26 - 28 August 2019
SAFNOG 5

Routing Security – What it matters

Michuki Mwangi
Regional Development Manager for Africa
Mwangi@isoc.org

Background

There are 64,420 networks (Autonomous Systems) connected to Internet, each using a unique Autonomous System Number (ASN) to identify itself

~10,000 multi-homed ASes – networks connected to >=2 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

The routing system is under attack!

MANRS

How big is the problem?

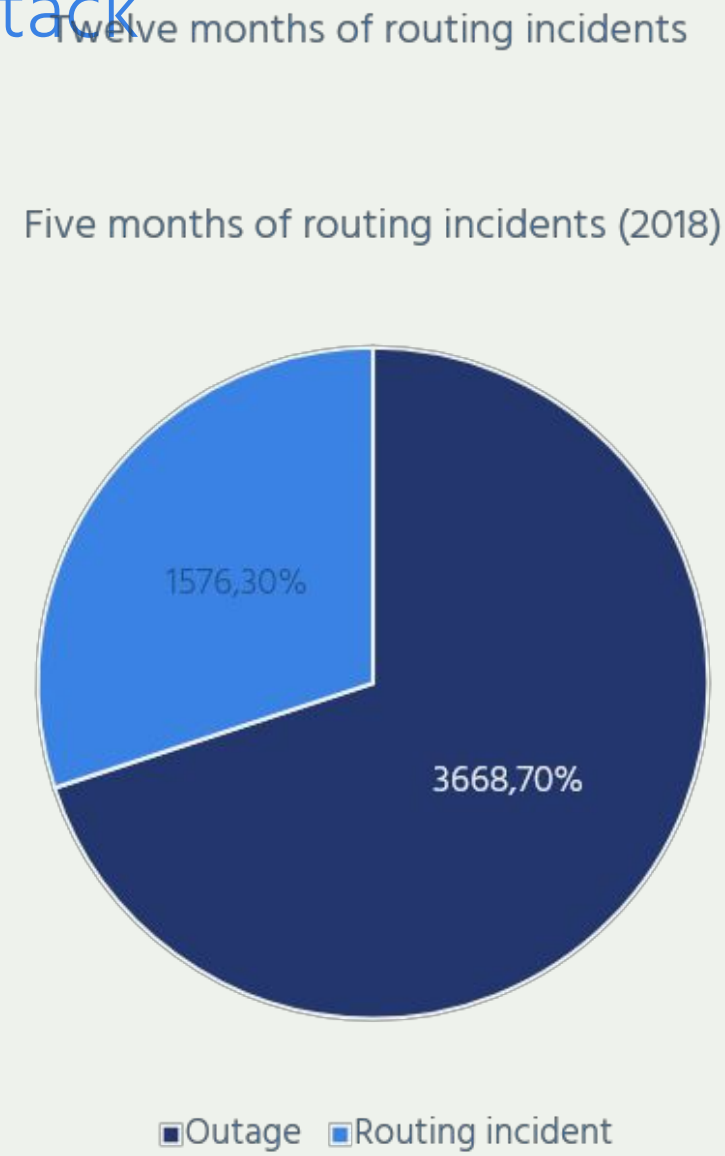
Some Facts & Figures

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.	*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.*
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*

