Better routing security through concerted action

Aftab Siddiqui

siddiqui@isoc.org

BGP is the glue that makes the Internet work.

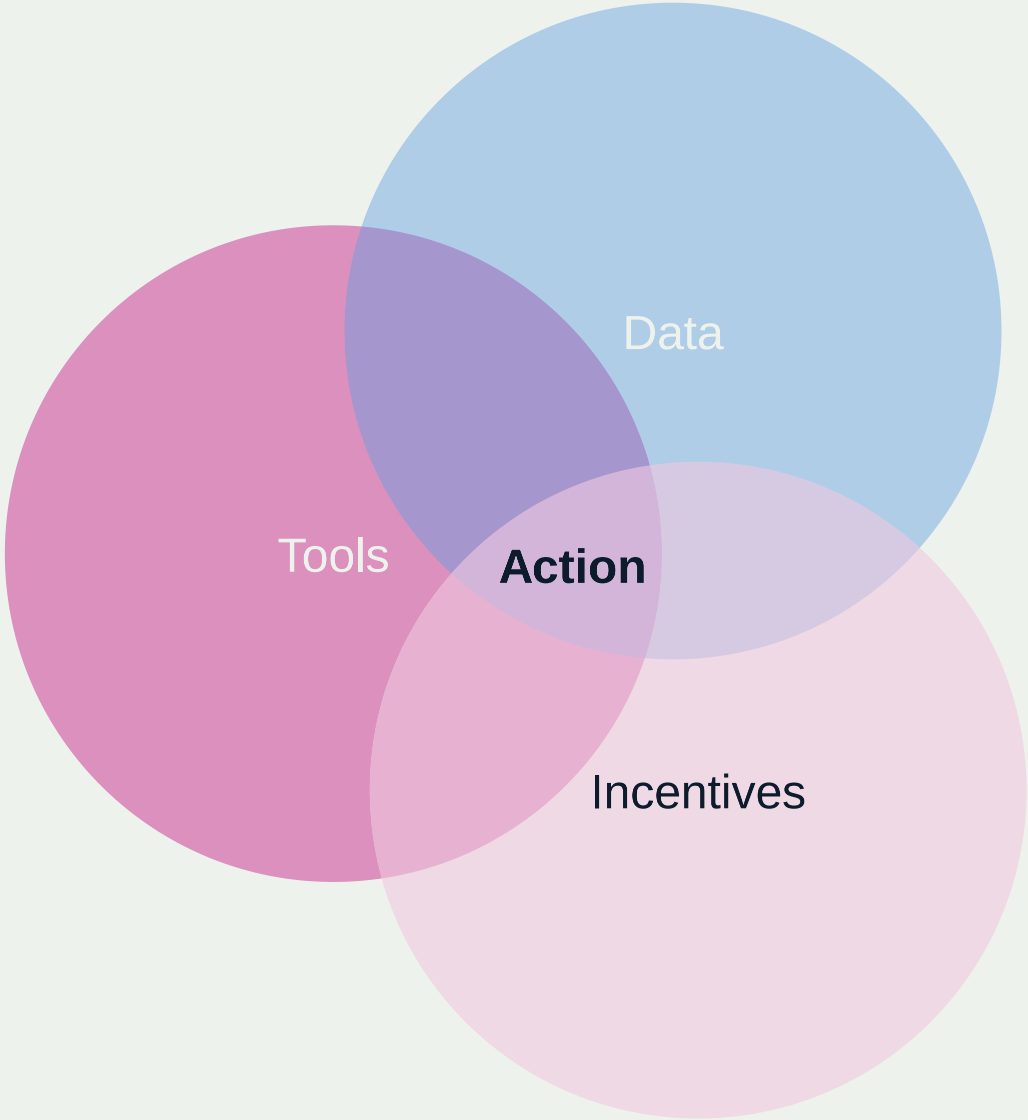
BGP – 30 years in the making

- BGP was designed when the Internet was made up of a smaller number of ASes with strong social and institutional incentives to cooperate
- BGP is still based on “Trust” and chain of trust spans continents
- With the Internet’s commercialization and global adoption, BGP poses greater risks of routing incidents caused by mistaken configurations or by deliberate attacks
- Several attempts have been made to standardise how to implement some security features in BGP e.g. **BGP Operations and Security – RFC7454**

BGP – 30 years in the making

- **Issues we are dealing with today**
- BGP Hijacks/Prefix Hijacks
- BGP Leaks/Route Leaks (RFC7908)
- Bogon Announcements (IPv4/v6, ASN)
- Global Validation

