



**RIPE NCC**

RIPE NETWORK COORDINATION CENTRE

# Internet Data Analysis with RIPE RIS

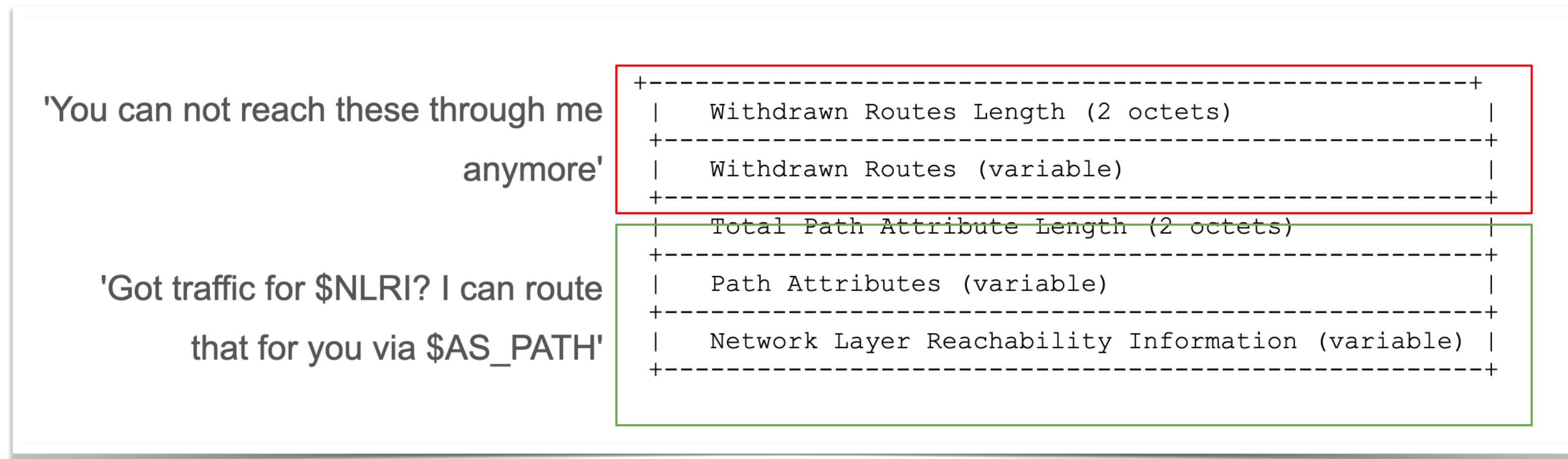
Advanced Topics

Emile Aben | 2022 | TMA PhD School

# BGP Packet Formats



- BGP Open. Initial session setup. Parameter negotiation
  - MRT data contains STATE messages (state 6 = ESTABLISHED )
- BGP Update



# BGP Info Normalisation



- 1 BGP packet format contains many “state changes”
- For analysis: Process one “state change” at a time

`./bgpdump <file>`

```
TIME: 02/23/08 12:50:00
TYPE: BGP4MP/MESSAGE/Update
FROM: 213.179.39.65 AS16186
TO: 193.0.4.28 AS12654
WITHDRAW
 192.23.187.0/24
 213.42.0.0/17
 195.229.128.0/17
 195.229.0.0/17
```

vs.

`./bgpdump -m <file>`

```
BGP4MP|1203771000|W|213.179.39.65|16186|192.23.187.0/24
BGP4MP|1203771000|W|213.179.39.65|16186|213.42.0.0/17
BGP4MP|1203771000|W|213.179.39.65|16186|195.229.128.0/17
BGP4MP|1203771000|W|213.179.39.65|16186|195.229.0.0/17
```

- “No flags” format will tell you about uncommon attributes

# AS Path Surprises



- Sequence of same ASN: Traffic Engineering/“prepending”

```
91.205.158.0/24 2497 174 62206 56399 207313 207313
91.205.158.0/24 25152 6939 56399 207313 207313
91.205.158.0/24 4777 2516 174 62206 56399 207313 207313
```

```
4777 6939 23947 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004
25152 6939 23947 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004
```

- AS Path poisoning: Paths ends with: ASx ASy (..) ASx

```
25152 6939 1273 15924 44327 16010 44327
4777 2516 1273 15924 44327 16010 44327
```

