

6 July 2018

MANRS

Mutually Agreed Norms for Routing Security



Kevin Meynell
Manager, Technical & Operational
Engagement
meynell@isoc.org

The Problem

A Routing Security Overview

The Basics: How Routing Works

There are ~60,000 networks (Autonomous Systems) across the Internet, each using a unique Autonomous System Number (ASN) to identify itself to other networks.

Routers use Border Gateway Protocol (BGP) to exchange “reachability information” - networks they know how to reach.

Routers build a “routing table” and pick the best route when sending a packet, typically based on the shortest path.

The Routing Problem

Border Gateway Protocol (BGP) is based entirely on *trust* between networks

- No built-in validation that updates are legitimate
- The chain of trust spans continents
- Lack of reliable resource data



Routing Incidents are Increasing

In 2017 alone, 14,000 routing outages or attacks – such as hijacking, leaks, and spoofing – led to a range of problems including stolen data, lost revenue, reputational damage, and more.

About 40% of all network incidents are *attacks*, with the mean duration per incident lasting 19 hours.

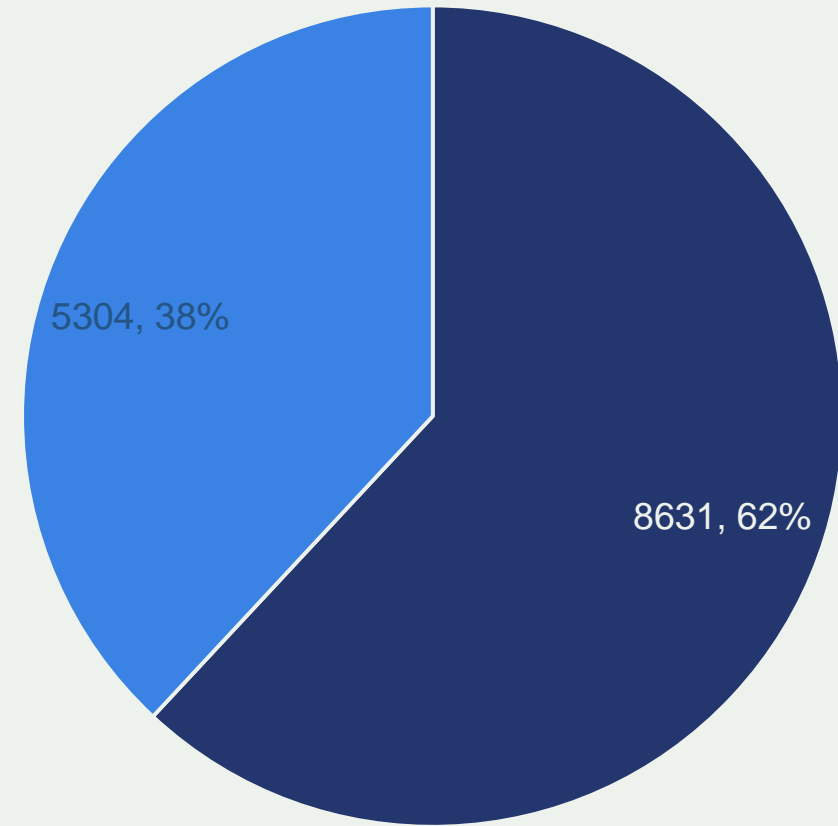
Incidents are global in scale, with one operator's routing problems cascading to impact others.

Source: BGPStream

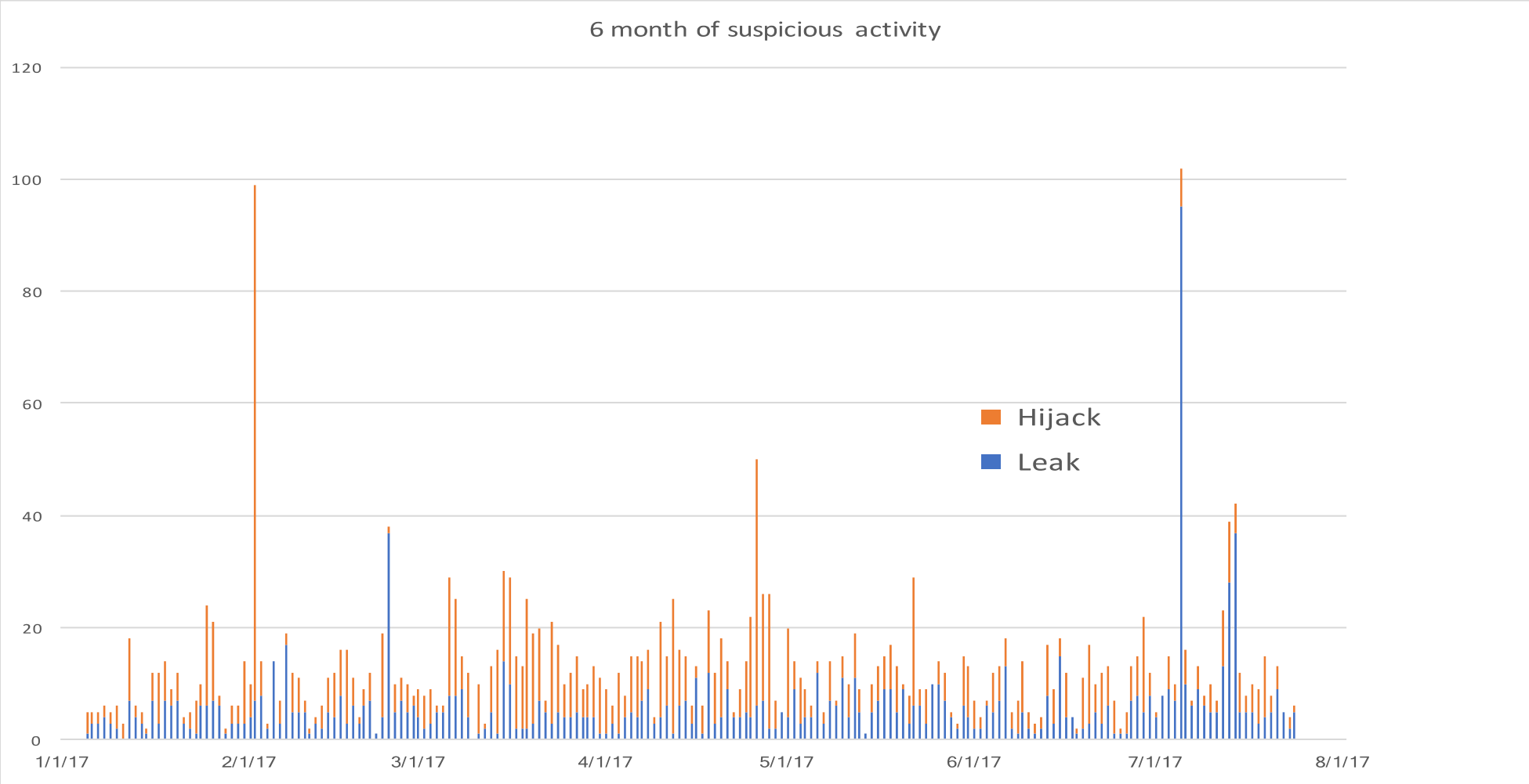
The routing system is constantly under attack (2017)

- 13,935 total incidents (either outages or attacks, like route leaks and hijacks)
- Over 10% of all Autonomous Systems on the Internet were affected
- 3,106 Autonomous Systems were a victim of at least one routing incident
- 1,546 networks were responsible for 5304 routing incidents

Twelve months of routing incidents



No Day Without an Incident



Which Leads To ...



