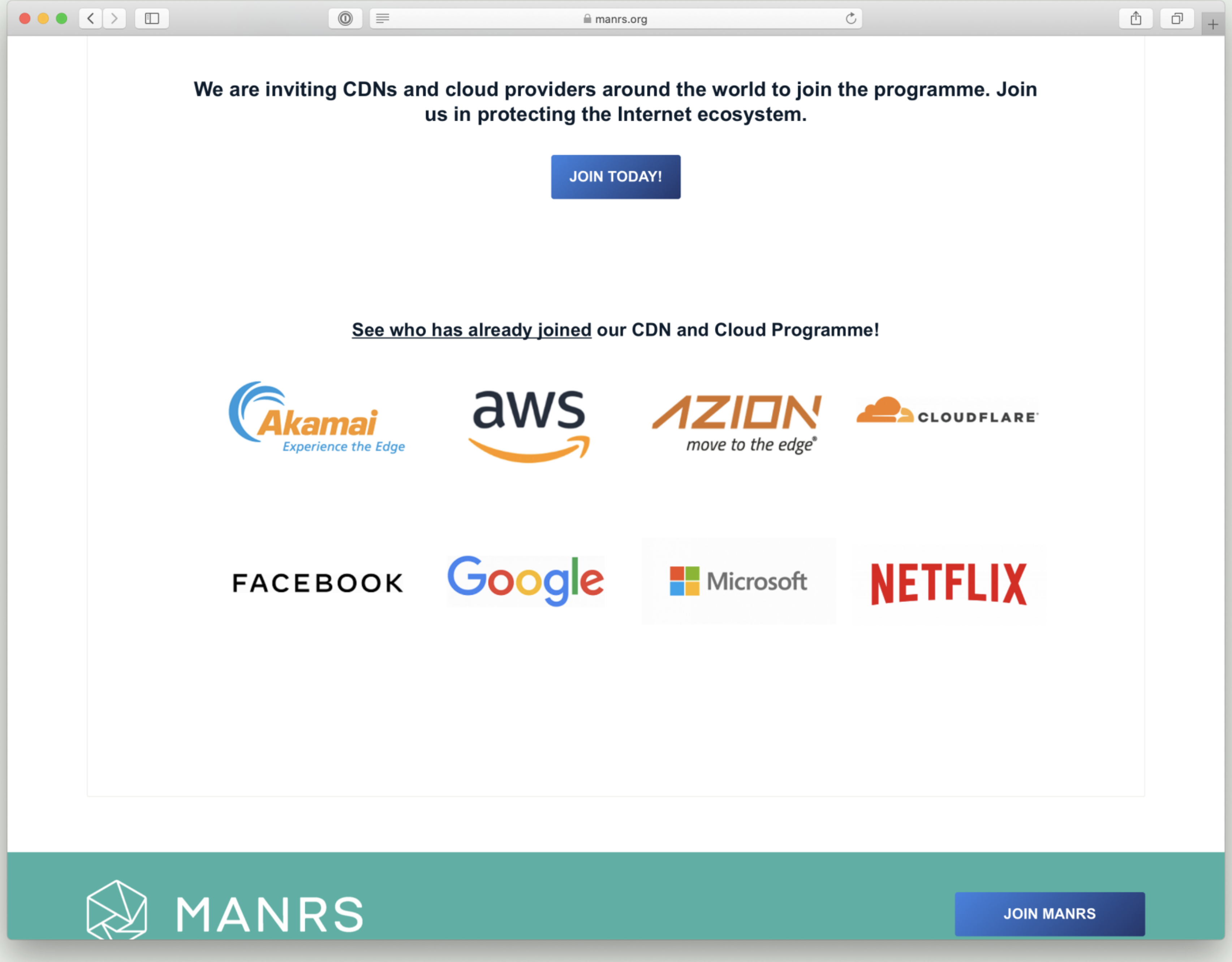
Encourage MANRS adoption

Actively encourage MANRS adoption among the peers

Action 6

Provide monitoring and debugging tools to peering partners

Provide monitoring tools to indicate incorrect announcements from peers that were filtered by the CDN&Cloud operator.



We are inviting CDNs and cloud providers around the world to join the programme. Join us in protecting the Internet ecosystem.