- Config typo: Prepend config differs on different platforms

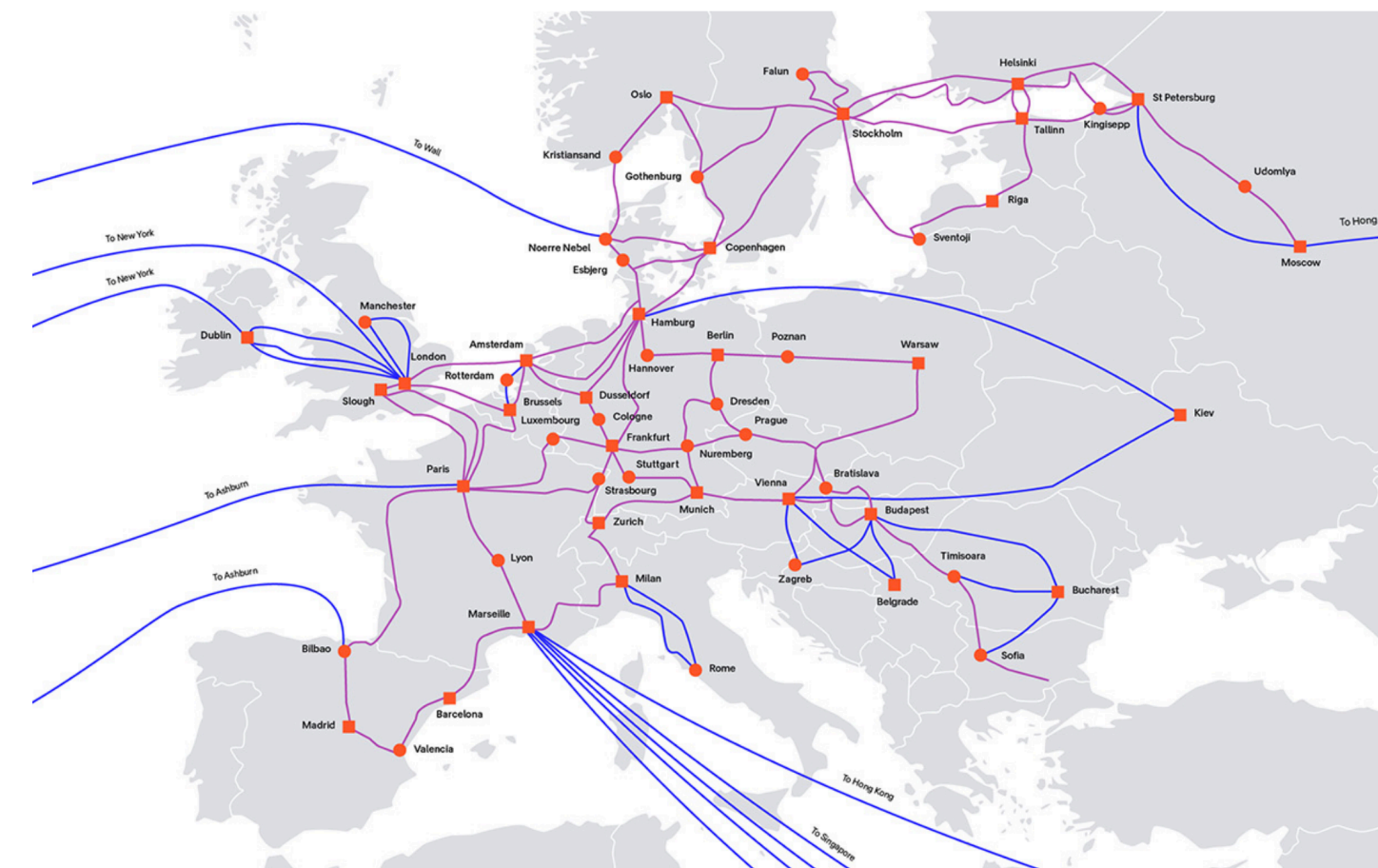
```
45.82.88.0/22 2497 3356 8400 25144
45.82.88.0/22 25152 2914 3356 8400 25144
45.82.88.0/22 4777 6939 5391 25144 2
```

- Deliberate attempts to misguide (hijacks)