The routing system is constantly under attack

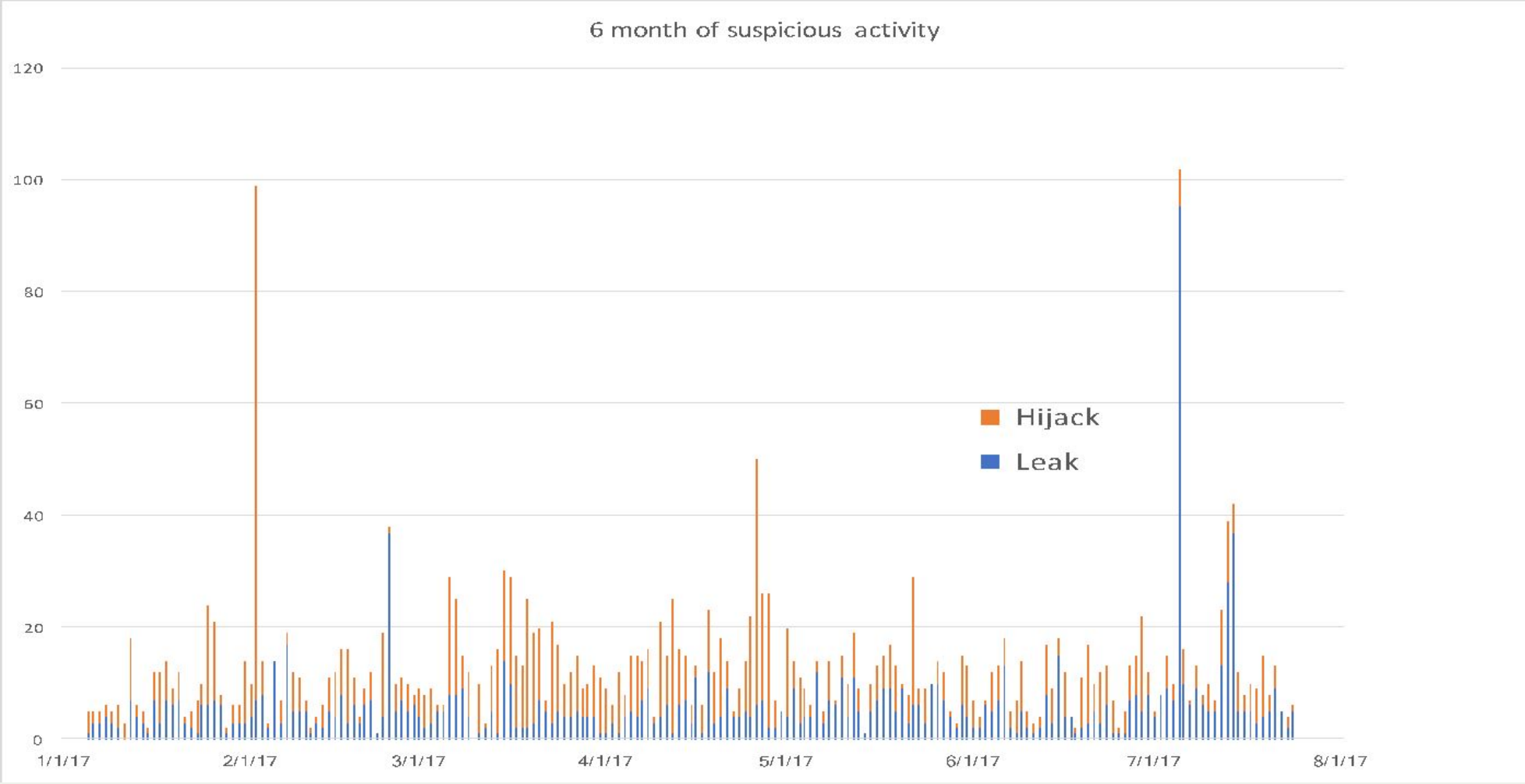
- 13,935 total incidents (either outages or attacks like route leaks and hijacks)
- Over 10% of all Autonomous Systems on the Internet were affected
- 3,106 Autonomous Systems were a victim of at least one routing incident
- 1,546 networks were responsible for 5304 routing incidents
- 547 networks were responsible for 1576 routing incidents



MANRS

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

No Day Without an Incident



http://bgpstream.com/

MANRS

Why it matters for Africa

The evolving landscape

CDN	ASN	NAPAfrica	JINX	IXPN Lagos
Akamai	20940	Yes	No	No
Amazon	16509	No	No	No
Cloudflare	13335	Yes	Yes	Yes
Facebook	32934	Yes	No	Yes
Google	15169	Yes	Yes	Yes
Netflix	2906	Yes	No	No
Twitter	13414	No	No	No

NB: ASNs visible at IXP Route-Servers

- More large CDNs are connected (peering) in Africa – errors can have a global effect - How a Nigerian ISP Accidentally Knocked Google Offline
- Larger percentage of ISP traffic is via IXP;
  - Some ISPs may not have sufficient transit capacity
  - Unnecessary incidents constrain the limited IXP technical support resources
- Overall, incidents affect your customers.

Mutually Agreed Norms for Routing Security (MANRS)

Provides crucial fixes to eliminate the most common threats in the global routing system

Brings together established industry best practices

Based on collaboration among participants and shared responsibility for the Internet infrastructure

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 Participants – as of July 2019

196 Network Operators

322 Autonomous Systems (ASNs)

33 Internet Exchange Points

10 partners (promotion, capacity building etc..)