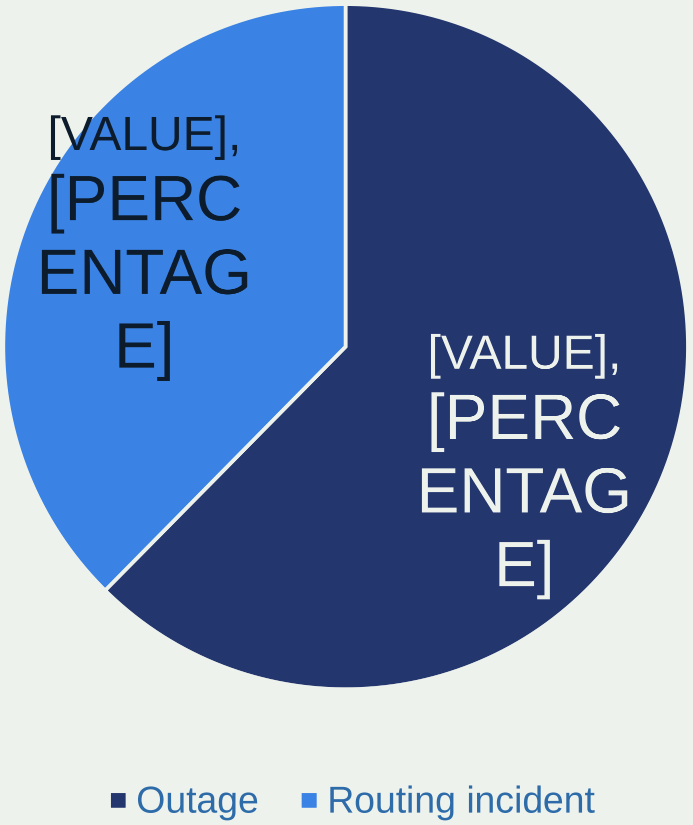
BGP is unsecure – what’s missing?



There is a problem

- 12,600 total incidents (either outages or attacks, like route leaks and hijacks)
- About 4.4% of all Autonomous Systems on the Internet were affected
- 2,737 Autonomous Systems were a victim of at least one routing incident
- 1,294 networks were responsible for 4739 routing incidents

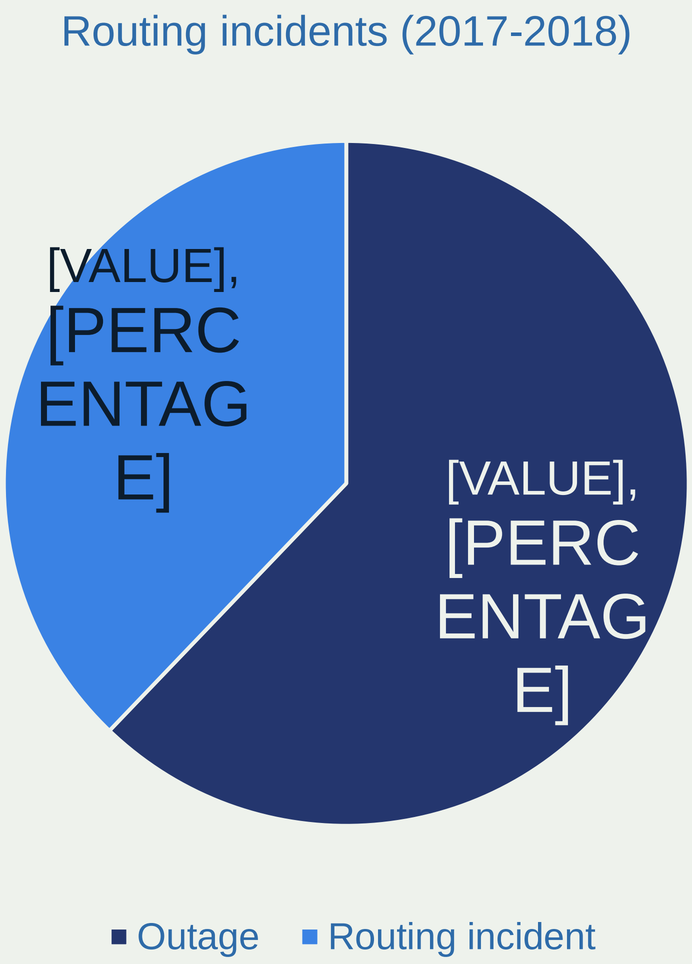
Twelve months of routing incidents (2018)



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

There is a problem (comp. 2017)

- 12,600 (↓9.6%) total incidents (either outages or attacks, like route leaks and hijacks)
- About 4.4% (↓1%) of all Autonomous Systems on the Internet were affected
- 2,737 (↓12%) Autonomous Systems were a victim of at least one routing incident
- 1,294 (↓17%) networks were responsible for 4739 routing incidents



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

2 years in review (2017, 2018)