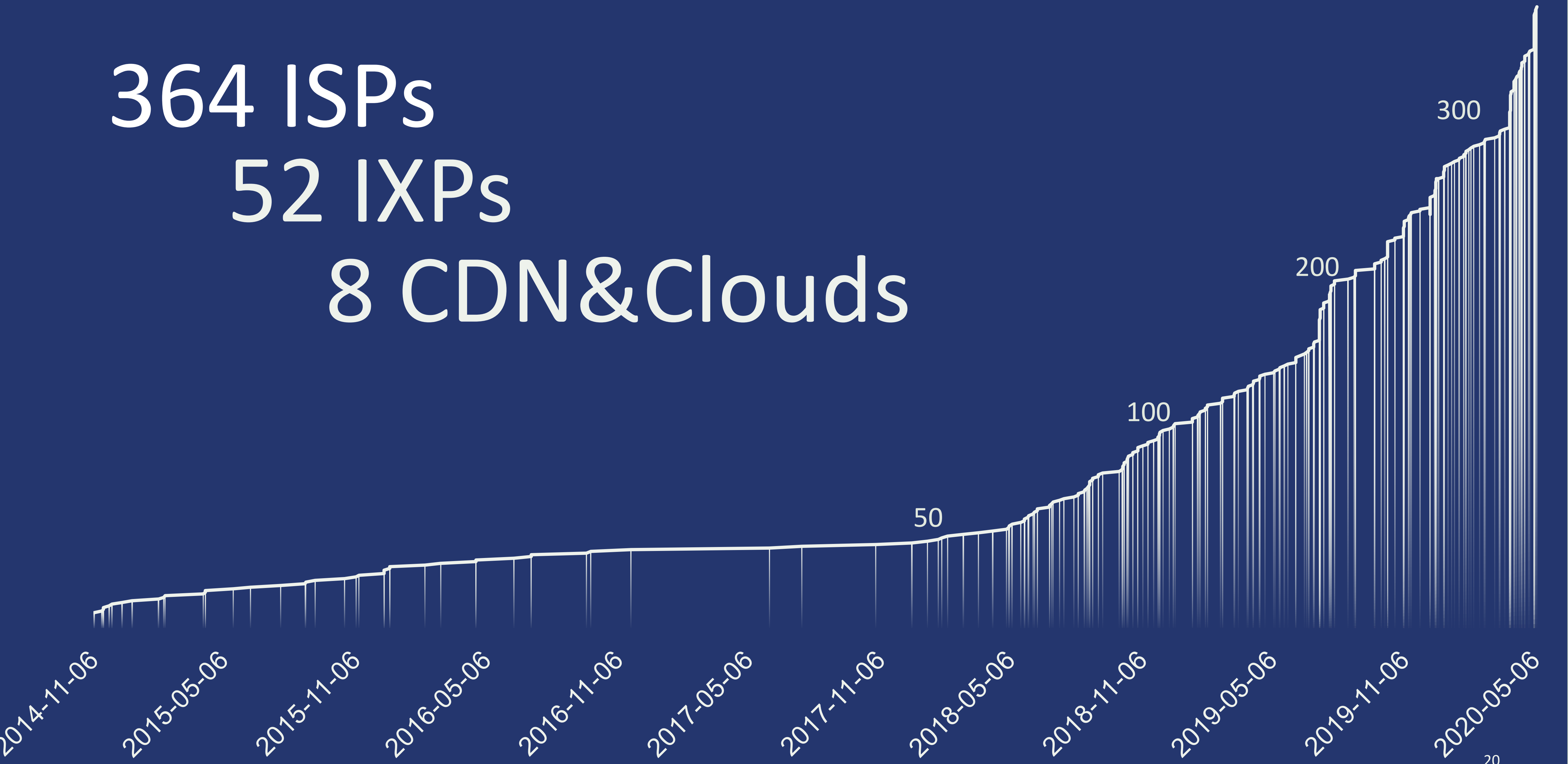
See who has already joined our CDN and Cloud Programme!

GROWTH OF THE MANRS MEMBERSHIP (NETWORK OPERATORS)