MANRS Participants in Africa

1775 ASNs assigned to Africa

5 ASNs participating in MANRS for Network Operators

- SEACOM (AS37100) - 4 actions
- WorkOnline (AS37271) - 4 actions
- Orange Morocco (AS36925) - 4 actions
- MORENET (AS327700) - 4 actions
- iWay Africa (AS36915) - 4 actions

2 IXPs participating in MANRS for IXPs

- RINEX
- NAPAfrica

NB: There are a number of ASNs & IXP that are already MANRS conformant though!

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

MANRS

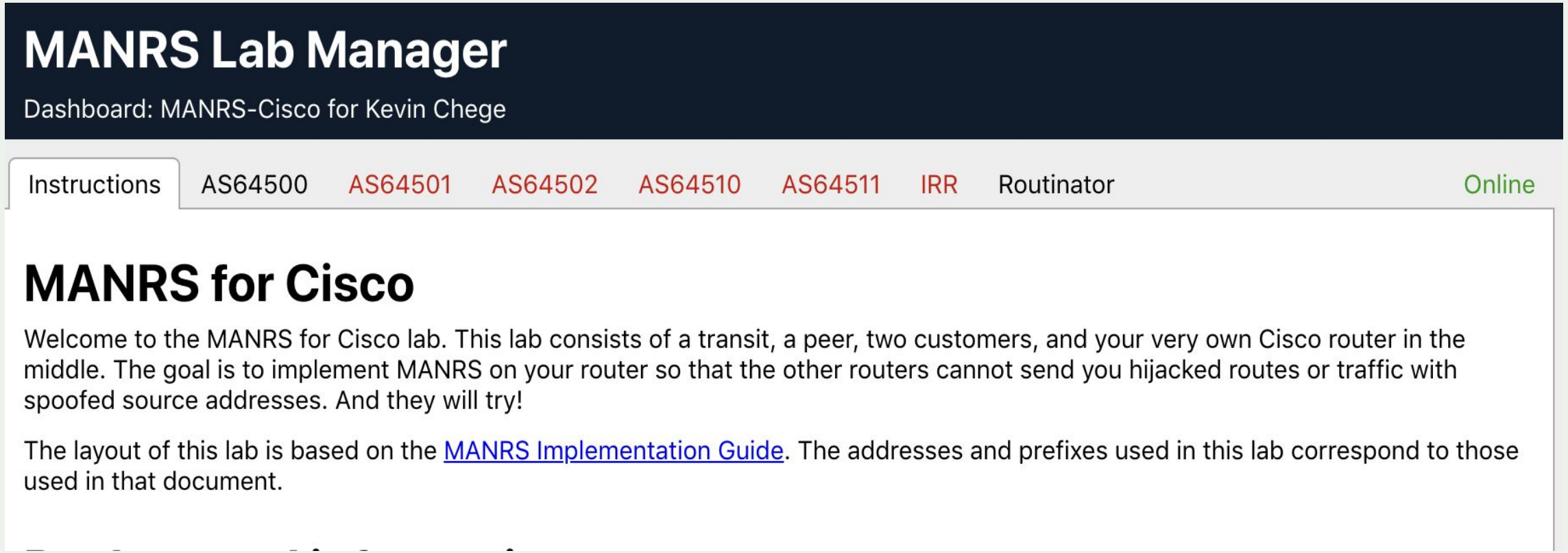
Version 1.0, BCOP series
Publication Date: 25 January 2017

MANRS Online Training

To build skills on filtering, ISOC are developing an online lab that will allow network admins to test filtering techniques in a virtual environment

The lab currently supports the following routing platforms

Cisco
Juniper
Mikrotik



Each trainee will be provided with a topology of 5 routers, and an RPKI validator (RPKI). One of the 5 routers is configurable and the other 4 are sending traffic to it that needs to be filtered

The lab is due for completion in the coming weeks and will be made available to engineers globally. Information will be sent via regional tech mailing lists

MANRS Observatory - https://observatory.manrs.org/

Tool to impartially benchmark ASes to improve reputation and transparency

Provide factual state of security and resilience of Internet routing system over time