Statistics of routing incidents generated from BGPStream data

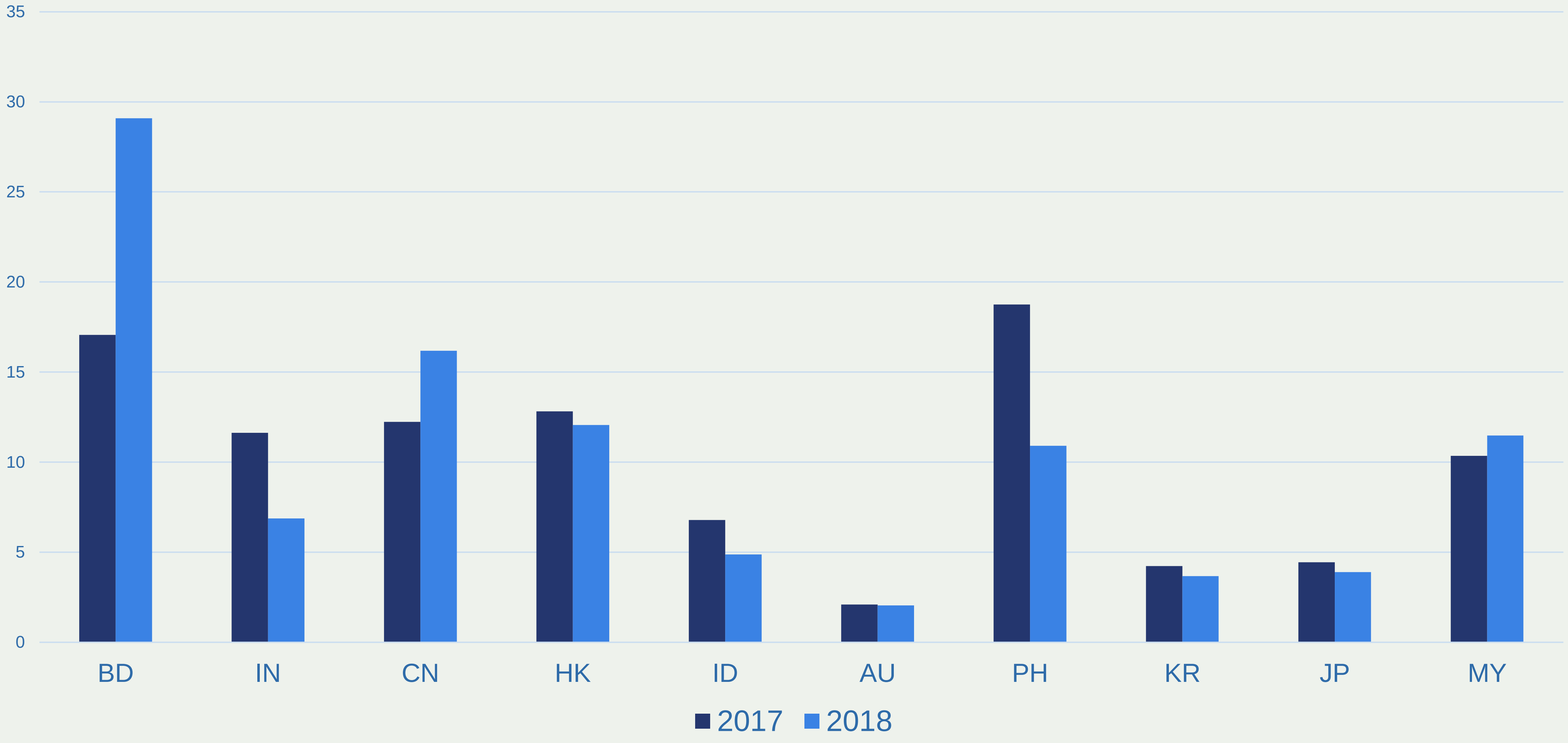
Caveats:

- Sometimes it is impossible to distinguish an attack from a legitimate (or consented) routing change
- CC attribution is based on geolocation MaxMind's GeoLite City data set

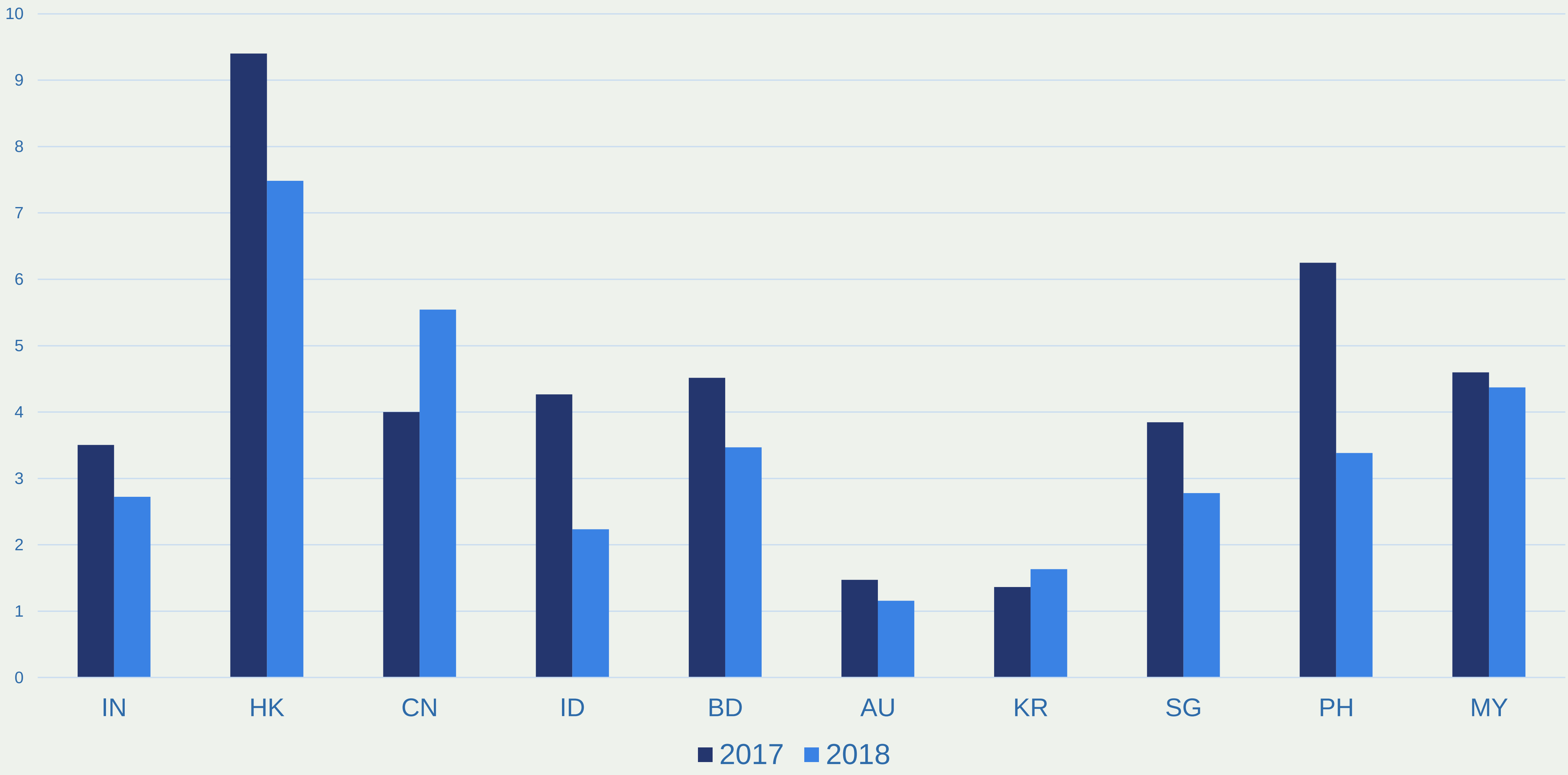
But:

- Using the same methodology we should get a pretty accurate picture of the dynamics

Potential victims: 2017 ➡ 2018



Culprits: Positive dynamics



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

Network operators

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

IXPs

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.

Content (work in progress)

Action 1

Prevent propagation of incorrect routing information

Action 2

Prevent traffic with spoofed source IP addresses

Action 3

Facilitate global operational communication and coordination

Action 4

Facilitate validation of routing information on a global scale

Action 5

Promote MANRS

Action 6

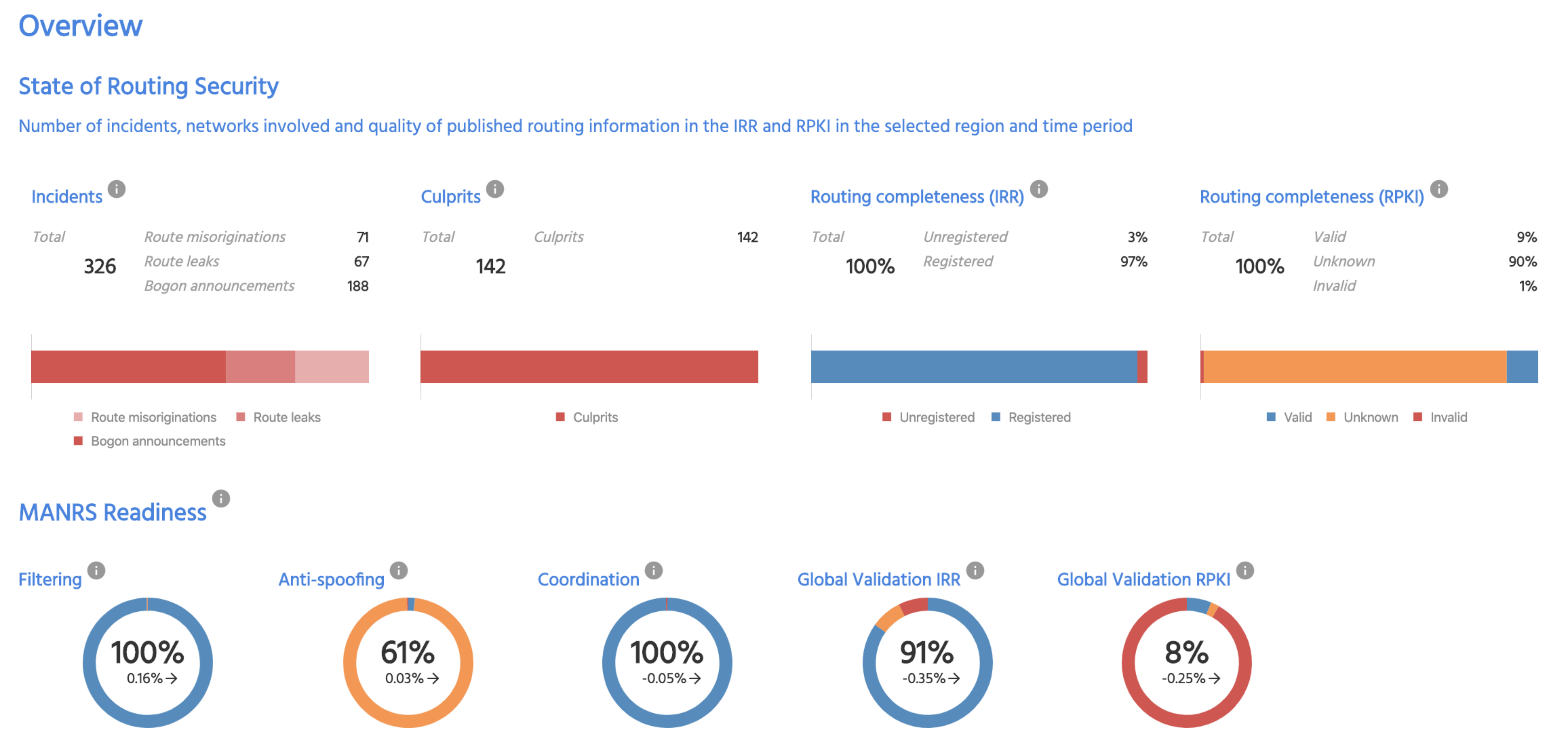
Provide monitoring and debugging tools to peering partners

