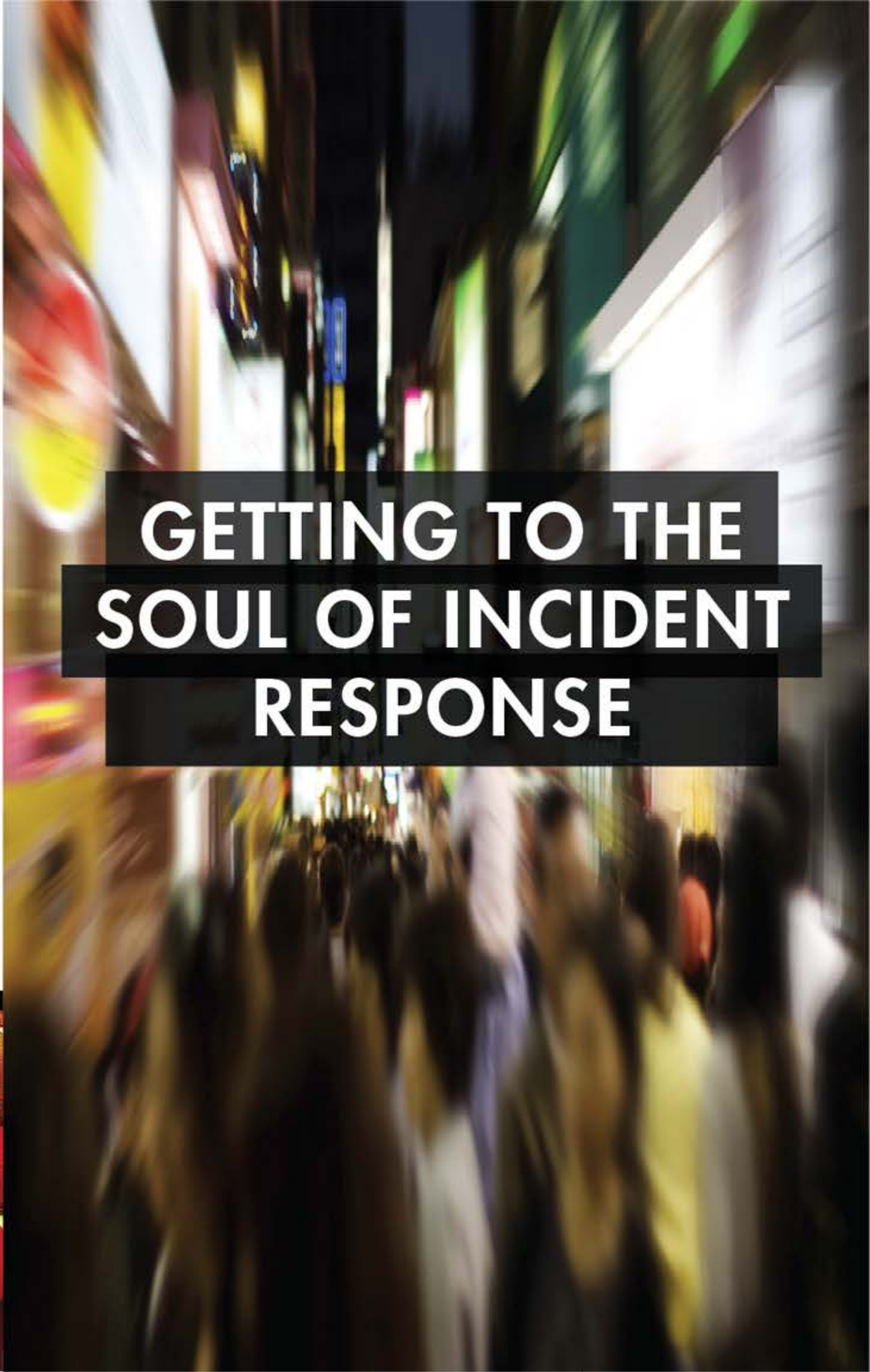
28th ANNUAL FIRST CONFERENCE

SEOUL

JUNE 12 - 17, 2016



GETTING TO THE SOUL OF INCIDENT RESPONSE

A fistful of metrics

John @achillean Matherly

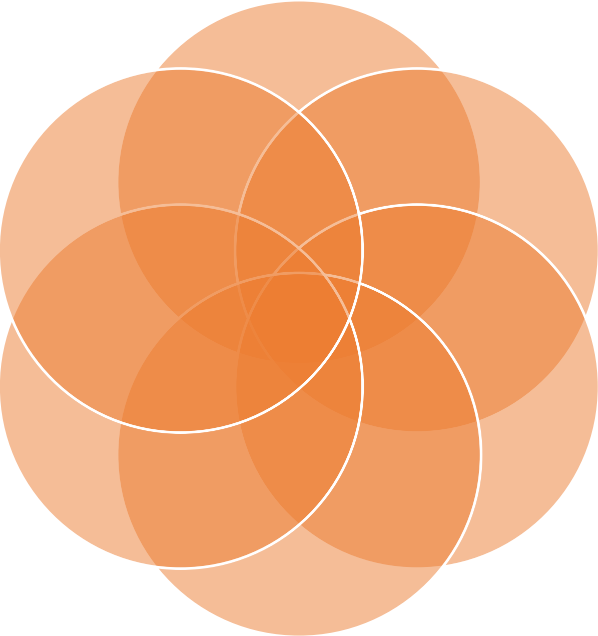
Eireann @blackswanburst Leverett

“Things always become obvious after the fact.”

“Remember that you are a Black Swan.”

- Nassim Nicholas Taleb

The goals of this presentation



Give you metrics you like.

Give you metrics you don’t like.

Make you think, argue, and innovate.

Invent metrics quickly, THEN see if they are useful. NOT present old ones.

Intellectual explorations for John and I.

The honour of standing in front of you again.

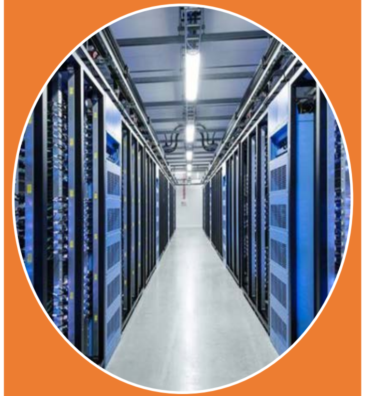
Metrics Answer Questions

- Which is more widespread – ELK RCE or Unauthenticated MongoDB?
- What is the SSL capital of the world?
- How many cars in the USA have novelty license plates?
- Which countries are jumping on board IoT?
- Where are the bad neighborhoods of SSL?
- Is Internet-eavesdropping cultural?

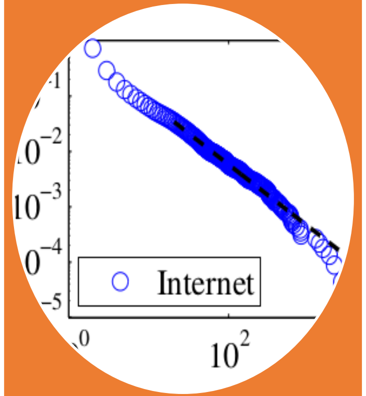
Principles we found

If your metric wouldn't help an attacker why are you measuring it? It's dual use is a sign of it's utility for defense!

Reduce external dependencies to ensure reproducibility.



Machine only metrics don't translate to non-technical folks. That's why economists say "per capita" and LD-50 is used by toxicologists.



Distributions matter. Populations are important.

All data is biased. Understanding the bias and adjust accordingly.

L-W cost

How does it work:

- Choose a vuln
- Scan network
- Distinguish vulnerable from N/A in total network
- Divide the cost over the vulnerable hosts

Why the cost?