Allow MANRS participants to easily check for conformance

Collates publicly available data sources

- BGPStream
- CIDR Report
- CAIDA Spoofer Database
- RIPE Database / Whois
- PeeringDB
- IRRs

MANRS Dashboard

LOGOUT

OVERVIEW HISTORY DETAILS COMPARISON ABOUT

MONTH July 2019

Overview

State of Routing Security

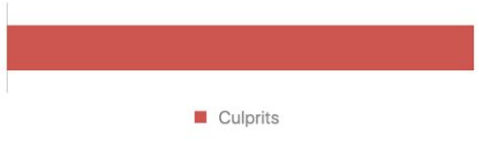
Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

Incidents

Total		
1'663	Route misoriginations	228
	Route leaks	253
	Bogon announcements	1'182

Culprits

Total		
826	Culprits	826

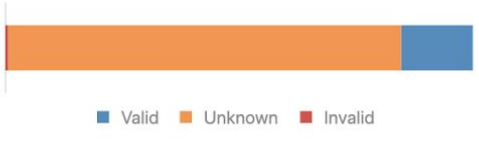


Routing completeness (IRR)

Total		
100%	Unregistered	7%
	Registered	93%

Routing completeness (RPKI)

Total		
100%	Valid	15%
	Unknown	84%
	Invalid	1%



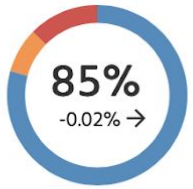
MANRS Readiness

Filtering

Anti-spoofing

Coordination

Global Validation IRR



Global Validation RPKI