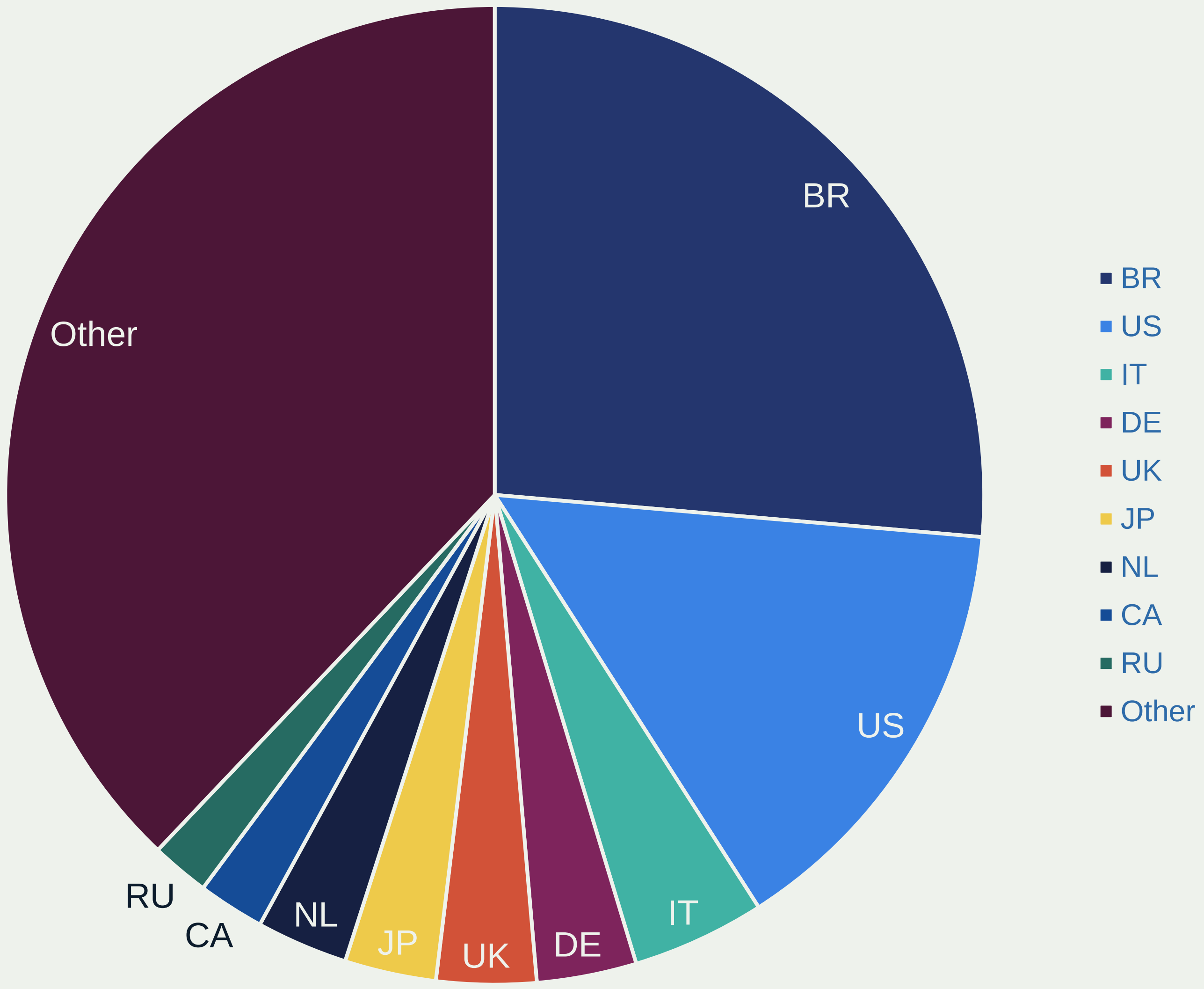
364 ISPs

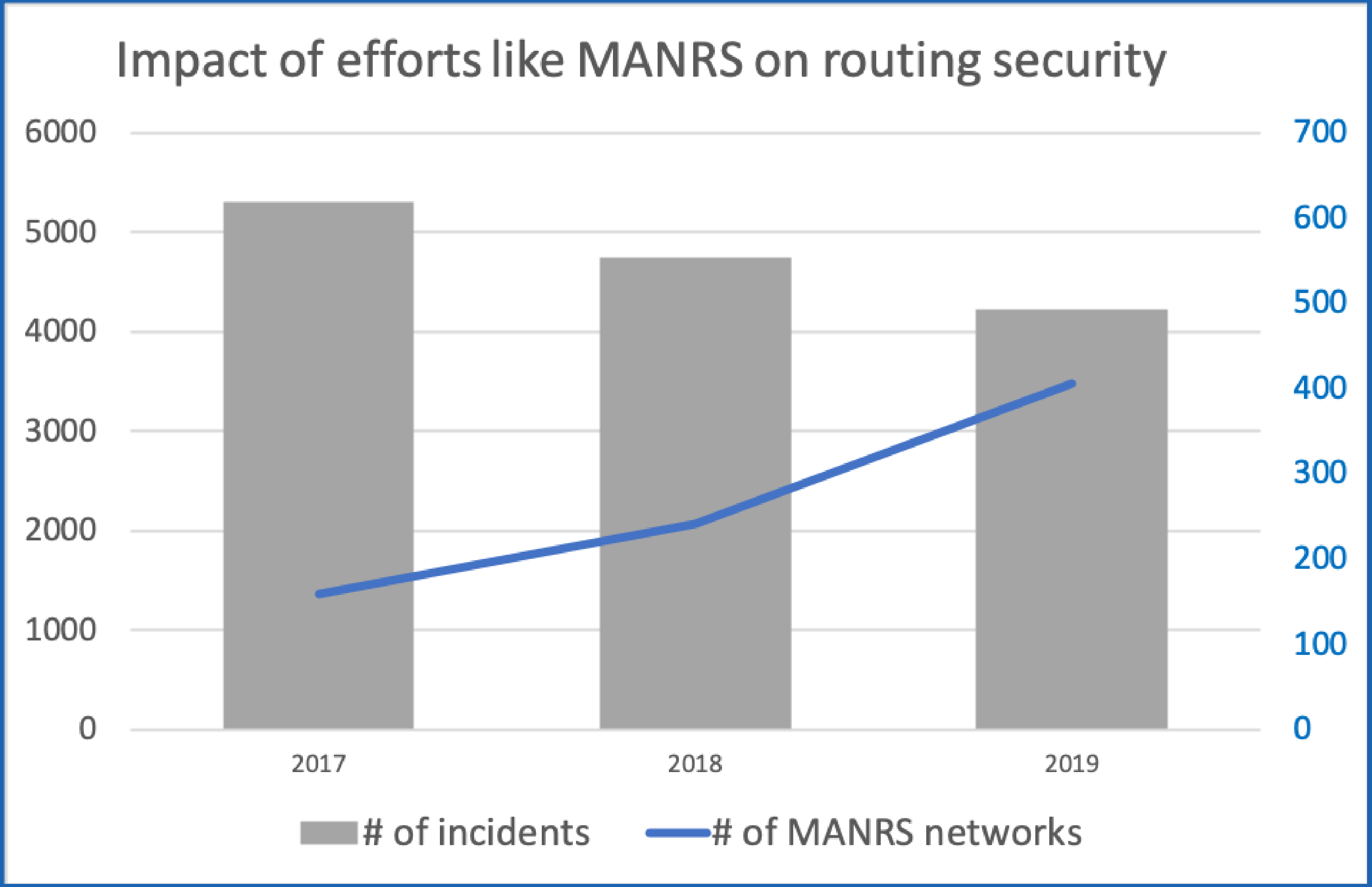
52 IXPs

8 CDN&Clouds



Demography of participants (ISPs)




Impact of efforts like MANRS on routing security
6000
5000
4000
3000
2000
1000
0
700
600
500
400
300
200
100
0
2017
2018
2019
# of incidents
# of MANRS networks

Measuring MANRS Readiness

MANRS Observatory

Motivation

Inform MANRS members about their degree of commitment

- Improve reputation and transparency of the effort
- Facilitate continuous improvement and correction

