

# Malicious Potential: rDDoS

@blackswanburst

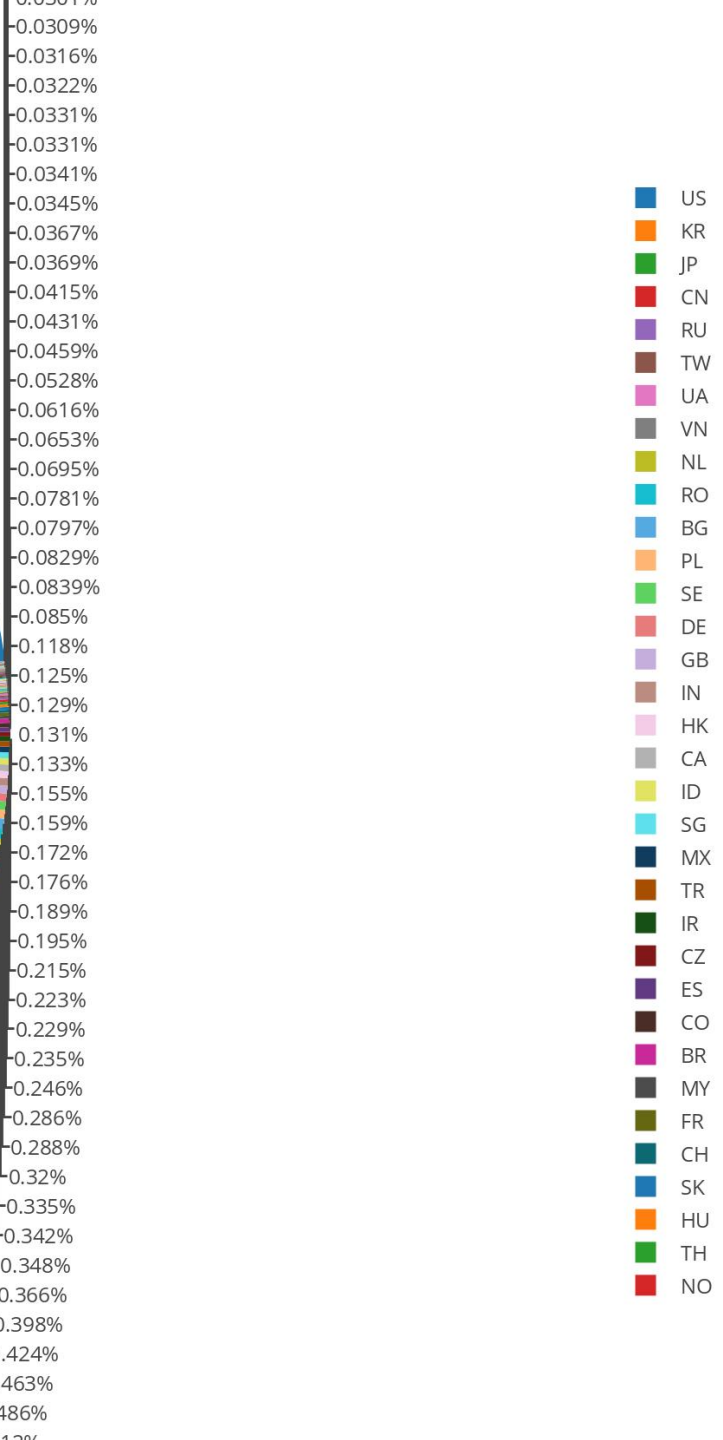