Ready Aspiring Lagging

MANRS **Dashboard**

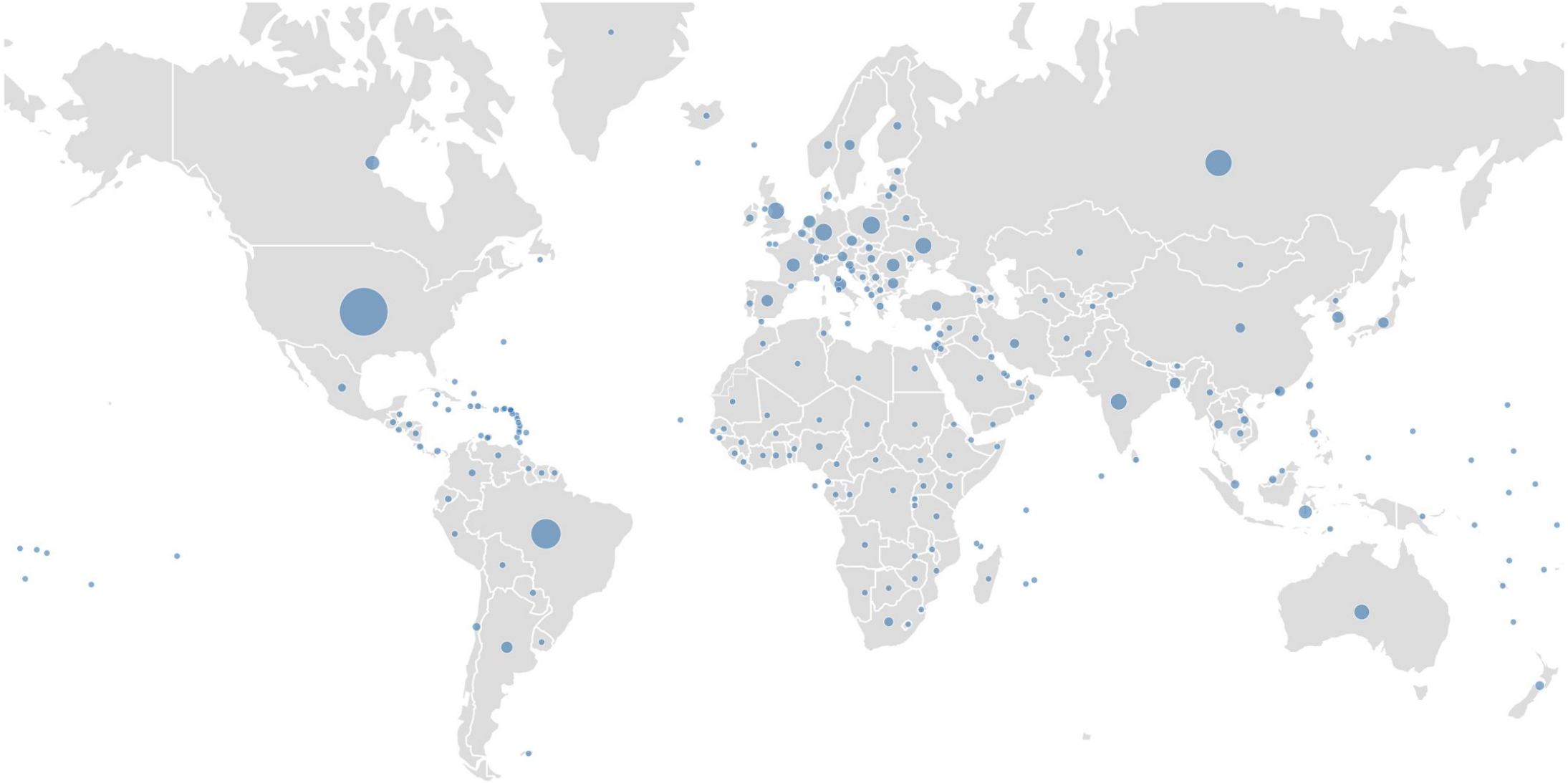
LOGOUT

OVERVIEW | HISTORY | DETAILS | COMPARISON | ABOUT

Global view

Size: **Count** | Incidents | Culprits

Region: **Country** | UN Regions | UN Sub-Regions | RIR Regions



MONTH July 2019 COUNTRY South Africa Botswana Zambia Zimbabwe Namibia Angola Malawi Mozambique Lesotho Eswatini Tanzania, United Republic of

Overview

State of Routing Security

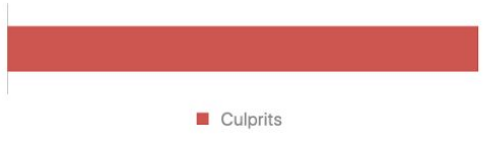
Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

Incidents

Total		
39	Route misoriginations	4
	Route leaks	4
	Bogon announcements	31

Culprits

Total		
18	Culprits	18

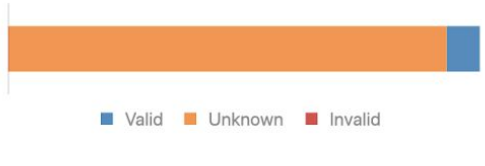


Routing completeness (IRR)

Total		
100%	Unregistered	2%
	Registered	98%

Routing completeness (RPKI)

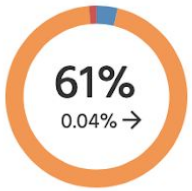
Total		
100%	Valid	7%
	Unknown	93%
	Invalid	0%