Provide a factual state of routing security as it relates to MANRS

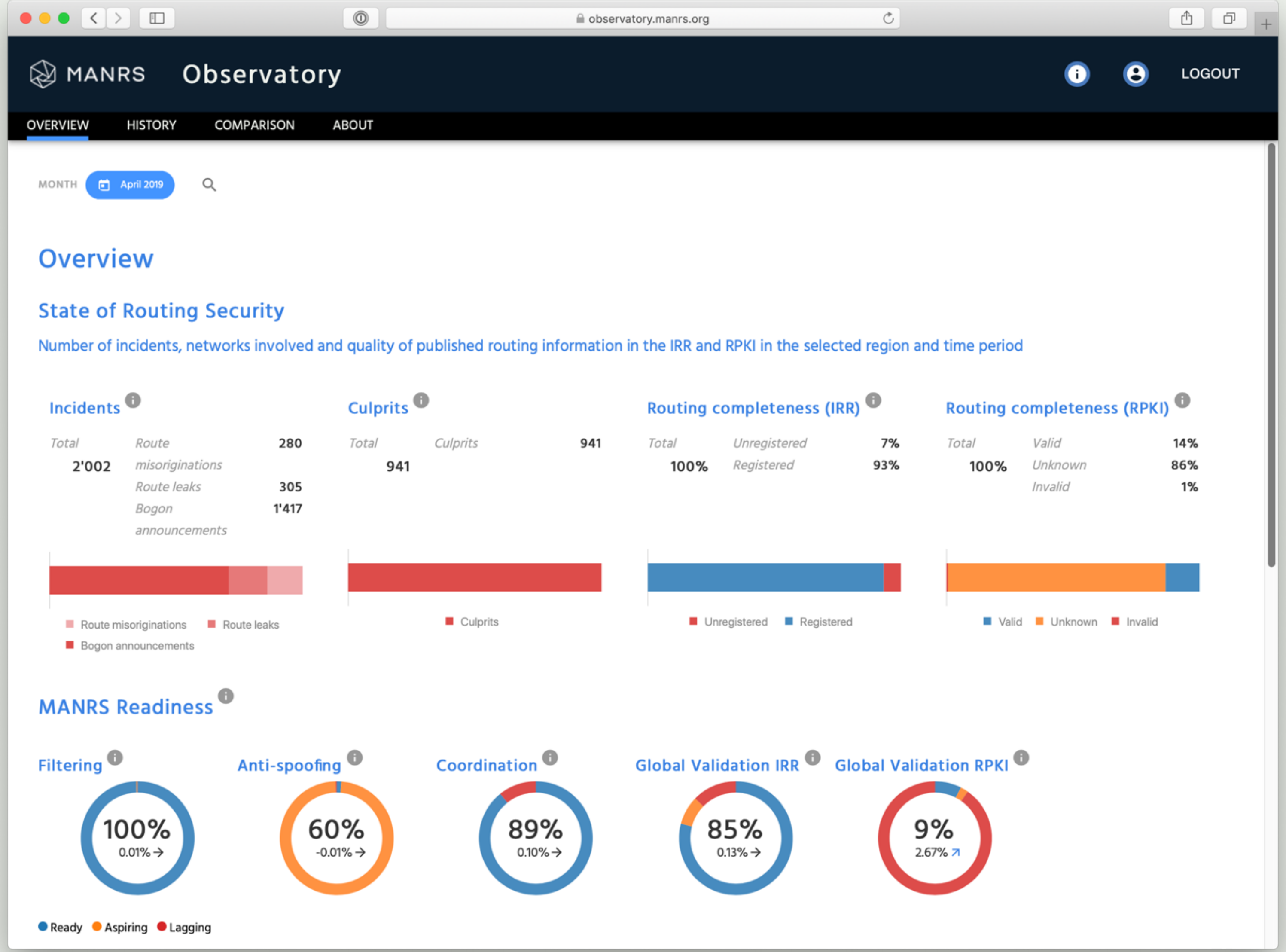
- Support the problem statement with data
- Demonstrate the impact and progress
- Network, country, region, over time

Improve robustness of the evaluation process

- Make it more comprehensive and consistent
- Reduce the load
- Allow preparation (self-assessment)

MANRS Observatory

Provides a factual state of routing security as it relates to MANRS



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

Total	*Route misoriginations*	280
2'002	*Route leaks*	305
	Bogon announcements	1'417

Culprits

Total	*Culprits*	941
941		

Routing completeness (IRR)

Total	*Unregistered*	7%
100%	*Registered*	93%

Routing completeness (RPKI)