Can we track these data long term?

MANRS Observatory & Member Reports

- Longitudinal measurements of how routing security evolves
- MANRS as a reference point - ”MANRS Readiness”
- Inform the members of their readiness
- Improve transparency and credibility of the effort

State of routing security: APNIC region, May 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		
326	*Route misoriginations*	71
	Route leaks	67
	Bogon announcements	188

■ Route misoriginations ■ Route leaks
■ Bogon announcements

Culprits

Total		
142	*Culprits*	142

■ Culprits

Routing completeness (IRR)

Total		
100%	*Unregistered*	3%
	Registered	97%

■ Unregistered ■ Registered

Routing completeness (RPKI)

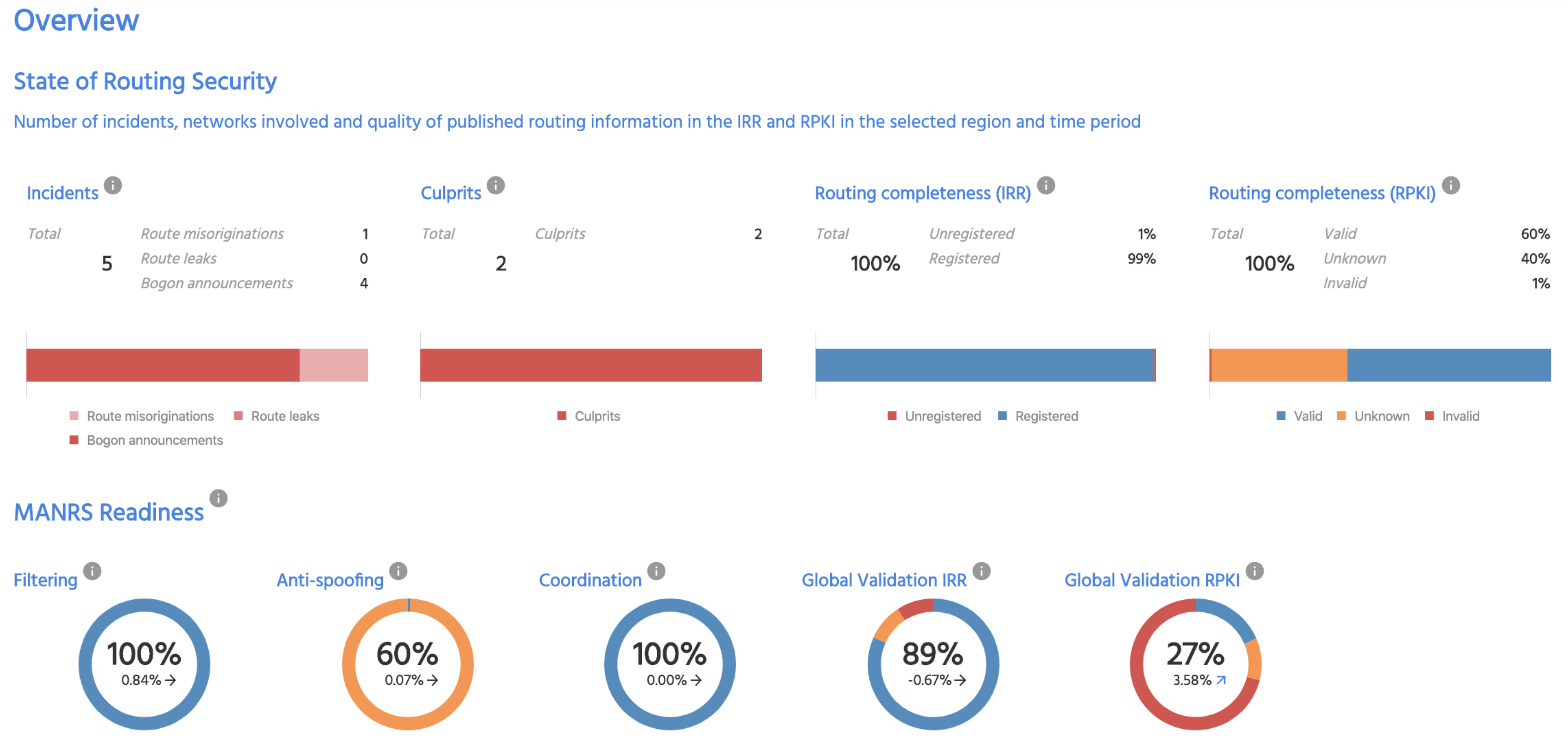
Total		
100%	*Valid*	9%
	Unknown	90%
	Invalid	1%