- Because it translates to non-technical
- This is for vulnerability across constituencies.
- It’s easy to talk about.

Example usage:

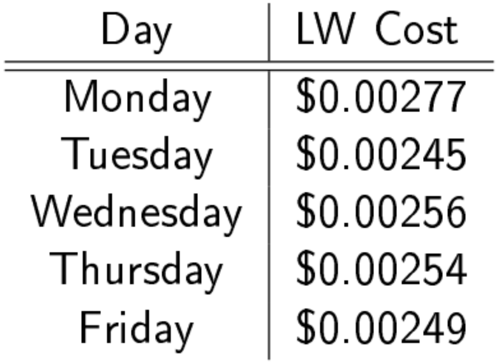
- SSH brute forcing hosts on our internal network had a L-W cost of $4.89 USD.

Example usage:

- Elastic Search RCE has an L-W cost of $0.00024 across all of IPv4

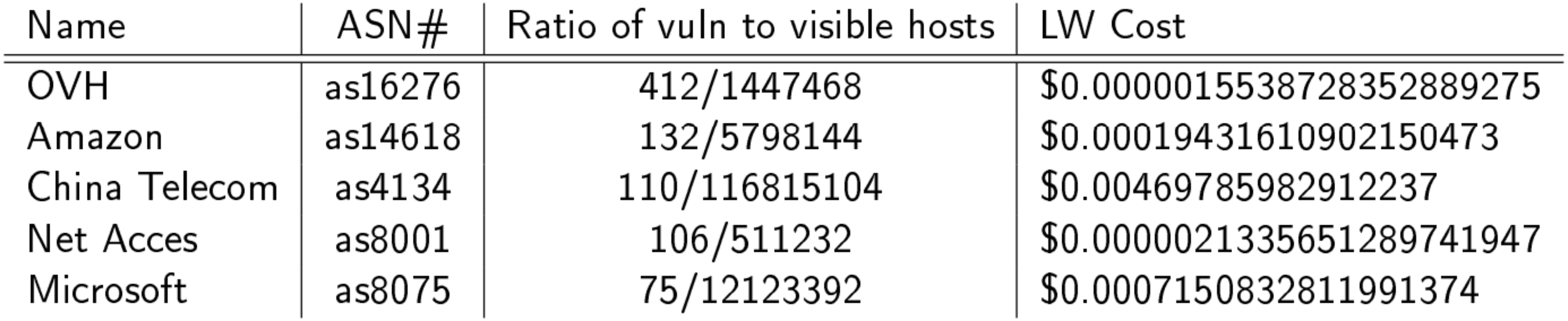
How can I use it in practice?

1. You can compare networks
2. You can compare change over time
3. You can even imagine vulnerabilities you haven’t seen yet, and see how much effort it would take to patch