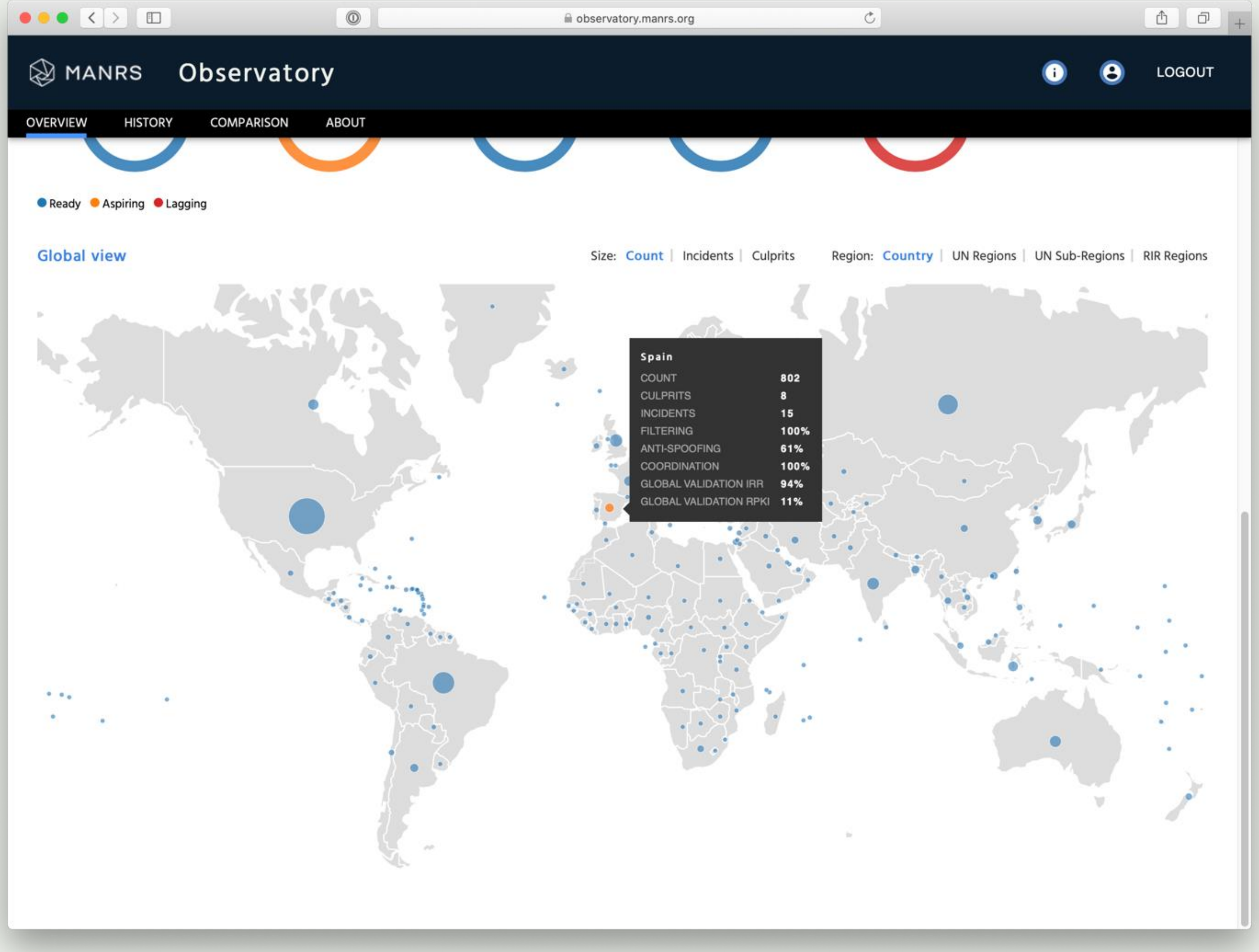
Total	*Valid*	14%
100%	*Unknown*	86%
	Invalid	1%

MANRS Readiness

Filtering	Anti-spoofing	Coordination	Global Validation IRR	Global Validation RPKI