CNET > Tech Culture >
How Pakistan knocked YouTube offline (a

How Pakistan knocked YouTube offline (and how UK traffic diverted through Ukraine happens as a result)

Posted by Andree Toonk - November 6, 2015 - Hijack - 1 Comment

MARCH 12, 2015 COMMENTS (35) VIEWS: 37374 ENGINEERING, INTERNET, LATENCY, PERFORMANCE, SECURITY
DOUG MADORY

Routing Leak briefly takes down Google

Massive route leak causes Internet slowdown
Posted by Andree Toonk - June 12, 2015 - BGP instability - No Comments

DDoS Attacks Storm Linode Servers Worldwide

BY DOUGLAS BONDERUD • JANUARY 5, 2016

MARCH 13, 2015 COMMENTS (34) VIEWS: 47297 SECURITY DOUG MADORY

UK traffic diverted through Ukraine

Global Impacts of Recent Leaks

Event type	Country	ASN
BGP Leak		Origin AS: PO box T511 Ph... Leaker AS: Viettel Corpora...
BGP Leak		Origin AS: Lirax net EOC... Leaker AS: Traffic Broa...

BGP hijack incident by Syrian telecom...
Posted by Andree Toonk - December 9, 2014 - Hijack - 2 Comments

JANUARY COMMENTS (17) VIEWS: 36909 SECURITY DOUG MADORY

The Vast World of Fraudulent Routing

CSO

Home > Data Protection > Cyber Attacks/Espionage

TODAY'S TOP STORIES

DDoS attack on BBC may have been biggest in history

Most read:

On-going BGP Hijack Targets Palestinian ISP

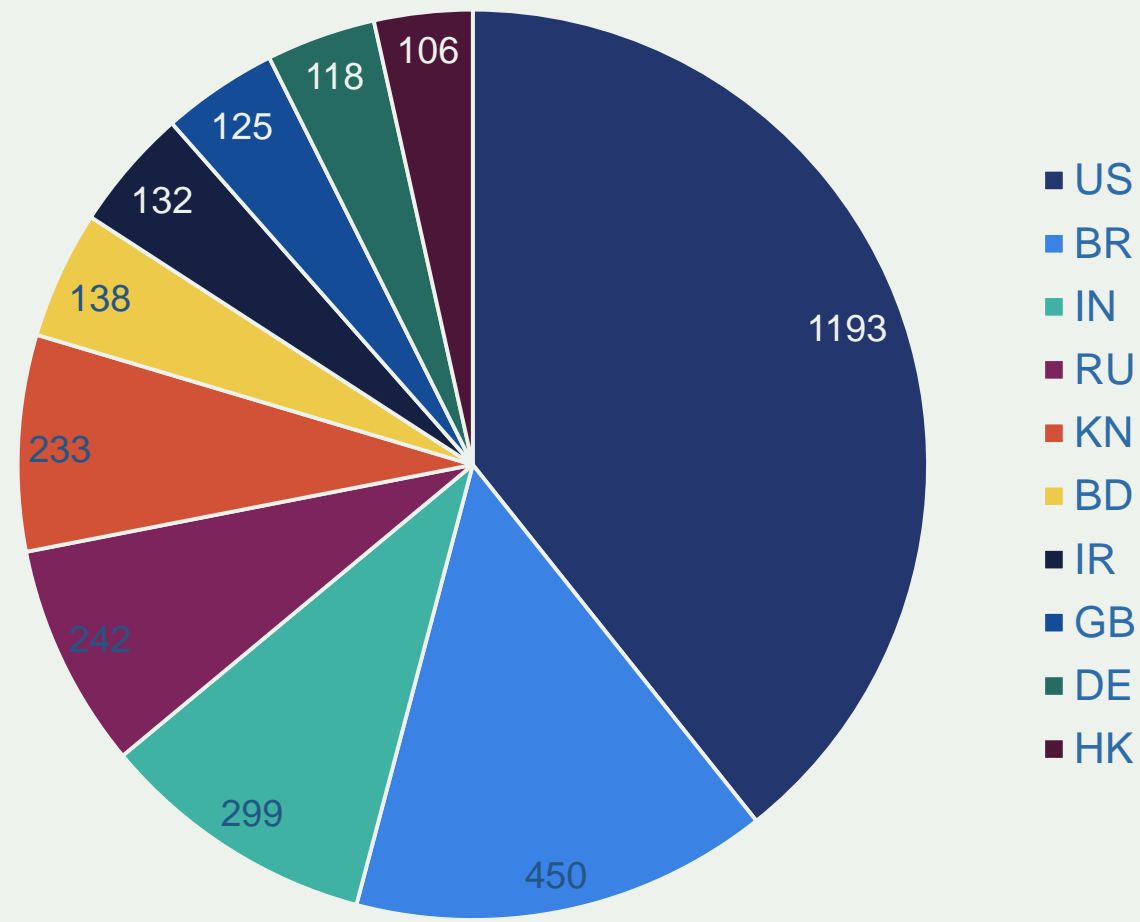
JANUARY 9, 2015 COMMENTS (2) VIEWS: 23018 UNCATEGORIZED DOUG MADORY