■ Valid ■ Unknown ■ Invalid

MANRS Readiness

Filtering	Anti-spoofing	Coordination	Global Validation IRR	Global Validation RPKI
100% 0.16% →	61% 0.03% →	100% -0.05% →	91% -0.35% →	8% -0.25% →

State of routing security: Taiwan, May 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		
5	*Route misoriginations*	1
	Route leaks	0
	Bogon announcements	4

🟥 Route misoriginations 🟥 Route leaks 🟥 Bogon announcements

Culprits

Total		
2	*Culprits*	2

🟥 Culprits

Routing completeness (IRR)

Total		
100%	*Unregistered*	1%
	Registered	99%

🟥 Unregistered 🟦 Registered

Routing completeness (RPKI)

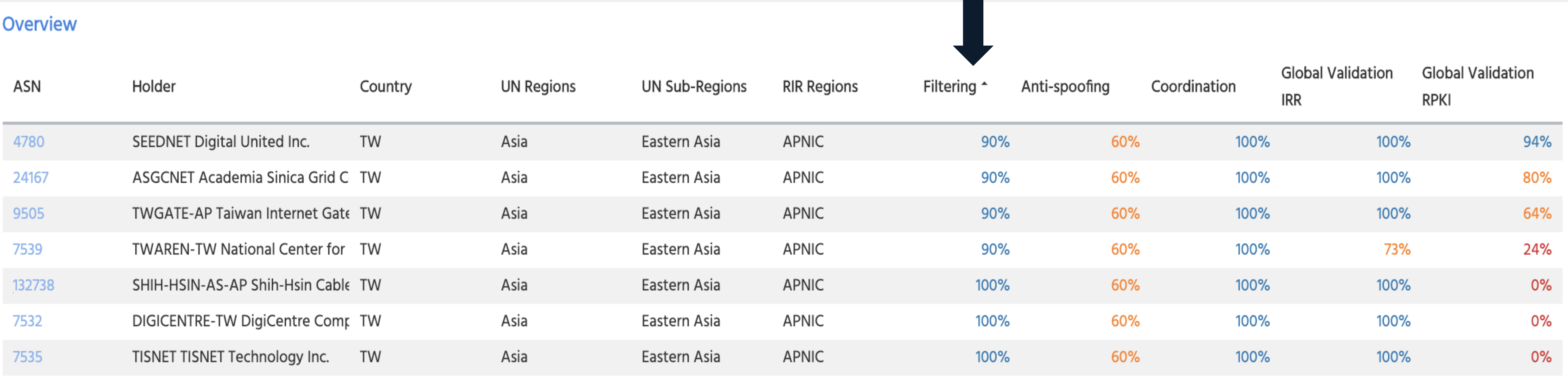
Total		
100%	*Valid*	60%
	Unknown	40%
	Invalid	1%

🟦 Valid 🟧 Unknown 🟥 Invalid

MANRS Readiness

Filtering	Anti-spoofing	Coordination	Global Validation IRR	Global Validation RPKI
100% 0.84% →	60% 0.07% →	100% 0.00% →	89% -0.67% →	27% 3.58% ↗

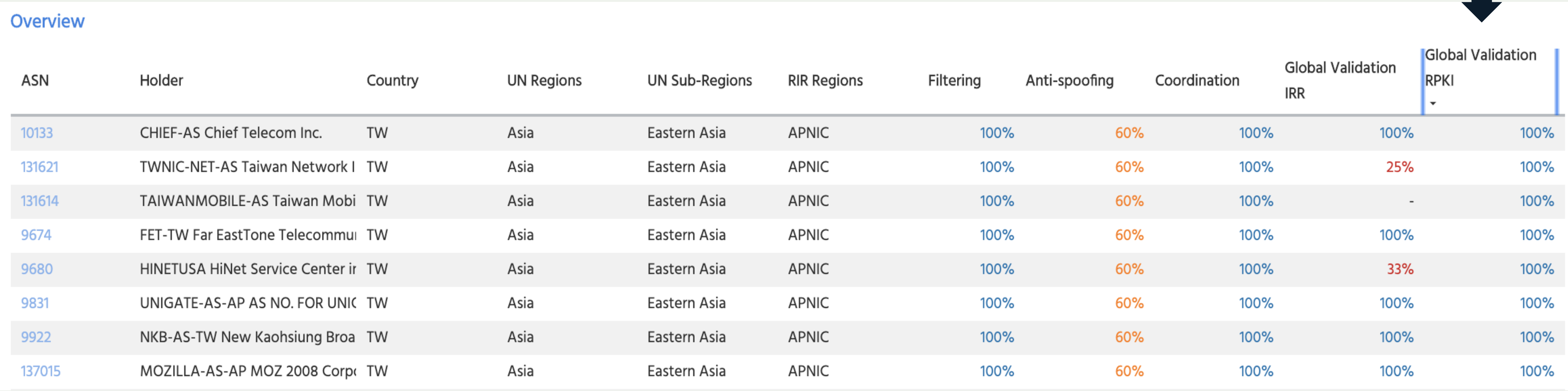
State of routing security: Taiwan, May 2019