100%	60%	89%	85%	9%
0.01% →	-0.01% →	0.10% →	0.13% →	2.67% ↗

MANRS Observatory

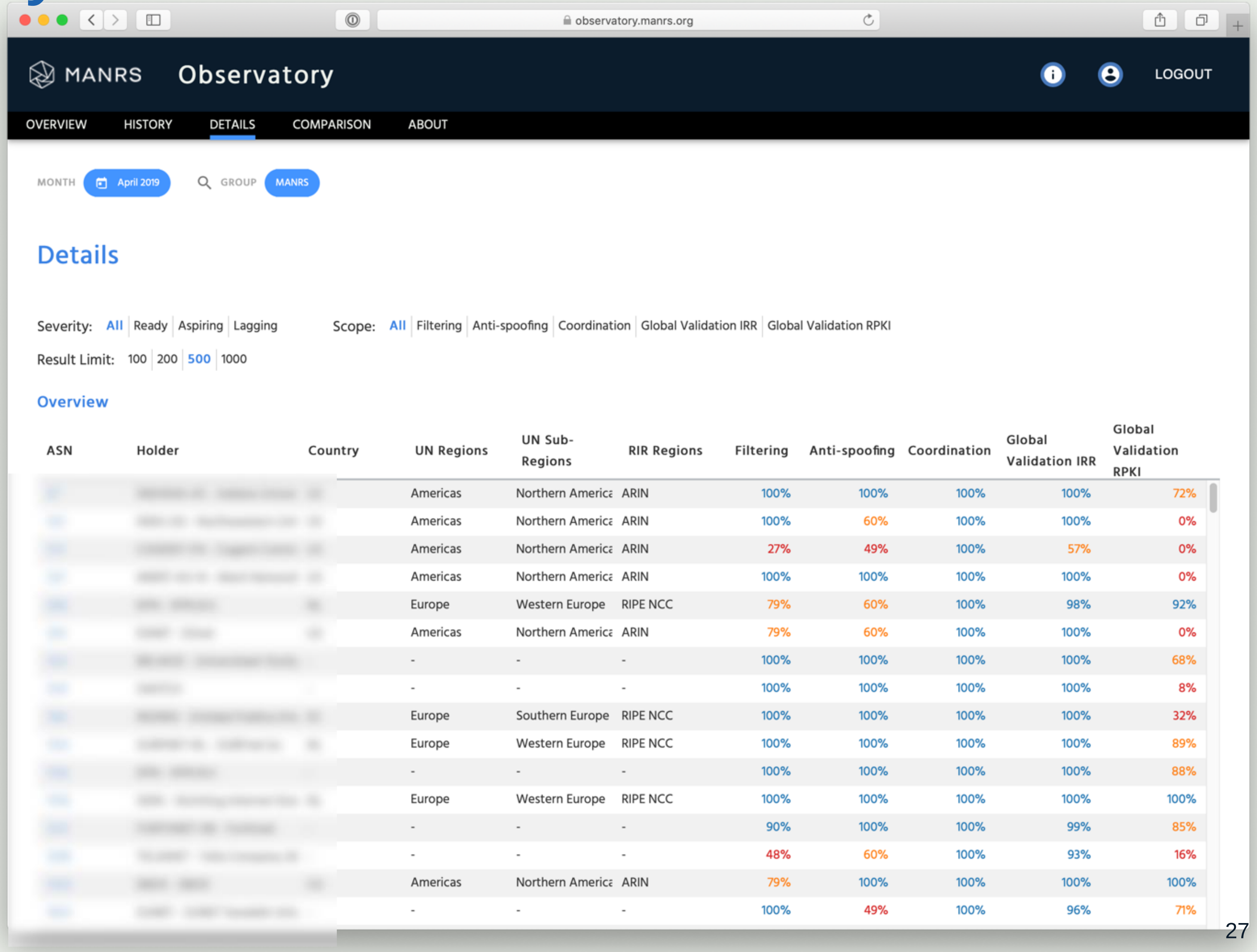
Provides a factual state of routing security as it relates to MANRS


