

1 September 2019
RONOG 6

Mutually Agreed Norms for Routing Security

Observing Your MANRS




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

Background

There are 65,203 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!



How big is the problem?

Some Facts & Figures

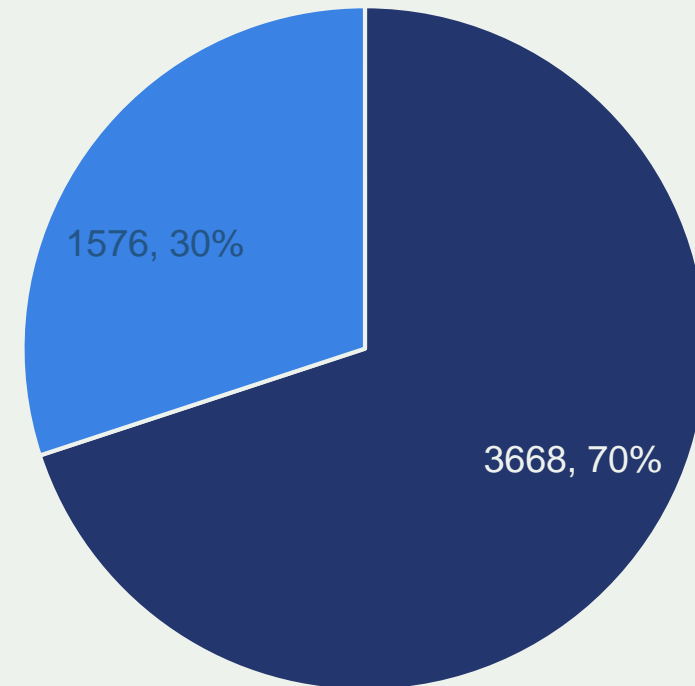
Routing Incidents Cause Real World Problems

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.	<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>June 2019. Verizon accepted incorrect routes from DQE Communications that diverted traffic destined for Cloudflare, Facebook & Amazon.</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>