Routing Incidents Cause Real World Problems

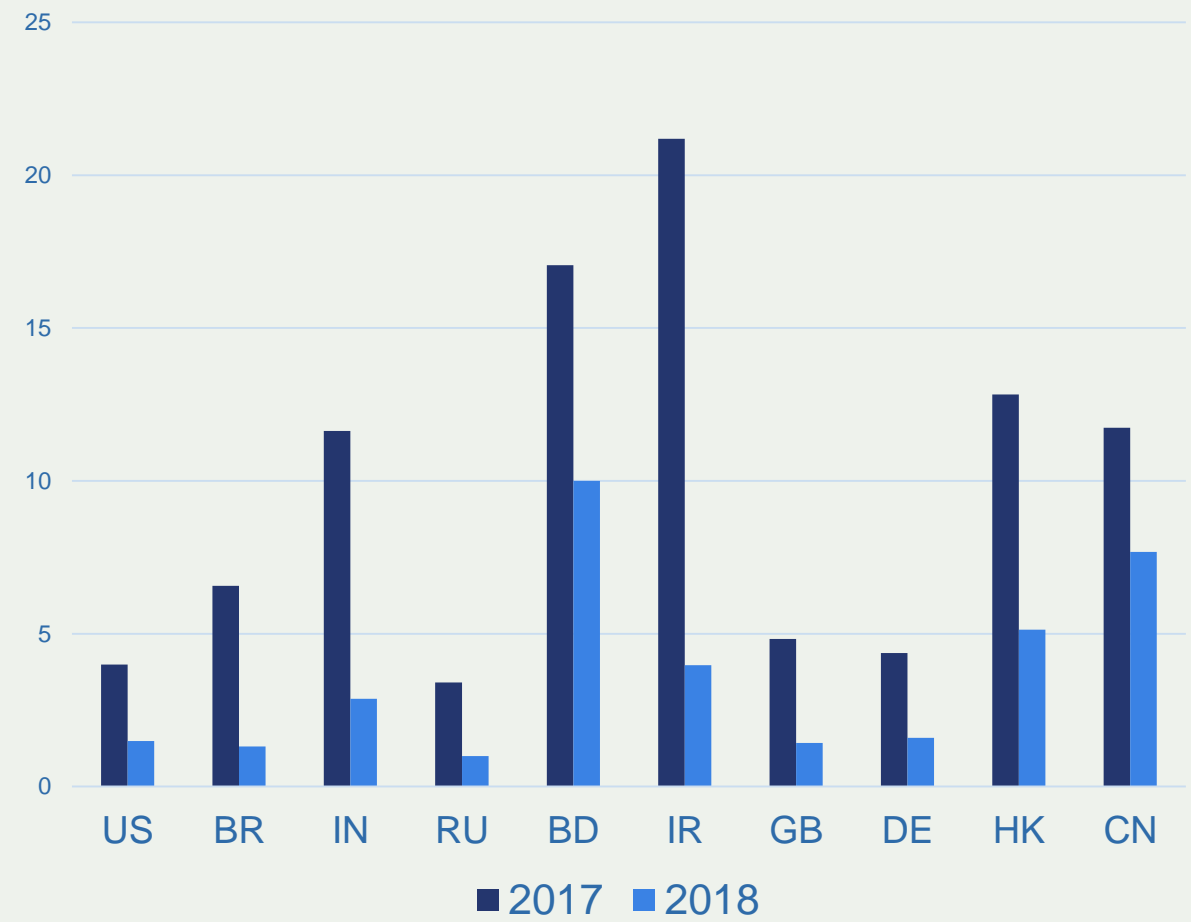
Event	Explanation	Repercussions	Example
Prefix/Route Hijacking	A network operator or attacker impersonates another network operator, pretending that a server or network is their client.	Packets are forwarded to the wrong place, and can cause Denial of Service (DoS) attacks or traffic interception.	<i>The 2008 YouTube hijack April 2018 Amazon Route 53 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>September 2014. VolumeDrive began announcing to Atrato nearly all the BGP routes it learned from Cogent causing disruptions to traffic in places as far-flung from the USA as Pakistan and Bulgaria.</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>