Overview

ASN	Holder	Country	UN Regions	UN Sub-Regions	RIR Regions	Filtering ▲	Anti-spoofing	Coordination	Global Validation IRR	Global Validation RPKI
4780	SEEDNET Digital United Inc.	TW	Asia	Eastern Asia	APNIC	90%	60%	100%	100%	94%
24167	ASGCNET Academia Sinica Grid C	TW	Asia	Eastern Asia	APNIC	90%	60%	100%	100%	80%
9505	TWGATE-AP Taiwan Internet Gate	TW	Asia	Eastern Asia	APNIC	90%	60%	100%	100%	64%
7539	TWAREN-TW National Center for	TW	Asia	Eastern Asia	APNIC	90%	60%	100%	73%	24%
132738	SHIH-HSIN-AS-AP Shih-Hsin Cable	TW	Asia	Eastern Asia	APNIC	100%	60%	100%	100%	0%
7532	DIGICENTRE-TW DigiCentre Comp	TW	Asia	Eastern Asia	APNIC	100%	60%	100%	100%	0%
7535	TISNET TISNET Technology Inc.	TW	Asia	Eastern Asia	APNIC	100%	60%	100%	100%	0%

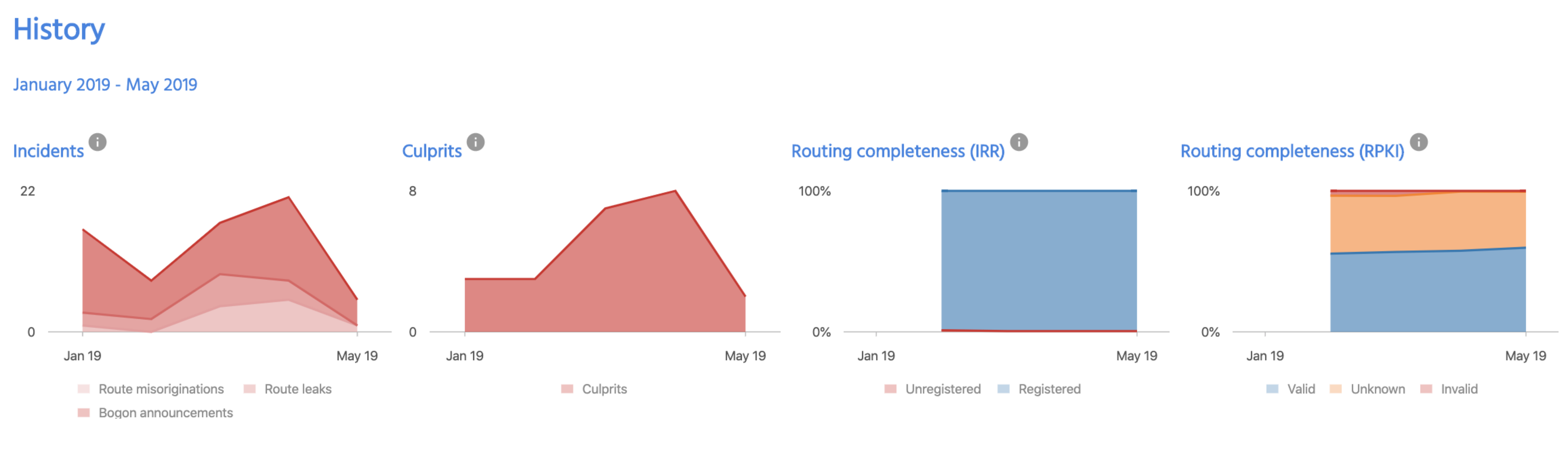
State of routing security: Taiwan, May 2019



Overview

ASN	Holder	Country	UN Regions	UN Sub-Regions	RIR Regions	Filtering	Anti-spoofing	Coordination	Global Validation IRR	Global Validation RPKI
10133	CHIEF-AS Chief Telecom Inc.	TW	Asia	Eastern Asia	APNIC	100%	60%	100%	100%	100%
131621	TWNIC-NET-AS Taiwan Network I	TW	Asia	Eastern Asia	APNIC	100%	60%	100%	25%	100%
131614	TAIWANMOBILE-AS Taiwan Mobi	TW	Asia	Eastern Asia	APNIC	100%	60%	100%	-	100%
9674	FET-TW Far EastTone Telecommu	TW	Asia	Eastern Asia	APNIC	100%	60%	100%	100%	100%
9680	HINETUSA HiNet Service Center ir	TW	Asia	Eastern Asia	APNIC	100%	60%	100%	33%	100%
9831	UNIGATE-AS-AP AS NO. FOR UNI(	TW	Asia	Eastern Asia	APNIC	100%	60%	100%	100%	100%
9922	NKB-AS-TW New Kaohsiung Broa	TW	Asia	Eastern Asia	APNIC	100%	60%	100%	100%	100%
137015	MOZILLA-AS-AP MOZ 2008 Corp(	TW	Asia	Eastern Asia	APNIC	100%	60%	100%	100%	100%