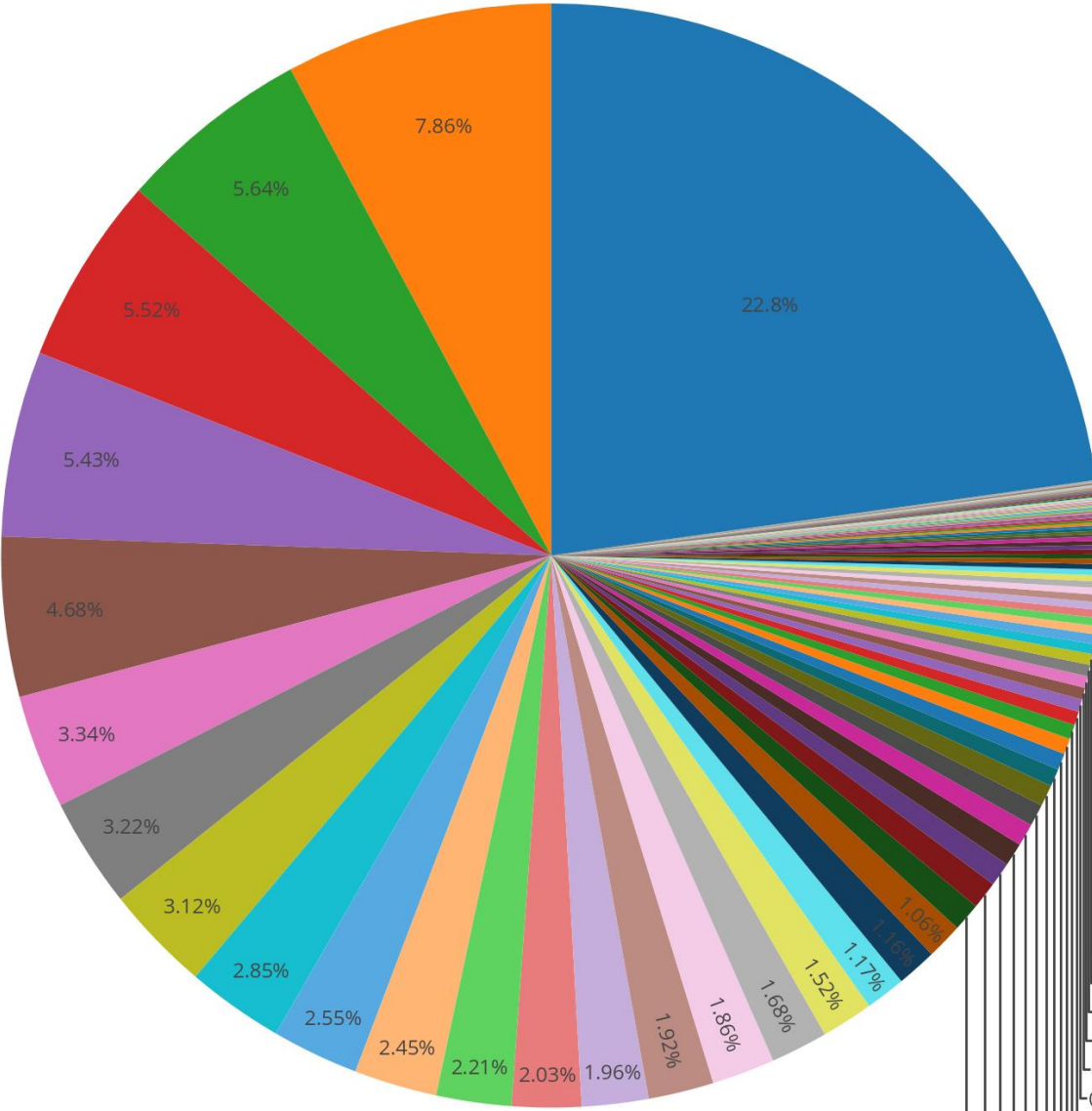
Eireann Leverett