MANRS Readiness

Filtering

Anti-spoofing



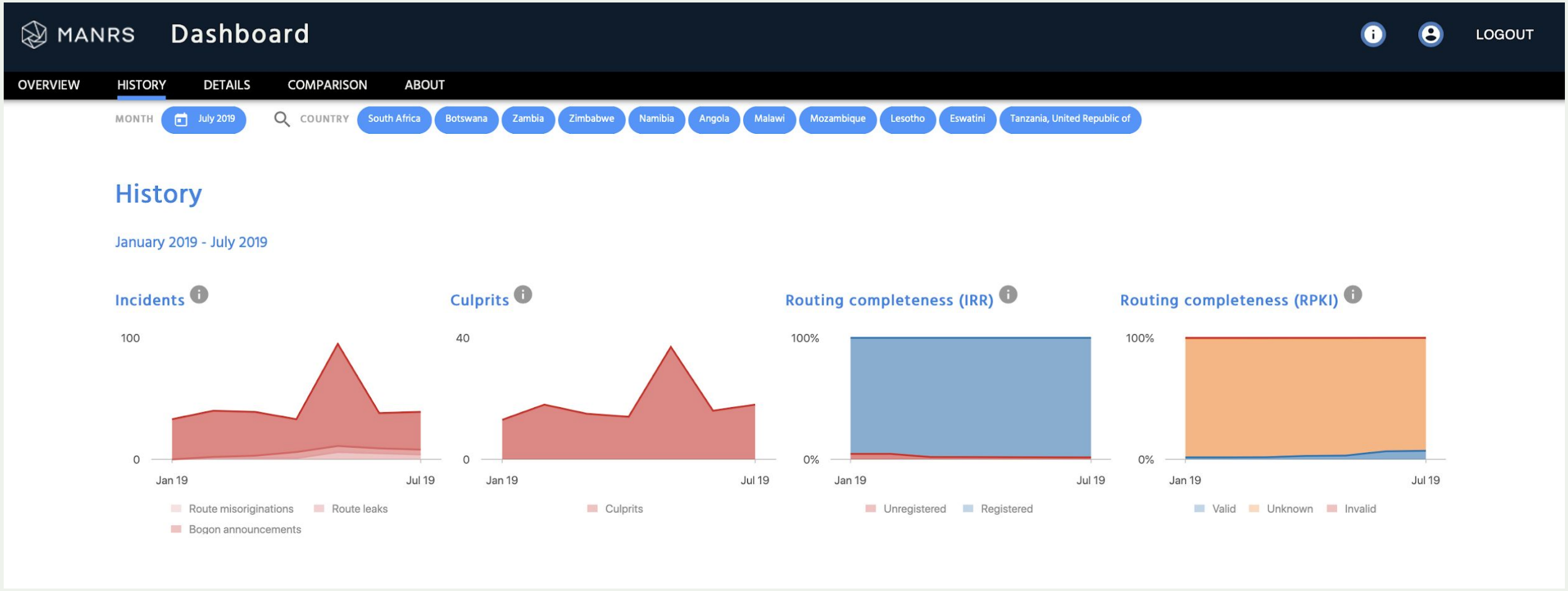
Coordination

Global Validation IRR

Global Validation RPKI

Ready Aspiring Lagging

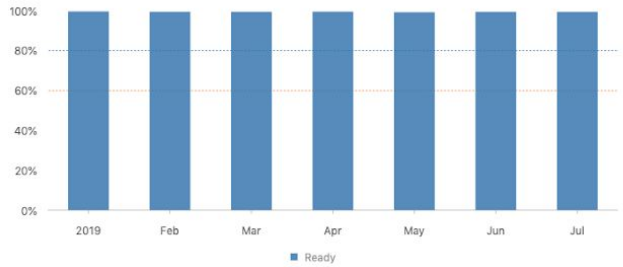
MANRS Observatory



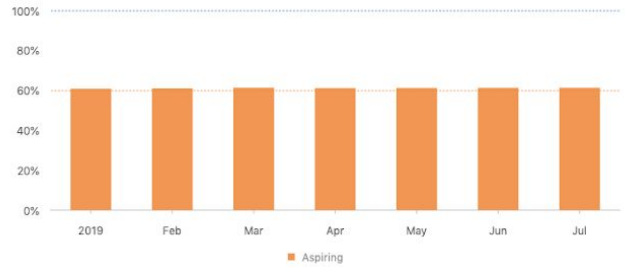
MANRS Readiness

Overall | Metrics

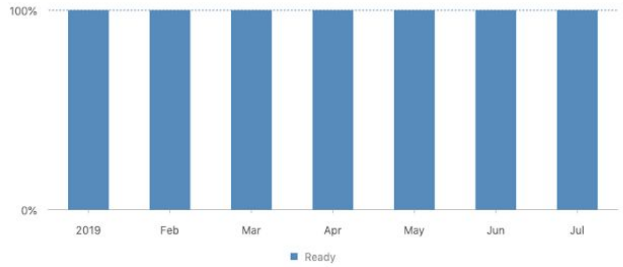
Filtering



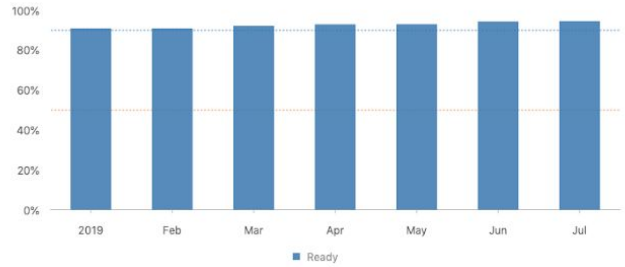
Anti-spoofing



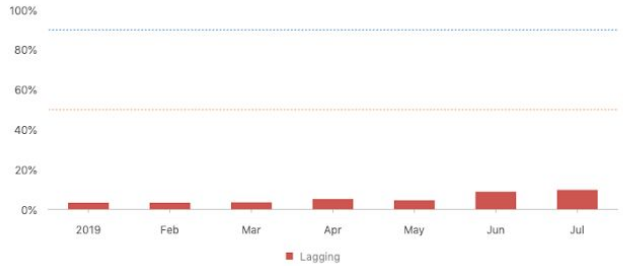
Coordination



Global Validation IRR



Global Validation RPKI



MANRS Dashboard

LOGOUT

OVERVIEW HISTORY DETAILS COMPARISON ABOUT

MONTH July 2019 ASN 2018

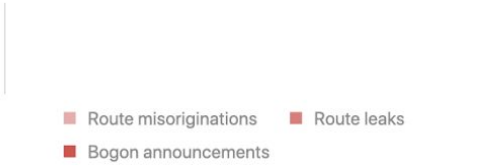
Overview

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		
0	Route misoriginations	0
	Route leaks	0
	Bogon announcements	0



Culprits

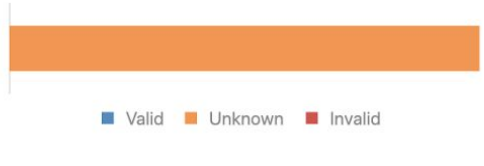
Total		
0	Culprits	0

Routing completeness (IRR)

Total		
100%	Unregistered	0%
	Registered	100%

Routing completeness (RPKI)

Total		
100%	Valid	0%
	Unknown	100%
	Invalid	0%



MANRS Readiness

Filtering

Anti-spoofing

Coordination

Global Validation IRR

Global Validation RPKI

Ready Aspiring Lagging

MANRS Observatory

MANRS Dashboard

LOGOUT

OVERVIEW HISTORY DETAILS COMPARISON ABOUT

Details - ASN 2018

Download data

M1 - Route leak by the AS

Absolute: **0.0** Normalized: **100%** Incident Count: **0**

M2 - Route misorigin by the AS

Absolute: **0.0** Normalized: **100%** Incident Count: **0**

M1C - Route leak by a direct customer

Absolute: **0.0** Normalized: **100%** Incident Count: **0**

M2C - Route hijack by a direct customer

Absolute: **0.0** Normalized: **100%** Incident Count: **0**