The routing system is constantly under attack

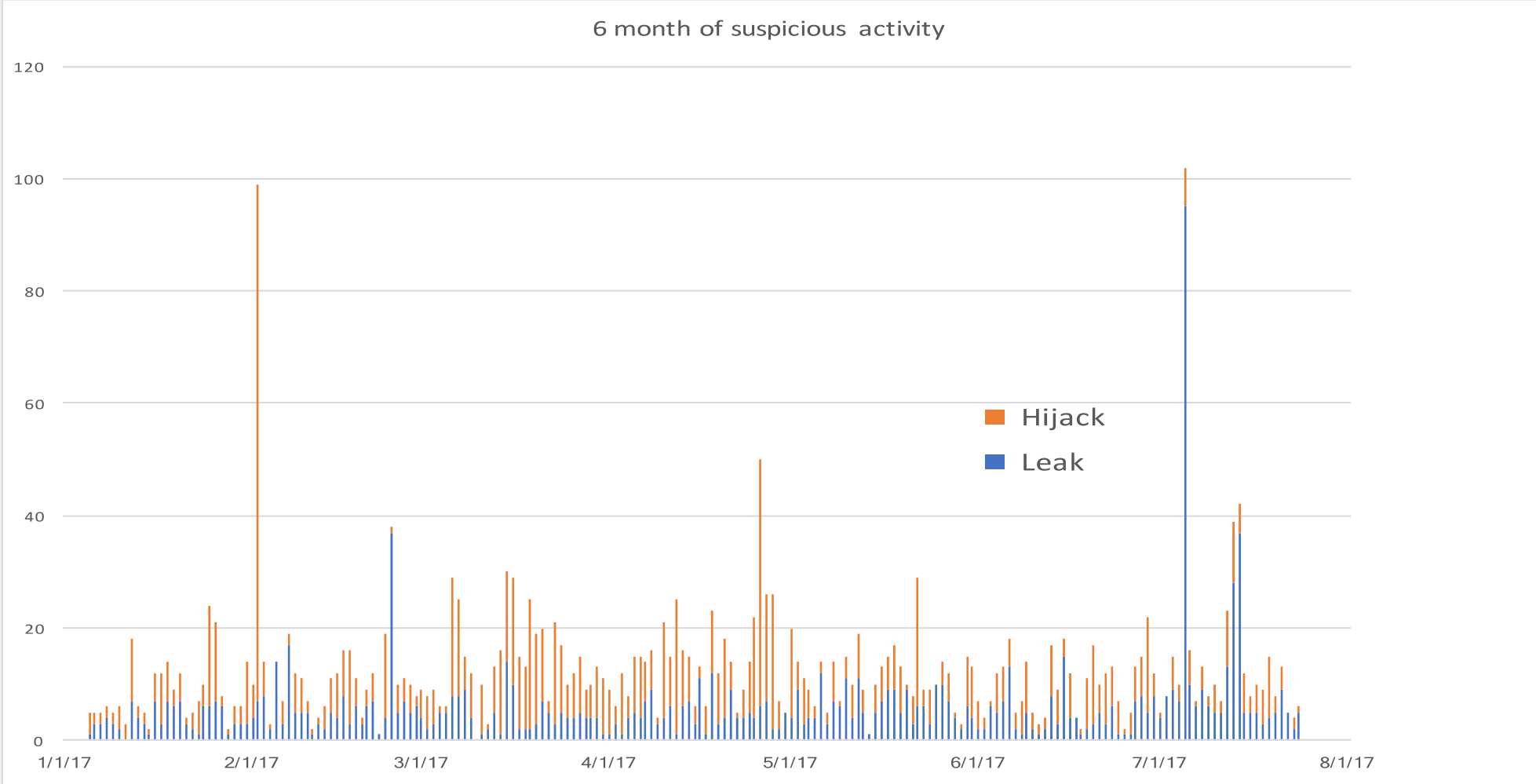
- 13,935 total incidents (either outages or attacks like route leaks and hijacks)
- Over 10% of all Autonomous Systems on the Internet were affected
- 3,106 Autonomous Systems were a victim of at least one routing incident
- **1,546 networks were responsible for 5304 routing incidents**
- **547 networks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

Five months of routing incidents (2018)



■ Outage ■ Routing incident

No Day Without an Incident



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

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

MANRS Participants – as of September 2019

213 Network Operators

341 Autonomous Systems (ASNs)

40 Internet Exchange Points

10 partners (promotion, capacity building etc..)

MANRS Participants in Romania



1,299 ASNs advertised in Romania

0 ASNs participating in MANRS!

Many Romanian ASNs appear MANRS conformant though!

How to Implement MANRS

Documentation & 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



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 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 / RIPE Stats
- PeeringDB
- IRRs
- RPKI Validator

MONTH August 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 i

Total	1'815
Route misoriginations	257
Route leaks	250
Bogon announcements	1'308



Culprits i

Total	883
Culprits	883



Routing completeness (IRR) i

Total	100%
Unregistered	7%
Registered	93%



Routing completeness (RPKI) i

Total	100%
Valid	16%
Unknown	83%
Invalid	1%



MANRS Readiness i

Filtering i



Anti-spoofing i



Coordination i



Global Validation IRR i



Global Validation RPKI i



Ready Aspiring Lagging

MANRS Readiness ⁱ

Filtering ⁱ



Anti-spoofing ⁱ



Coordination ⁱ



Global Validation IRR ⁱ



Global Validation RPKI ⁱ



● Ready ● Aspiring ● Lagging

Global view

Size: [Count](#) | [Incidents](#) | [Culprits](#) Region: [Country](#) | [UN Regions](#) | [UN Sub-Regions](#) | [RIR Regions](#)