Concinnity Risks

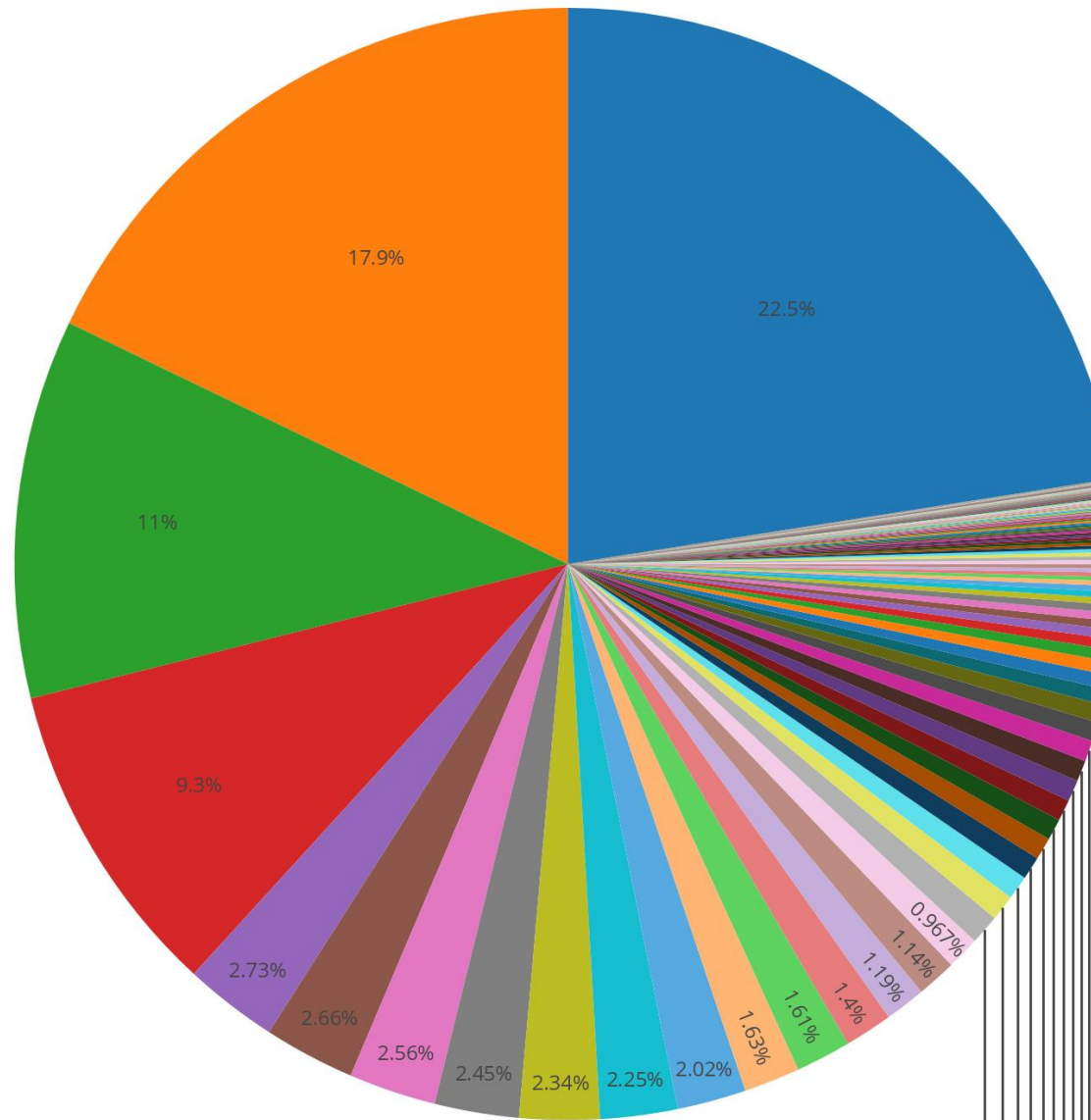
108.49 Tb/s

Is the rDDoS potential of the IPv4 internet.