# BGP And Geography



- It's complex!
  - Don't assume: a prefix is in a single location, IP geolocation is correct, ASNs are in a single country, even when there are datasets for these mappings!
  - ASNs are often mapped to single countries (via RIR stats). Can be misleading
    - 1299 = SE ? 1299 is (was?) headquartered in Sweden, network is worldwide



# BGP Communities



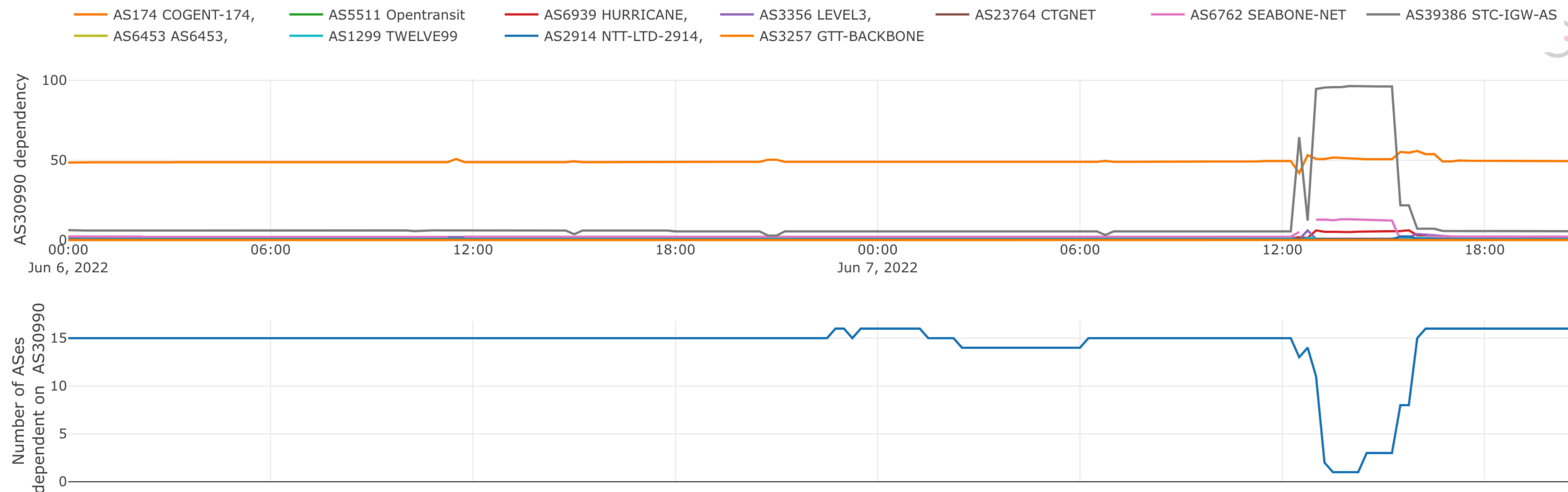
- It is possible to tag a route
  - Informational: “I announce/receive this route from location X”
  - Action: “prefer/depref/change this route”
- Each BGP route has 0+ communities, encoded as 32 bit values.
- Typically
  - The first 16 bits encode an ASN
  - The last 16 bits is informational/action

```
BGP4MP|1203770998|A|208.51.134.248|3549|207.157.90.0/24|3549 6389 8063 3464|IGP|208.51.134.248|0|2953|3549:2292 3549:30840|AG|3464 216.109.7.1|
BGP4MP|1203770998|A|208.51.134.248|3549|204.29.114.0/24|3549 7018 13760 3464|IGP|208.51.134.248|0|2503|3549:2023 3549:30840|AG|3464 216.109.7.1|
BGP4MP|1203770998|A|208.51.134.248|3549|216.109.13.0/24|3549 7018 13760 3464|IGP|208.51.134.248|0|2503|3549:2023 3549:30840|AG|3464 216.109.7.1|
BGP4MP|1203770998|A|208.51.134.248|3549|199.20.24.0/21|3549 7018 13760 3464|IGP|208.51.134.248|0|2503|3549:2023 3549:30840|AG|3464 216.109.7.1|
BGP4MP|1203770998|A|208.51.134.248|3549|129.66.192.0/18|3549 7018 13760 3464|IGP|208.51.134.248|0|2503|3549:2023 3549:30840|AG|3464 216.109.7.1|
```