MONTH August 2019

COUNTRY Romania

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

Total	8
Route misoriginations	3
Route leaks	0
Bogon announcements	5



Culprits ⁱ

Total	5
Culprits	5



Routing completeness (IRR) ⁱ

Total	100%
Unregistered	2%
Registered	98%



Routing completeness (RPKI) ⁱ

Total	100%
Valid	18%
Unknown	82%
Invalid	0%



MANRS Readiness ⁱ

Filtering ⁱ



Anti-spoofing ⁱ



Coordination ⁱ



Global Validation IRR ⁱ



Global Validation RPKI ⁱ



Ready Aspiring Lagging

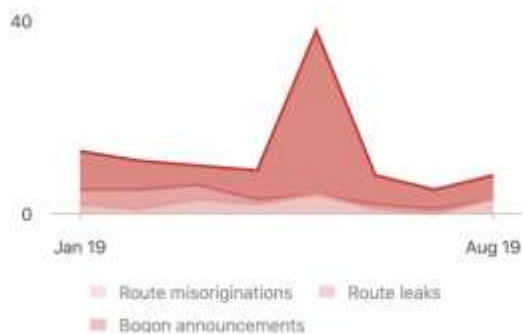
MONTH August 2019

COUNTRY Romania

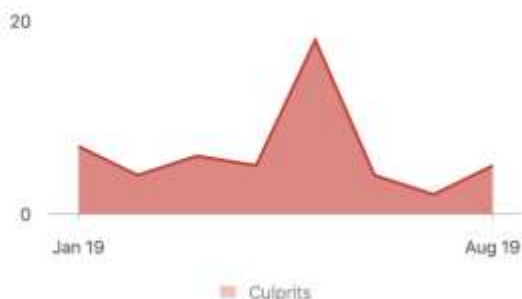
History

January 2019 - August 2019

Incidents i



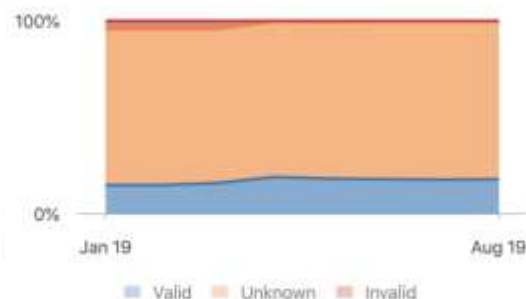
Culprits i



Routing completeness (IRR) i



Routing completeness (RPKI) i



MANRS Readiness i

Absolute | Relative

Filtering i



Anti-spoofing i





Coordination i



Global Validation IRR i



Global Validation RPKI i



MONTH August 2019 ASN 2614

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

- Route misoriginations
- Route leaks
- Bogon announcements

Culprits

Total	0
Culprits	0

- Culprits

Routing completeness (IRR)

Total	100%
Unregistered	1%
Registered	99%

- Unregistered
- Registered

Routing completeness (RPKI)

Total	100%
Valid	13%
Unknown	87%
Invalid	0%

- Valid
- Unknown
- Invalid

MANRS Readiness

Filtering



Anti-spoofing



Coordination



Global Validation IRR



Global Validation RPKI



- Ready
- Aspiring
- Lagging

MONTH August 2019 ASN 2614

Details - ASN 2614

[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



M5 - Spoofing IP blocks

Absolute: 0.5 Normalized: 60% Incident Count: -

Has records	Spoofed prefixes
False	-

M8 - Contact registration (RIR, IRR, PeeringDB)

Absolute: 0 Normalized: 100% Incident Count: -

Checked on	Has contact info
2019-08-01	True

M7IRR - Registered routes (% of routes registered)

Absolute: 1% Normalized: 99% Incident Count: -

Number of prefixes	Number of unregistered prefixes	Unregistered prefixes	Checked on
73	1	194302.34.0/24	2019-08-01

M7RPK1 - Valid RDAs for routes (% of routes registered)

Absolute: 87% Normalized: 13% Incident Count: -

Number of prefixes	Number of unknown prefixes	Checked on
68	59	2019-08-01

M7RPKIN - Invalid routes

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

Number of prefixes	Number of invalid prefixes	Invalid prefixes
68	0	-

MANRS Observatory Access

Publicly launched in August 2019 with MANRS Participants only

Current access policy:

Public are able to view Overall, Regional and Economy aggregated data

Only MANRS Participants have access to detailed data about their network

Caveats:

Still some false positives

There are sometimes good reasons for non-100% conformance

BUT, this is all inherently public data anyway!