2016 DNS rDDoS Potential by country (normalised by throughput)



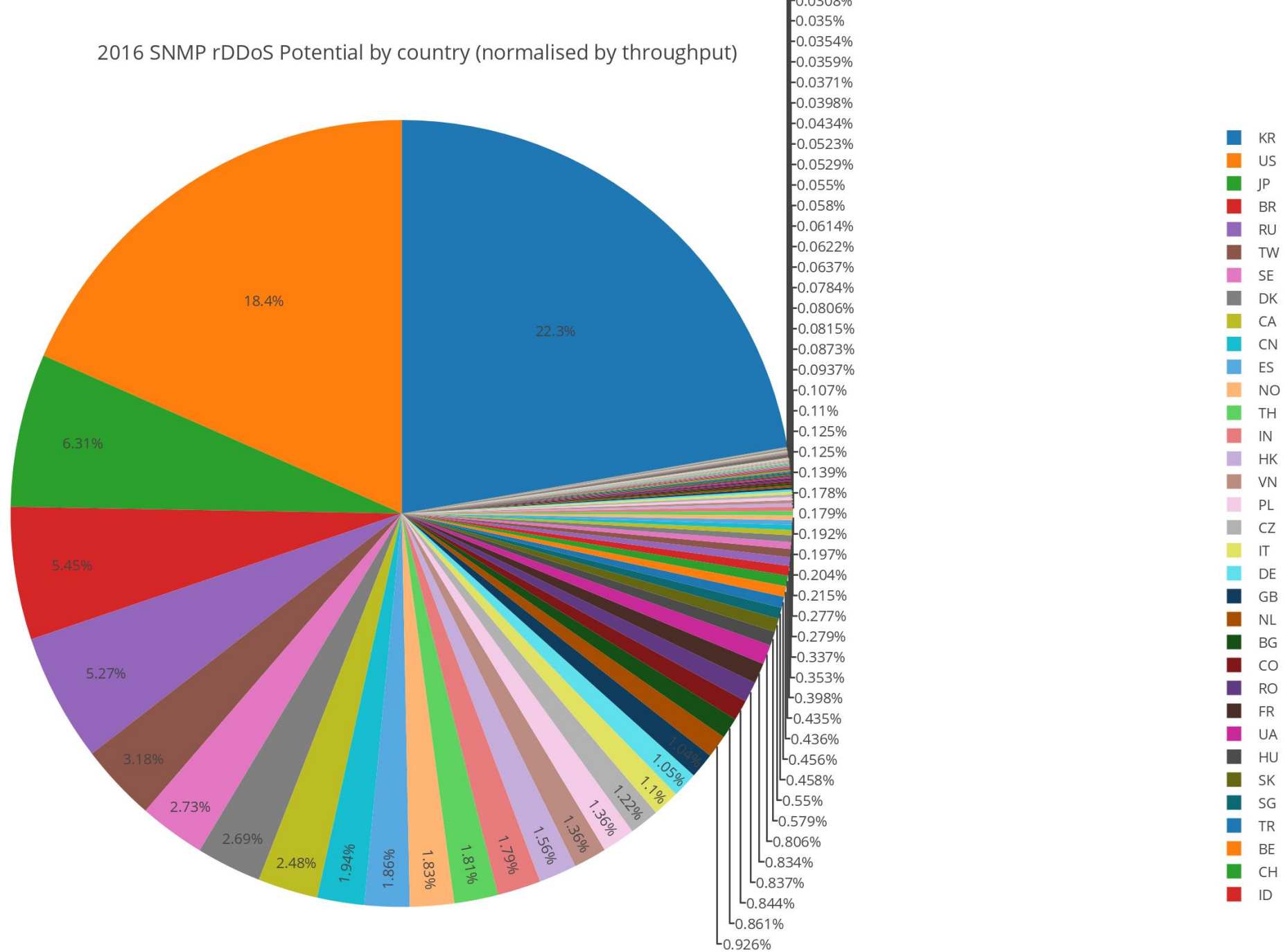
2016 NTP rDDoS Potential by country (normalised by throughput)