M3 - Bogon prefixes announced by the AS

Absolute: **0.0** Normalized: **100%** Incident Count: **0**

M3C - Bogon prefixes propagated by the AS

Absolute: **0.0** Normalized: **100%** Incident Count: **0**

M4 - Bogon ASNs announced by the AS

Absolute: **0.0** Normalized: **100%** Incident Count: **0**

MANRS Dashboard

LOGOUT

OVERVIEW HISTORY DETAILS COMPARISON ABOUT

M5 - Spoofing IP blocks

Absolute: **0.0** Normalized: **100%** Incident Count: **-**

Has records	Spoofed prefixes
True	-

M8 - Contact registration (RIR, IRR, PeeringDB)

Absolute: **0** Normalized: **100%** Incident Count: **-**

Checked on	Has contact info
2019-07-01	True

M7IRR - Registered routes (% of routes registered)

Absolute: **0%** Normalized: **100%** Incident Count: **-**

Number of prefixes	Number of unregistered prefixes	Unregistered prefixes	Checked on
573	0	-	2019-07-01

M7RPKI - Valid ROAs for routes (% of routes registered)

Absolute: **100%** Normalized: **0%** Incident Count: **-**

Number of prefixes	Number of unknown prefixes	Checked on
330	330	2019-07-01

M7RPKIN - Invalid routes

Absolute: **0%** Normalized: **100%** Incident Count: **-**

MANRS Observatory Access

Launched on 13th August 2019 -

Current access policy:

- Public will be able to view Overall, Regional and Nationally aggregated data
- Only MANRS Participants will have access to detailed data about their network

Caveats:

- Still some false positives
- There are sometimes good reasons for non-100% conformancy
- BUT, this is all inherently public data anyway!

MANRS IXP Programme

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.

Is the problem getting better or worse?