Potential victims

Incidents with a victim in a country, Top 10, 2017

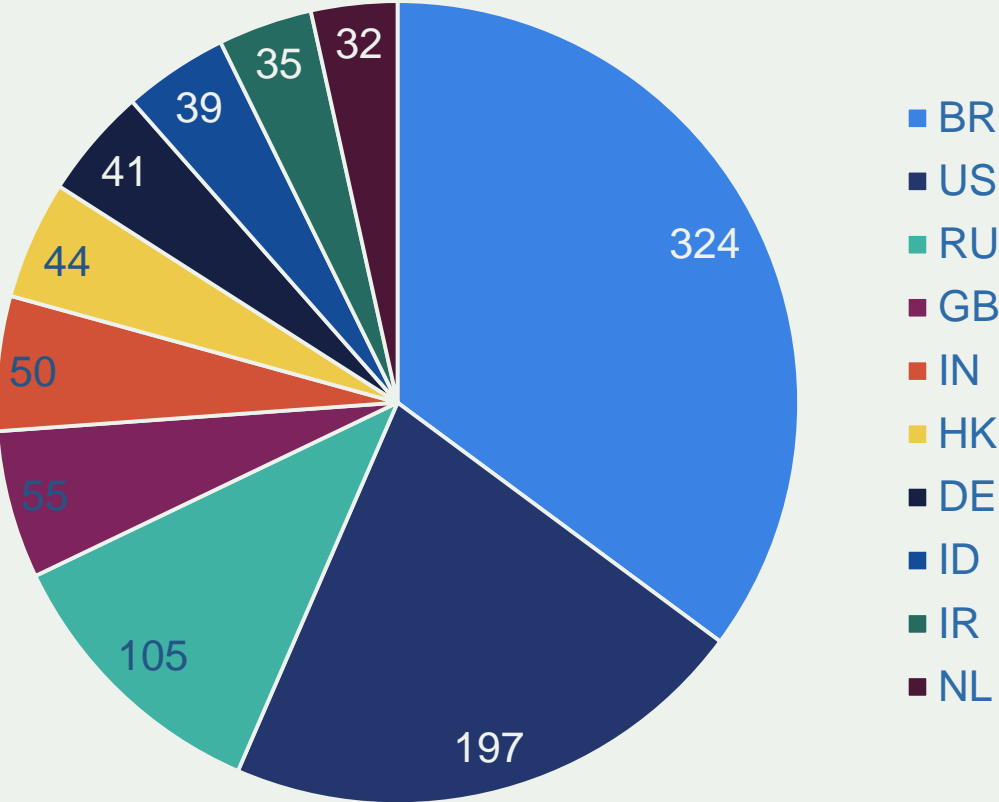


Changes in % of victimized network in country

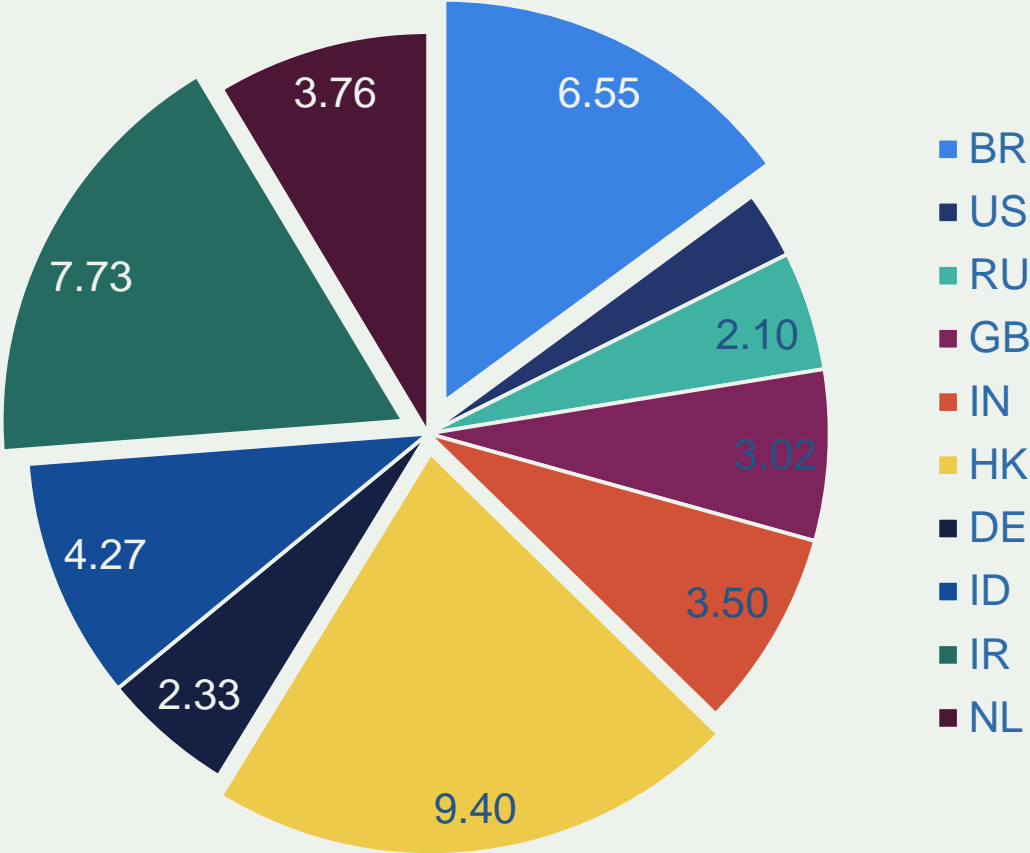


Potential culprits 2017

Number of AS's in a country responsible for a routing incident (a route leak or hijack)



Percent of AS's in a country responsible for a routing incident (a route leak or hijack)



Are there Solutions?

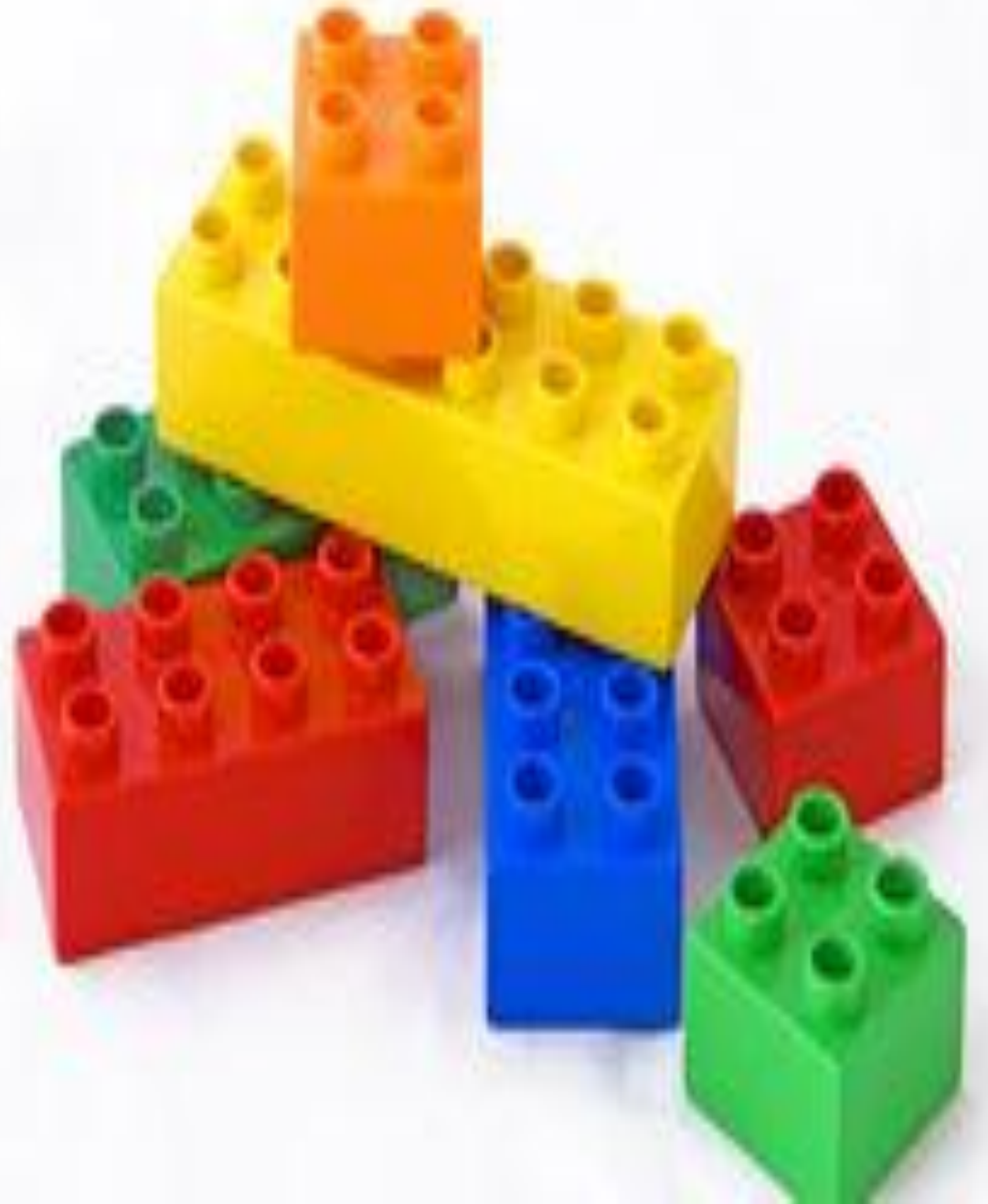
Yes...