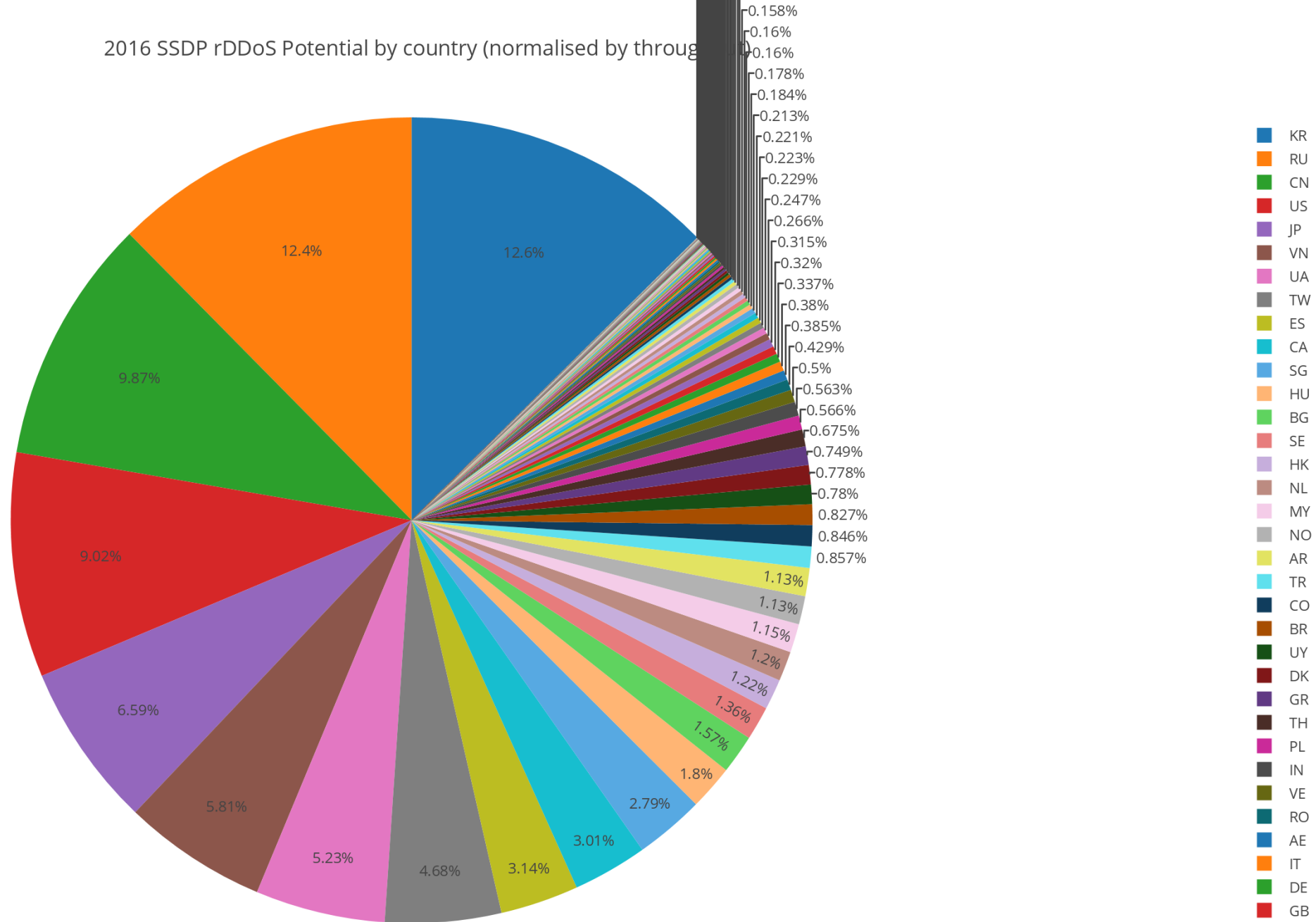
- 0.0305%
- 0.0322%
- 0.0355%
- 0.0381%
- 0.0394%
- 0.0415%
- 0.0459%
- 0.0462%
- 0.0506%
- 0.0511%
- 0.0542%
- 0.0564%
- 0.058%
- 0.0601%
- 0.0621%
- 0.0659%
- 0.0705%
- 0.0753%
- 0.0766%
- 0.0832%
- 0.0908%
- 0.1%
- 0.106%
- 0.111%
- 0.117%
- 0.121%
- 0.121%
- 0.124%
- 0.126%
- 0.139%
- 0.164%
- 0.191%
- 0.193%
- 0.233%
- 0.24%
- 0.243%
- 0.278%
- 0.306%
- 0.339%
- 0.388%
- 0.419%
- 0.524%
- 0.555%
- 0.608%
- 0.611%
- 0.617%
- 0.618%

- US
- KR
- JP
- RU
- CN
- SE
- DE
- RO
- HK
- GB
- DK
- CA
- NL
- NO
- CH
- SG
- UA
- TW
- HU
- CZ
- PL
- BR
- BG
- ES
- VN
- FR
- TH
- MX
- FI
- IN
- BE
- PT
- AU
- AT