MANRS Community

MANRS needs to be community driven

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

- Internet operators undertaking MANRS principles need to encourage use of best practices
- MANRS needs to be driven by leaders within their communities who strongly believe that routing security is an essential component for the future well being of the Internet
- Need feedback and recommendations for improving MANRS principles and best practices, e.g. MANRS Actions, MANRS Observatory, MANRS Implementation Guides, and training materials
- Internet Society can help with presentations, informational materials and merchandise (shirts and stickers)

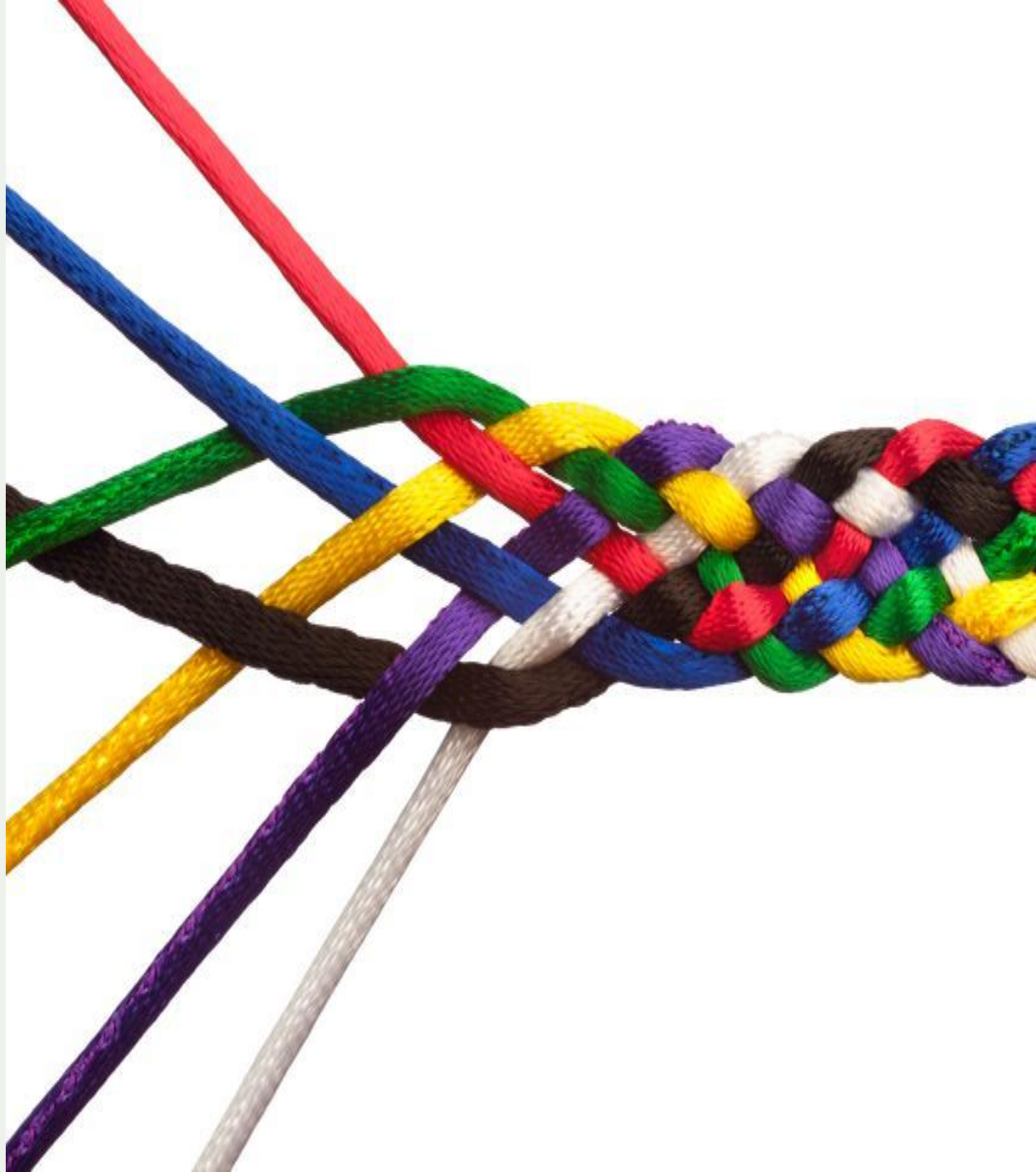
Join Us

Visit https://www.manrs.org

- Fill out the sign up form with as much detail as possible.

Get Involved in the Community

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



MANRS

Thank you.

Michuki Mwangi
mwangi@isoc.org

Visit us at
www.internetsociety.org
Follow us
@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