- 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 standard approach

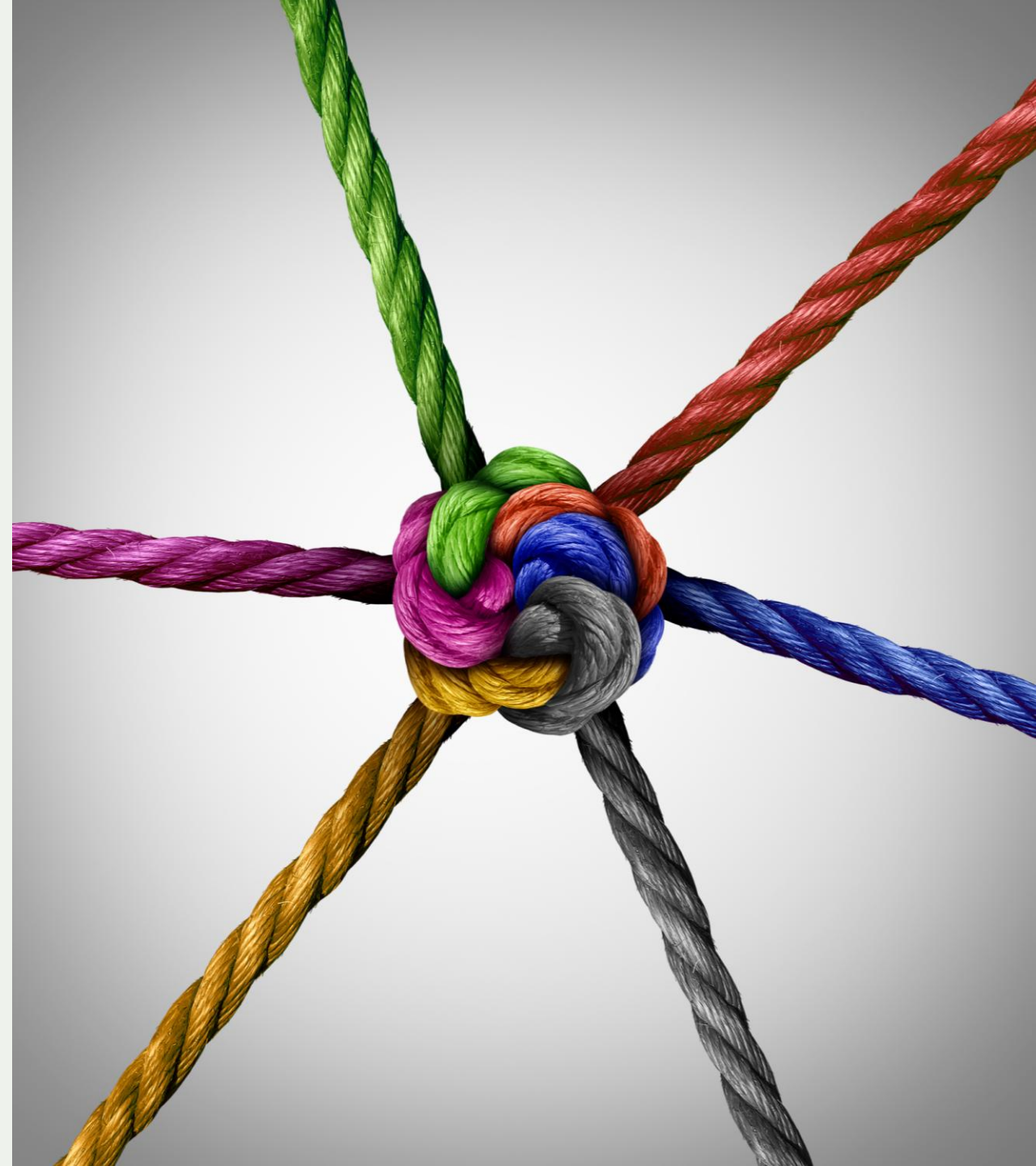


We Are In This Together

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)

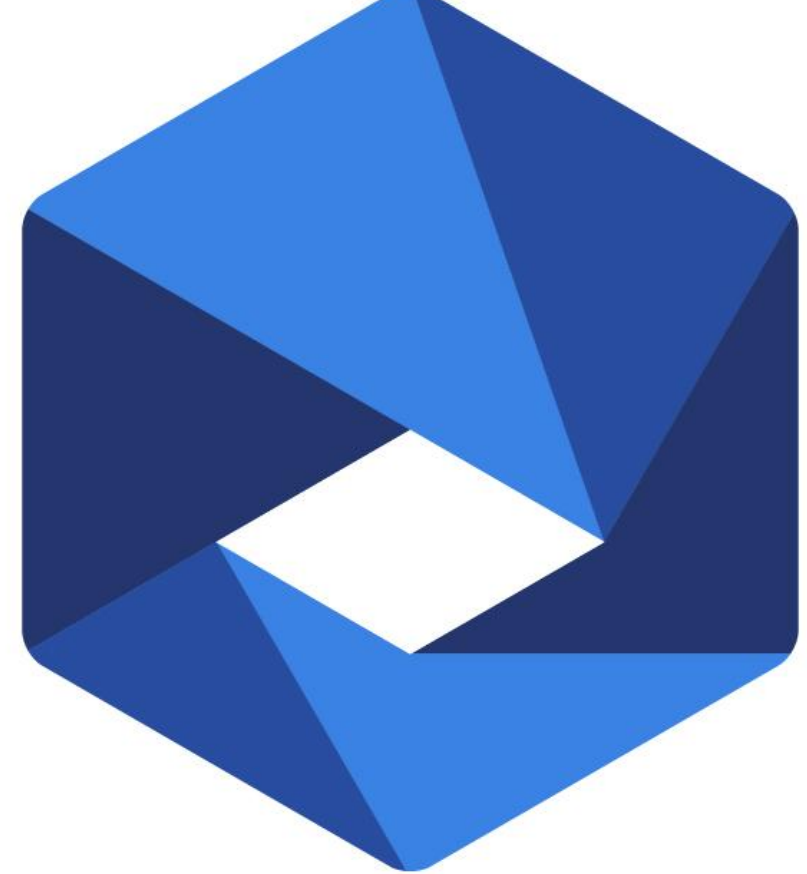
Provides crucial fixes to eliminate the most common routing threats

MANRS improves the security and reliability of the global Internet routing system, based on collaboration among participants and shared responsibility for the Internet infrastructure.

Mutually Agreed Norms for Routing Security

MANRS defines four simple but concrete actions that network operators must implement to dramatically improve Internet security and reliability.

- The first two operational improvements eliminate the root causes of common routing issues and attacks, while the second two procedural steps improve mitigation and decrease the likelihood of future incidents.



IANIR

MANRS Actions

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

Everyone benefits from improved Routing Security

Joining MANRS means joining a community of security-minded network operators committed to making the global routing infrastructure more robust and secure.

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

Consistent MANRS adoption yields steady improvement, but we need more networks to implement the actions and more customers to demand routing security best practices.