MANRS Community



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 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)



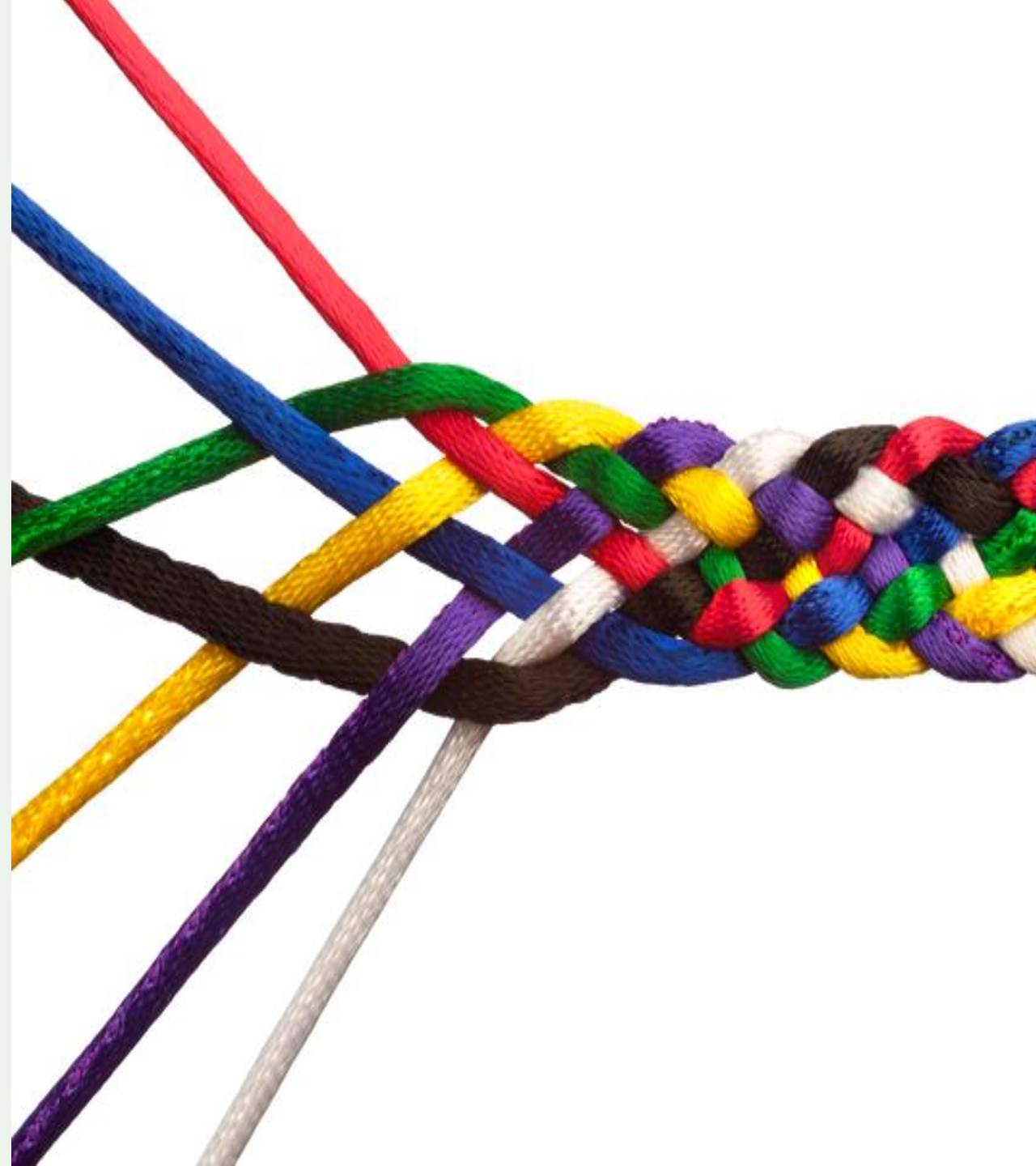
Join Us

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



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