# Derived Data: Internet Health Report



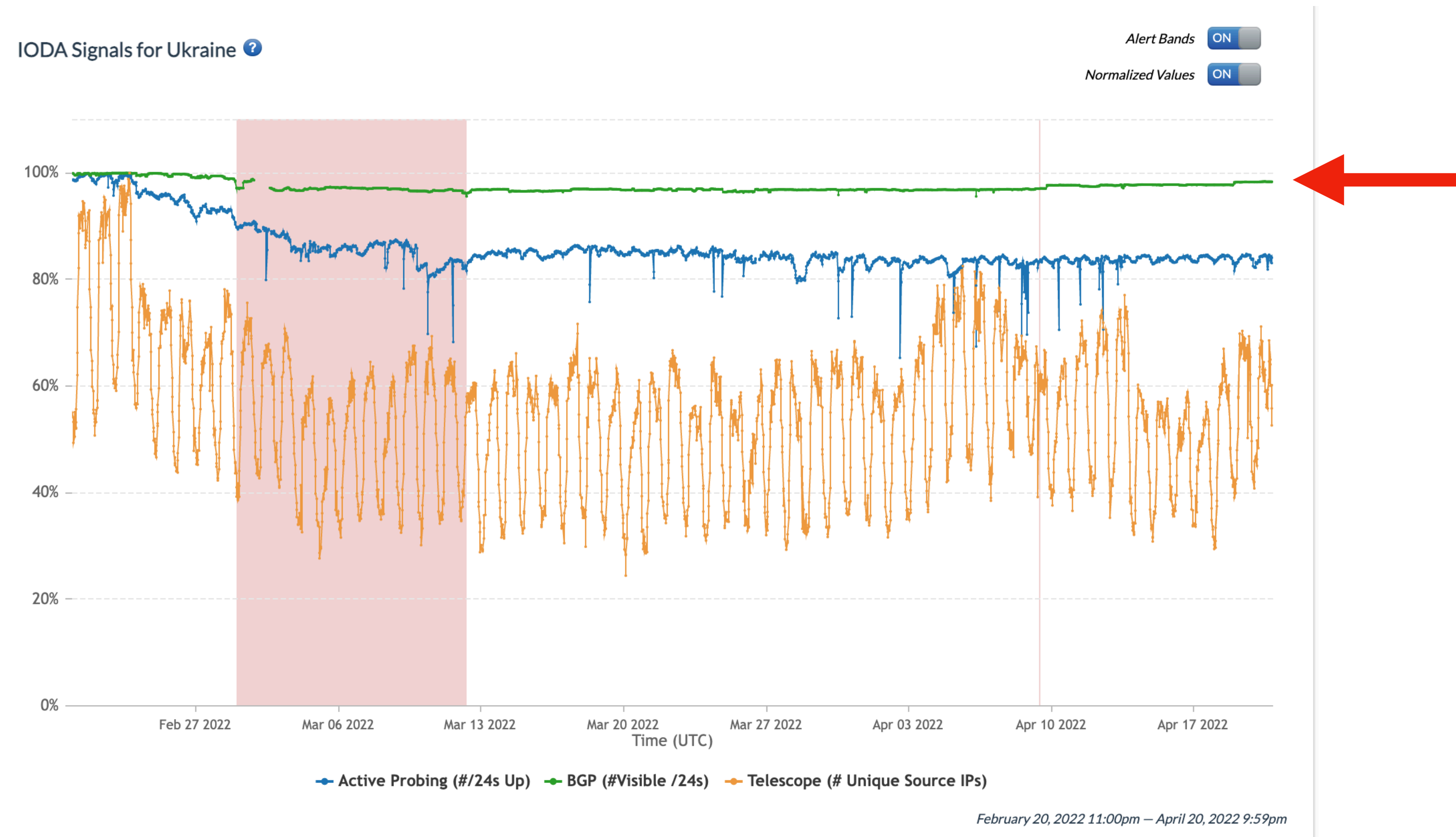
- <https://ihr.iijlab.net/>
- AS-Hegemony: How much does a network depend on another?