Evolution: January 2019 - May 2019



History

January 2019 - May 2019

Network Operators from Thailand

Organization	Service Area	ASNs	Action 1: Filtering	Action 2: Anti Spoofing	Action 3: Coordination	Action 4: Global Validation
Taiwan Computer Emergency Response Team / Coordination Center	TW	131621	✔□	✔□	✔□	✔□

Internet Exchange Points from Taiwan

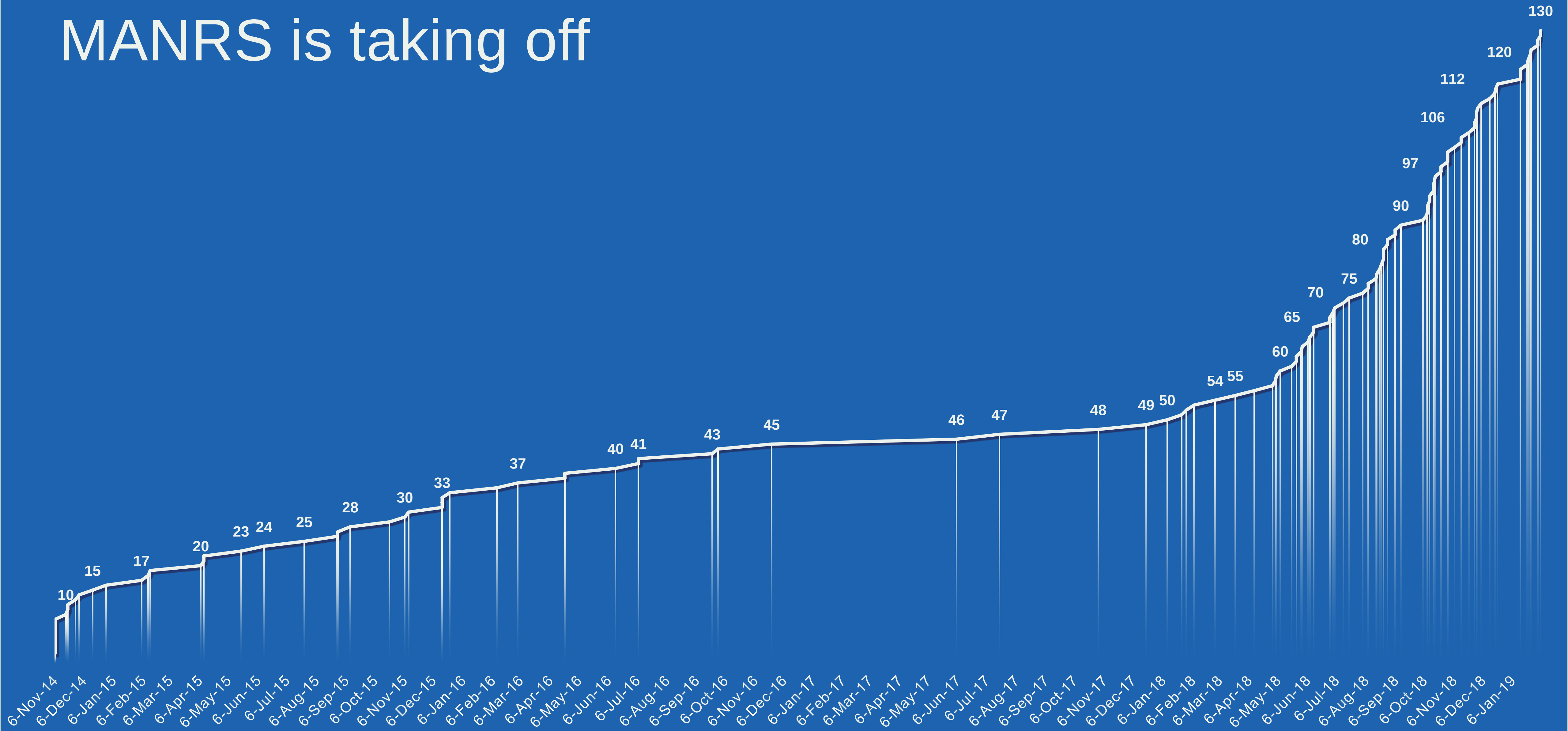
Organization	Service Area	Action 1: Prevent	Action 2: Promote	Action 3: Protect	Action 4: Coordinate	Action5: Tools

☹ □

Why join MANRS?

- Improve your security posture and reduce the number and impact of routing incidents
- Demonstrate that these practices are reality
- Join a community of security-minded operators working together to make the Internet better
- Use MANRS as a competitive differentiator

MANRS is taking off



only together, we can

manrs.org

#ProtectTheCore

MANRS Video:
https://www.youtube.com/embed/nJINk5p-HEE