observatory.manrs.org
MANRS
Observatory
LOGOUT
OVERVIEW
HISTORY
COMPARISON
ABOUT
● Ready ● Aspiring ● Lagging
Global view
Size: Count | Incidents | Culprits
Region: Country | UN Regions | UN Sub-Regions | RIR Regions

Spain	
COUNT	802
CULPRITS	8
INCIDENTS	15
FILTERING	100%
ANTI-SPOOFING	61%
COORDINATION	100%
GLOBAL VALIDATION IRR	94%
GLOBAL VALIDATION RPKI	11%

MANRS Observatory

Informs MANRS members about their degree of commitment



observatory.manrs.org

MONTH April 2019 GROUP MANRS

Details

Severity: All | Ready | Aspiring | Lagging

Scope: All | Filtering | Anti-spoofing | Coordination | Global Validation IRR | Global Validation RPKI

Result Limit: 100 | 200 | 500 | 1000

Overview

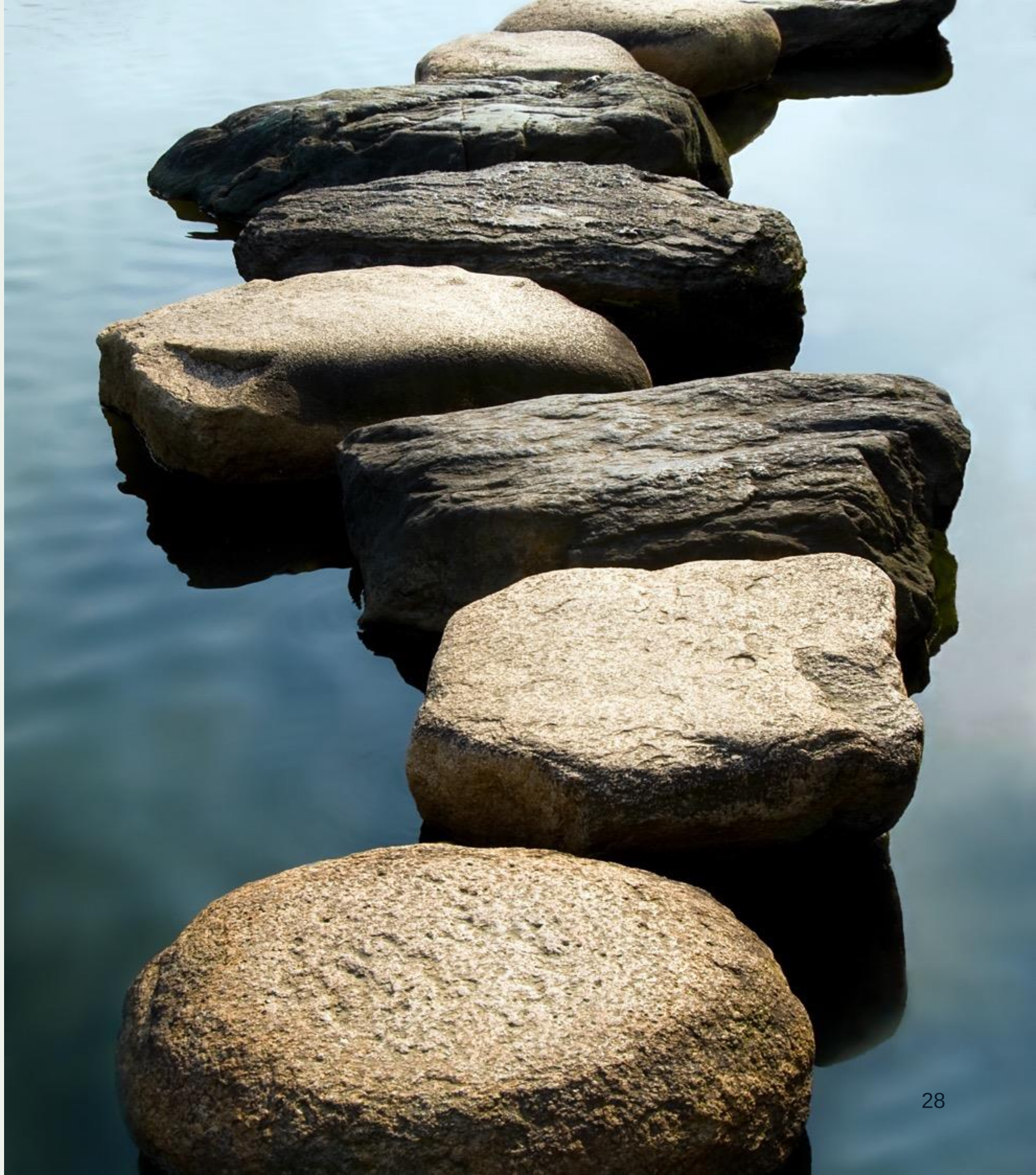
ASN	Holder	Country	UN Regions	UN Sub-Regions	RIR Regions	Filtering	Anti-spoofing	Coordination	Global Validation IRR	Global Validation RPKI
[redacted]	[redacted]	[redacted]	Americas	Northern Americ:	ARIN	100%	100%	100%	100%	72%
[redacted]	[redacted]	[redacted]	Americas	Northern Americ:	ARIN	100%	60%	100%	100%	0%
[redacted]	[redacted]	[redacted]	Americas	Northern Americ:	ARIN	27%	49%	100%	57%	0%
[redacted]	[redacted]	[redacted]	Americas	Northern Americ:	ARIN	100%	100%	100%	100%	0%
[redacted]	[redacted]	[redacted]	Europe	Western Europe	RIPE NCC	79%	60%	100%	98%	92%
[redacted]	[redacted]	[redacted]	Americas	Northern Americ:	ARIN	79%	60%	100%	100%	0%
[redacted]	[redacted]	[redacted]	-	-	-	100%	100%	100%	100%	68%
[redacted]	[redacted]	[redacted]	-	-	-	100%	100%	100%	100%	8%
[redacted]	[redacted]	[redacted]	Europe	Southern Europe	RIPE NCC	100%	100%	100%	100%	32%
[redacted]	[redacted]	[redacted]	Europe	Western Europe	RIPE NCC	100%	100%	100%	100%	89%
[redacted]	[redacted]	[redacted]	-	-	-	100%	100%	100%	100%	88%
[redacted]	[redacted]	[redacted]	Europe	Western Europe	RIPE NCC	100%	100%	100%	100%	100%
[redacted]	[redacted]	[redacted]	-	-	-	90%	100%	100%	99%	85%
[redacted]	[redacted]	[redacted]	-	-	-	48%	60%	100%	93%	16%
[redacted]	[redacted]	[redacted]	Americas	Northern Americ:	ARIN	79%	100%	100%	100%	100%
[redacted]	[redacted]	[redacted]	-	-	-	100%	49%	100%	96%	71%

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 problems, but it is an important step toward a globally robust and secure routing infrastructure.



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 operators 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

- Fill out the sign up form with as much detail as possible.
- We may ask questions and run tests

Get Involved in the Community

- Members support the initiative and implement the actions in their own networks
- Members maintain and improve the document and promote MANRS objectives

manrs.org

#ProtectTheCore

MANRS Observatory:

https://observatory.manrs.org

Questions?

https://www.manrs.org

Feedback: manrs@isoc.org