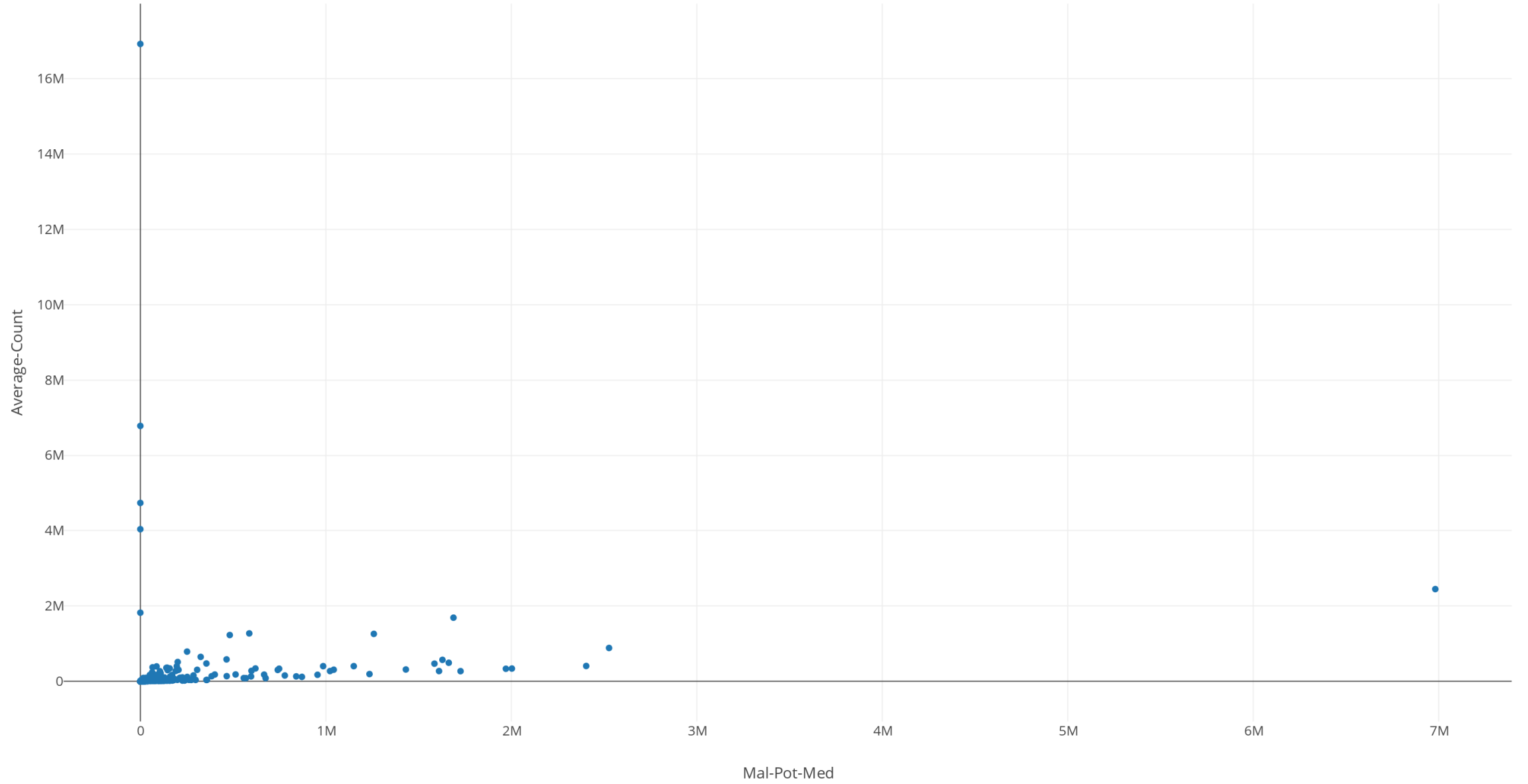
2016 SNMP rDDoS Potential by country (normalised by throughput)