# Derived Data: IODA



- <https://ioda.inetintel.cc.gatech.edu/>





# Other Useful Sites For BGP



- [bgp.he.net](http://bgp.he.net) (uses RIS data)
- [bgp.tools](http://bgp.tools)
- [peeringdb.com](http://peeringdb.com)

bgp.he.net/dns/www.ripe.net#\_ipinfo

RRICANE ELECTRIC  
INTERNET SERVICES

Search

[ripe.net](http://ripe.net)

DNS Info Website Info IP Info

104.18.20.44 > 104.18.16.0/20 > AS13335 > Cloudflare, Inc.  
 104.18.20.44 > 104.16.0.0/12 > AS13335 > Cloudflare, Inc.  
 104.18.21.44 > 104.18.16.0/20 > AS13335 > Cloudflare, Inc.  
 104.18.21.44 > 104.16.0.0/12 > AS13335 > Cloudflare, Inc.  
 2606:4700::6812:152c > 2606:4700::/44 > AS13335 > Cloudflare, Inc.  
 2606:4700::6812:152c > 2606:4700::/36 > AS13335 > Cloudflare, Inc.  
 2606:4700::6812:142c > 2606:4700::/44 > AS13335 > Cloudflare, Inc.  
 2606:4700::6812:142c > 2606:4700::/36 > AS13335 > Cloudflare, Inc.

		<a href="http://104.17.240.0/20">104.17.240.0/20</a>	Cloudflare, Inc.
		<a href="http://104.18.0.0/20">104.18.0.0/20</a>	Cloudflare, Inc.
		<a href="http://104.18.16.0/20">104.18.16.0/20</a>	Cloudflare, Inc.
		<a href="http://104.18.32.0/19">104.18.32.0/19</a>	Cloudflare, Inc.
		<a href="http://104.18.32.0/24">104.18.32.0/24</a>	Cloudflare, Inc.
		<a href="http://104.18.32.0/20">104.18.32.0/20</a>	Cloudflare, Inc.

Public Peering Exchange Points

Exchange IPv4	ASN IPv6	Speed	RS Peer
1-IX Internet Exchange 185.1.213.92	13335 2001:7f8:115::92	100G	<input type="radio"/>
48 IX 149.112.3.13	13335 2001:504:14::1:3335:1	10G	<input type="radio"/>
AKL-IX (Auckland NZ) 43.243.21.2	13335 2001:7fa:11:6:0:3417:0:1	100G	<input type="radio"/>
AMS-IX 80.249.211.140	13335 2001:7f8:1::a501:3335:1	300G	<input type="radio"/>
AMS-IX 80.249.210.118	13335 2001:7f8:1::a501:3335:2	300G	<input type="radio"/>
AMS-IX BA 206.41.106.62	13335 2001:504:3d:1:0:a501:3335:1	10G	<input type="radio"/>
AMS-IX Caribbean 200.0.20.10	13335 2001:13c7:6004::a501:3335:1	10G	<input type="radio"/>
AMS-IX Chicago 206.108.115.16	13335 2001:504:38:1:0:a501:3335:1	10G	<input type="radio"/>
AMS-IX Hong Kong 103.247.139.50	13335 2001:df0:296::a501:3335:2	10G	<input type="radio"/>
Any2Denver 206.51.46.41	13335 2605:6c00:303:303::41	10G	<input type="radio"/>
Any2West 206.72.211.63	13335 2001:504:13::211:63	300G	<input type="radio"/>
APE	13335	10G	<input type="radio"/>

Private Peering Facilities

Facility ASN	Country City
1623 Farnam 13335	United States of America Omaha
365 Data Centers Buffalo (BU1) 13335	United States of America Buffalo
365 Data Centers Indianapolis (IN1) 13335	United States of America Indianapolis
365 Data Centers Nashville (NA1) 13335	United States of America Nashville
365 Data Centers Tampa (TA1) 13335	United States of America Tampa
AIMS Kuala Lumpur 13335	Malaysia Kuala Lumpur
AT TOKYO (CC1/CC2) 13335	Japan Tokyo
Berytech Technological Pole 13335	Lebanon Beirut
BR.Digital Curitiba (CTA1) 13335	Brazil Curitiba
BR.Digital Fortaleza (FLA1) 13335	Brazil Fortaleza
BR.Digital Porto Alegre (PAE1) 13335	Brazil Porto Alegre
CarrierColo Berlin Luetzow (I/P/B/ site B) 13335	Germany Berlin
CE_Colo Prague 13335	Czechia Prague