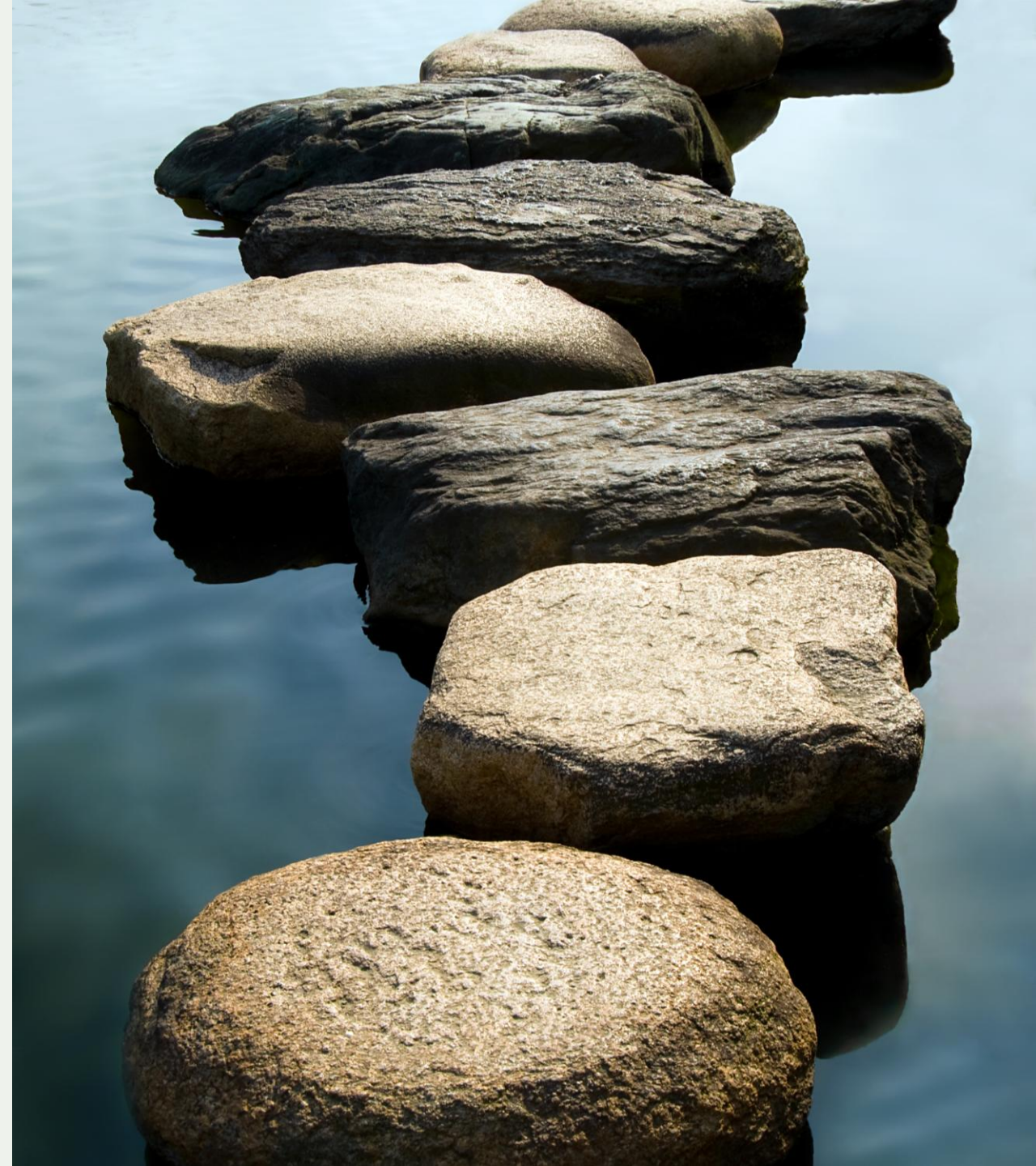
The more network operators apply MANRS actions, the fewer incidents there will be, and the less damage they can do.

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



The Business Case for MANRS and Routing Security

Engaged 451 Research to better understand the attitudes and perceptions of Internet service providers and the broader enterprise community around the project



What We Learned from the Study

Security is Vital to Enterprises

- MANRS knowledge is low, but the desire for security is high
- Enterprises are willing to require MANRS compliance of their service providers

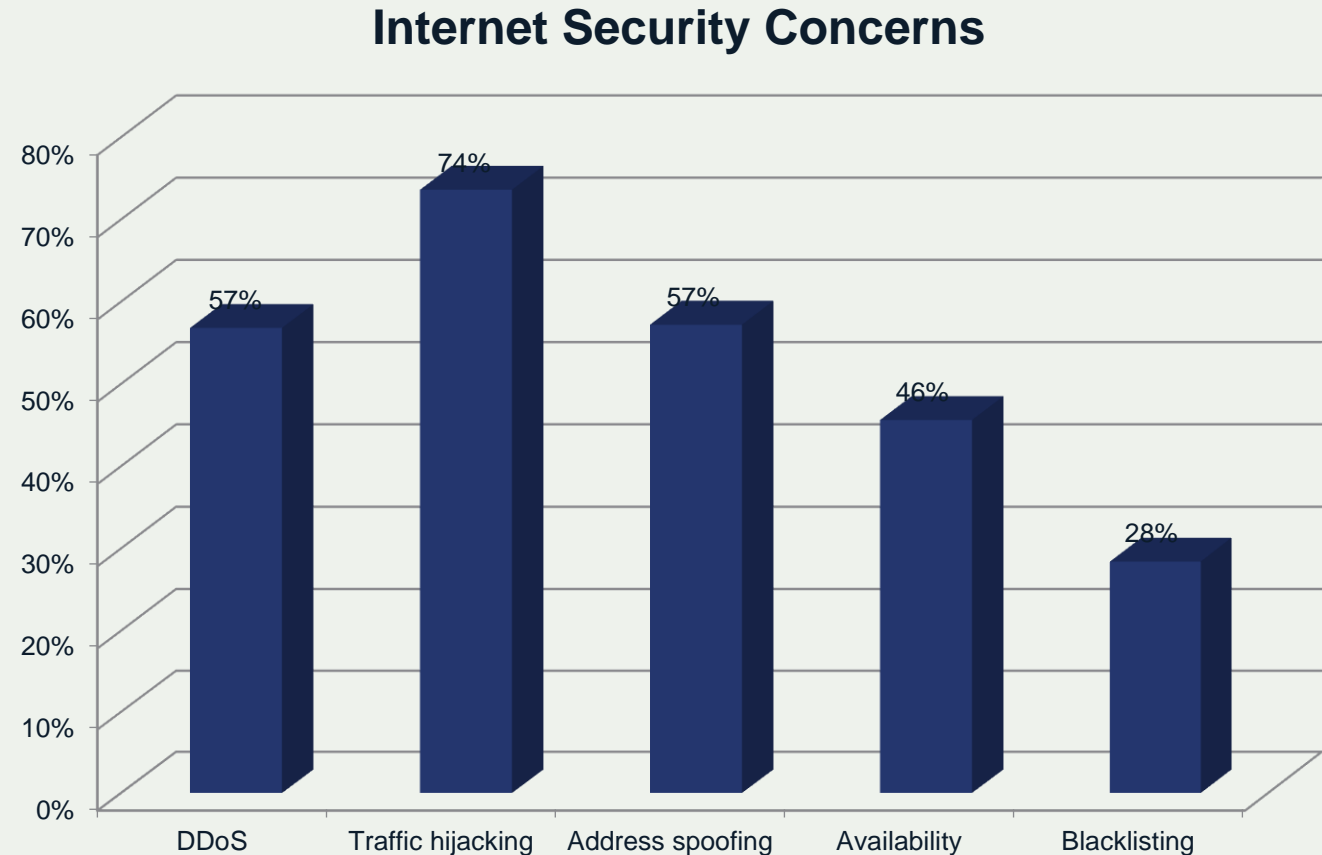
MANRS Adds Value for Service Providers

- Security can help service providers differentiate from their competitors; Identifiable value in a vague market
- Service providers may be able to add additional revenue streams based on information security feeds and other add-on services