2016 SSDP rDDoS Potential by country (normalised by through



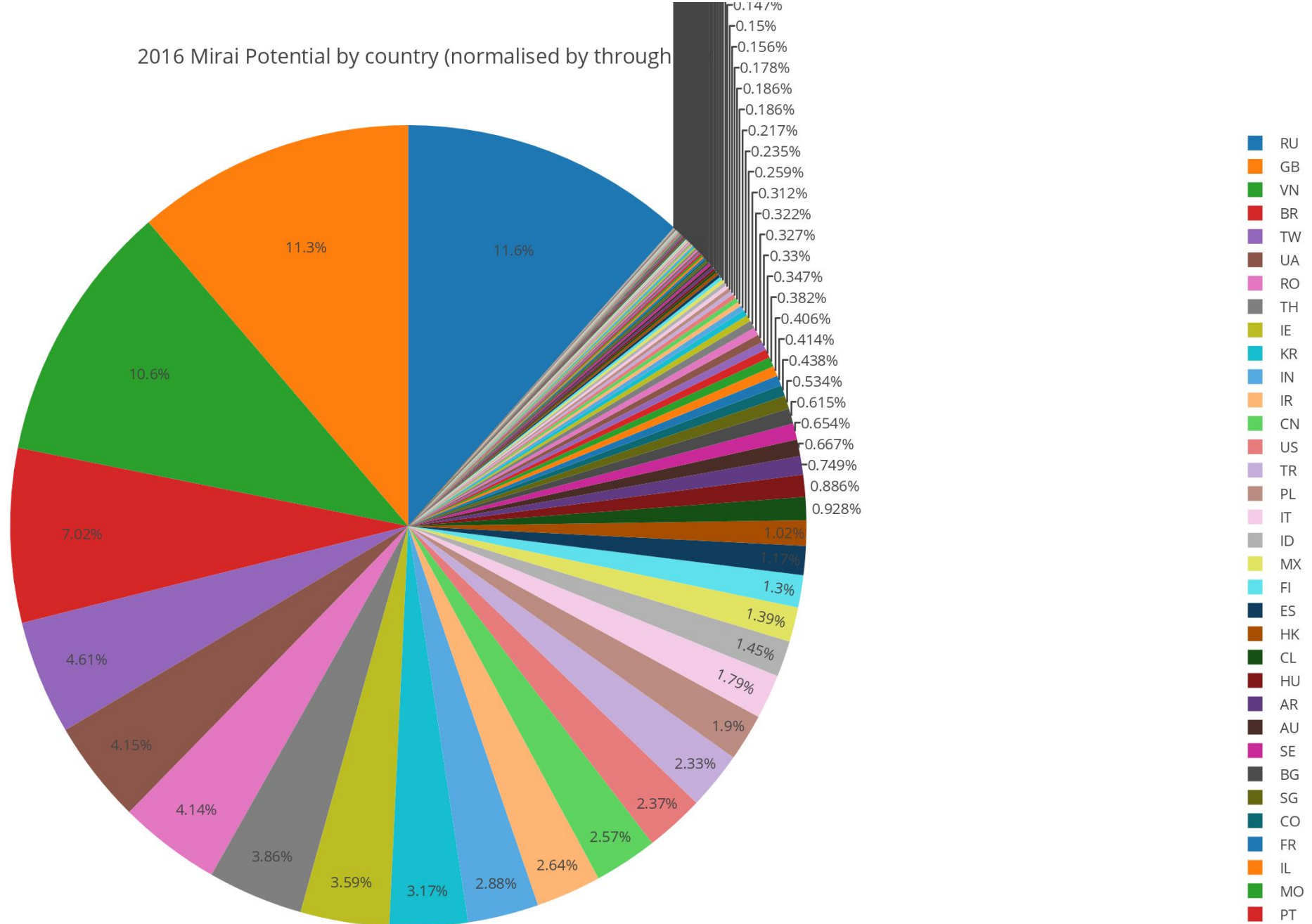
Average Country Count of reflectors vs rDDoS Potential







2016 Mirai Potential by country (normalised by through



# Example Calculation For Latvia

Min(

Upload-Median	Download-Median	Protocol	Amplification Factor	Average CC Count 2016
8.030351	13.83475692	DNS	41	9370.956522
8.030351	13.83475692	NTP	556.9	1758.8125
8.030351	13.83475692	SNMP	6.3	2117.978261
8.030351	13.83475692	SSDP	30.8	3549.340426
8.030351	13.83475692	Mirai	1	279.25

,

\*

)

\*

137.12 GB/S

With 5 protocols summed

# Generalised Equation

$$DDoS_{c_i} [\text{MBit/sec}] = \sum_{j=1}^n risk_j(c_i) * \min(US(c_i); AF(risk_j) * DS(c_i))$$

- Data Sources:
- <https://www.measurementlab.net/data/>
- <http://stats.cybergreen.net/>
- <https://www.us-cert.gov/ncas/alerts/TA14-017A>