Enterprise Security Concerns

- Widely varying concerns across a range of issues, with traffic hijacking leading the list
- Security focus is aligned with types of issues MANRS is looking to address
- Confidence that MANRS can help long-term routing security



MANRS Participants in Greece



206 ASNs assigned to Greece

2 ASNs participating in MANRS (0.97%)

FORTHnet AS1241)

- 4 actions

GRNET (AS 5408)

- 4 actions

GR-IX involved in MANRS IXP Partnership programme – (5 actions)

How to Implement MANRS

Documentation, Training & Tools

MANRS Implementation Guide

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

[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 Training Tutorials and Hands-on Lab

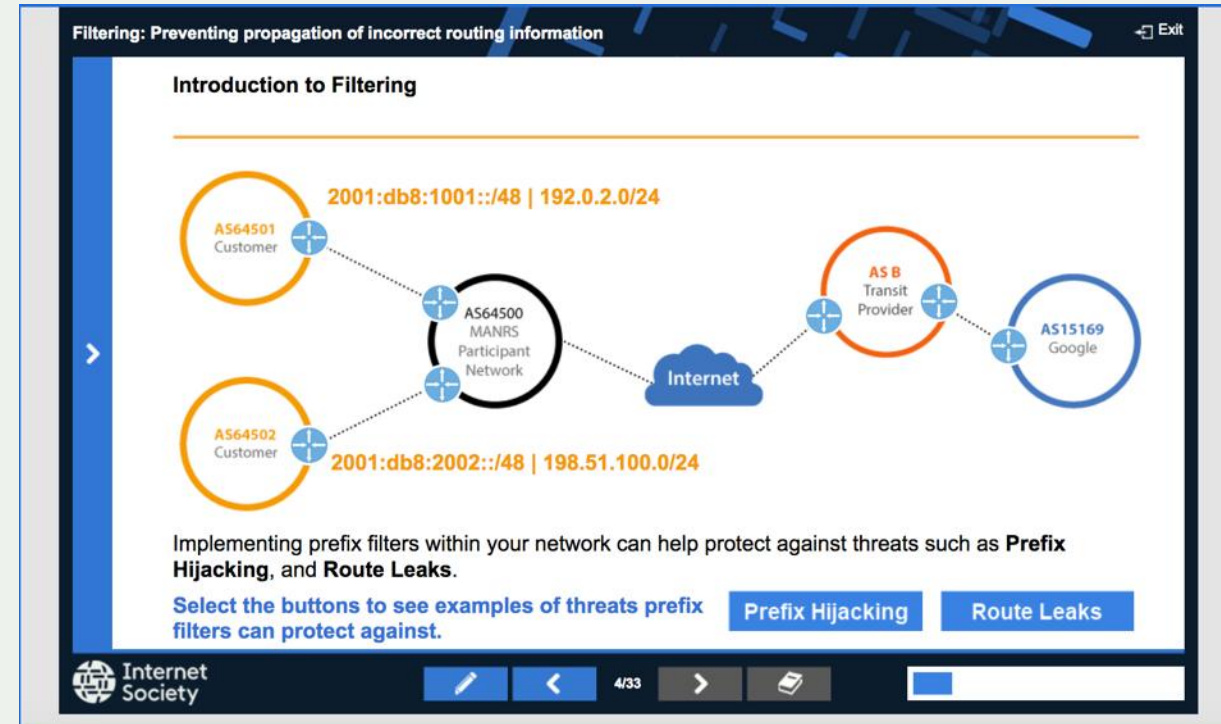
6 training tutorials based on information in the Implementation Guide.

A test at the end of each tutorial.

About to begin training moderators for online classes (43 applications received!)

The prototype lab is ready, finalizing the production version.

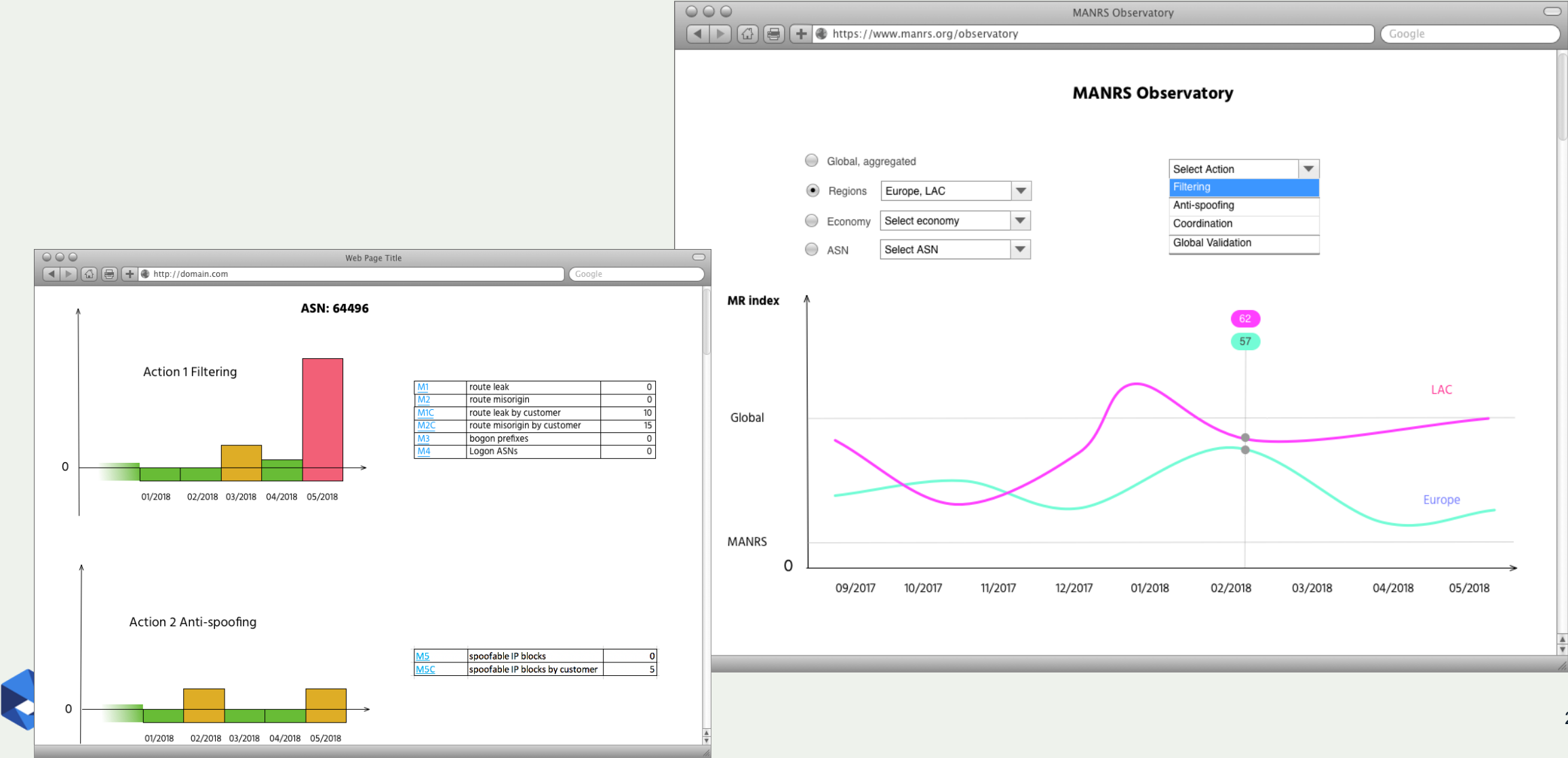
<https://www.manrs.org/tutorials>



Measuring Routing Security: MANRS Observatory

- Impartial benchmarking of MANRS members to improve reputation and transparency
- Provide factual state of security and resilience of Internet routing system over time
- Support the problem statement with data
- Self-assessment purposes and automating sign-up
- How to Measure?
 - Transparent - Use publicly available data sources and open source code
 - Passive - No cooperation is required from a network
- Metrics - Measure the rate of member (ASN) commitment (0 – non-compliant to 100 – fully compliant)

MANRS Member Report and MANRS Observatory




MANRS 'Ambassadors'

Overview



What is a MANRS ‘Ambassador’?

MANRS should be (and is) a collaborative initiative of Internet operators

- Internet operators undertaking MANRS principles need to encourage use of best practices
- A MANRS ‘ambassador’ is an opinion leader in his/her community who strongly believes that routing security is an essential component for the future well being of the Internet
- Generate MANRS awareness through word-of-mouth, presentations and social media in their communities
- Bring forward feedback and recommendations for improving MANRS principles, tools and disseminating best practices, e.g. MANRS observatory, network monitoring tools, and training materials
- Internet Society can help with presentations, informational materials and merchandise
 (shirts and stickers)

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 Programme – launched on 23 April!

IXP Participants

IXPs are important partners in the MANRS community

IXPs can be a collaborative focal point to discuss and promote the importance of routing security. To address the unique needs and concerns of IXPs, the community created a related but separate set of [MANRS actions for IXP members](#).

[Click Here to Join!](#)

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
INEX (Internet Neutral Exchange Association CLG)	IE	✓	✓		✓		✓	✓	✓
TorIX (Toronto Internet Exchange Community)	CA	✓	✓		✓		✓	✓	✓
DE-CIX	DE	✓	✓				✓	✓	✓
MSK-IX	RU	✓	✓		✓		✓	✓	✓
Netnod	SE	✓	✓		✓		✓	✓	
CRIX (NIC Costa Rica)	CR	✓	✓	✓	✓	✓		✓	✓
Asteroid (Asteroid)		✓	✓	✓	✓		✓	✓	✓



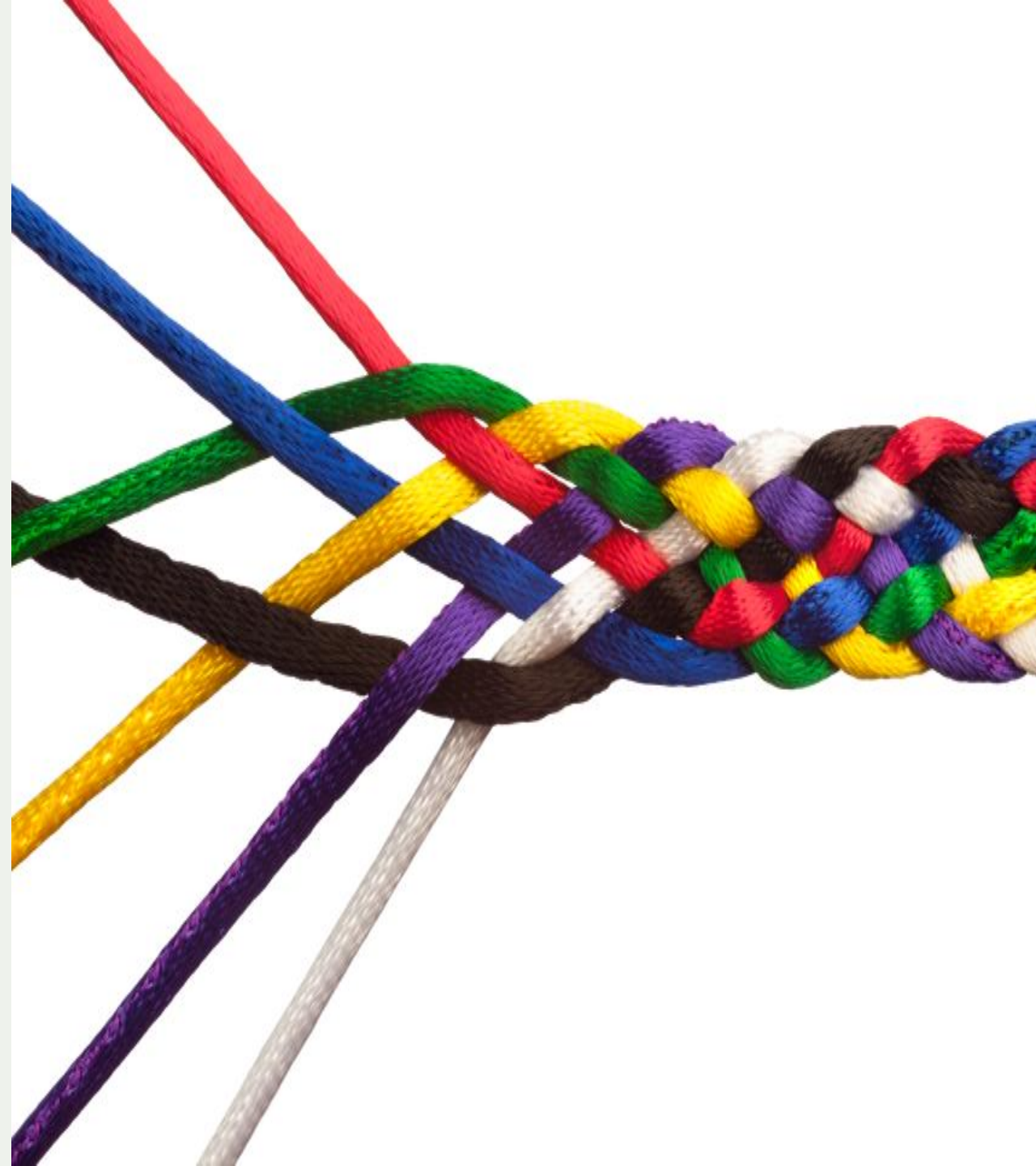
Join Us

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



Thank you.

Kevin Meynell
meynell@isoc.org

Visit us at
www.internetsociety.org
Follow us
[@internetsociety](https://twitter.com/internetsociety)

Galerie Jean-Malbuisson 15,
CH-1204 Geneva,
Switzerland.
+41 22 807 1444

1775 Wiehle Avenue,
Suite 201, Reston, VA
20190-5108 USA.
+1 703 439 2120