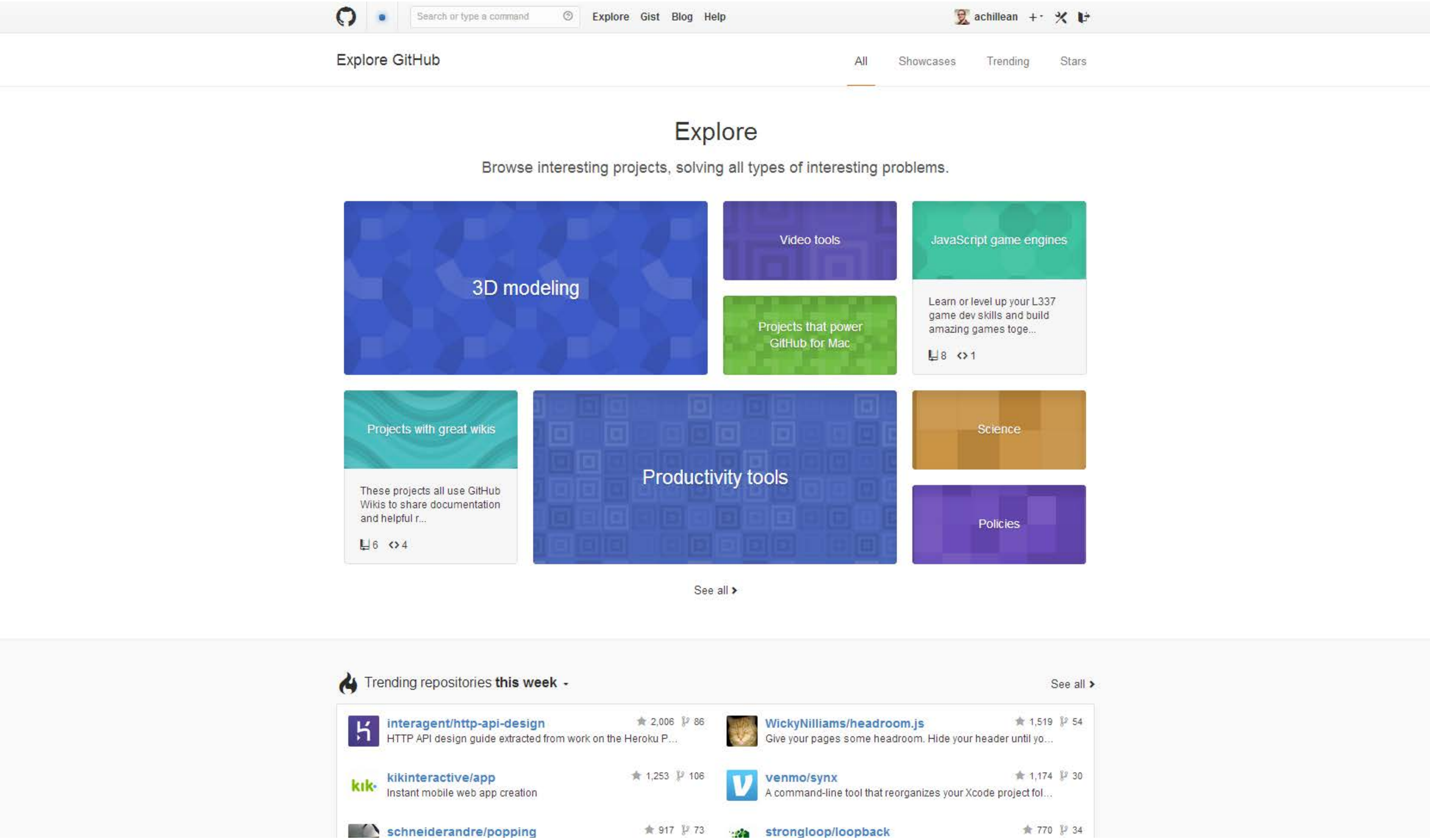
Day	LW Cost
Monday	$0.00277
Tuesday	$0.00245
Wednesday	$0.00256
Thursday	$0.00254
Friday	$0.00249

Table : CVE-2015-5377 ELK RCE Over time



Name	ASN#	Ratio of vuln to visible hosts	LW Cost
OVH	as16276	412/1447468	$0.000015538728352889275
Amazon	as14618	132/5798144	$0.00019431610902150473
China Telecom	as4134	110/116815104	$0.00469785982912237
Net Acces	as8001	106/511232	$0.0000021335651289741947
Microsoft	as8075	75/12123392	$0.0007150832811991374

Table : Top five vulnerable organisations



Explore

Browse interesting projects, solving all types of interesting problems.

Learn or level up your L337 game dev skills and build amazing games toge...

8 <> 1

These projects all use GitHub Wikis to share documentation and helpful r...

6 <> 4

Trending repositories **this week**

interagent/http-api-design ★ 2,006 86
HTTP API design guide extracted from work on the Heroku P...

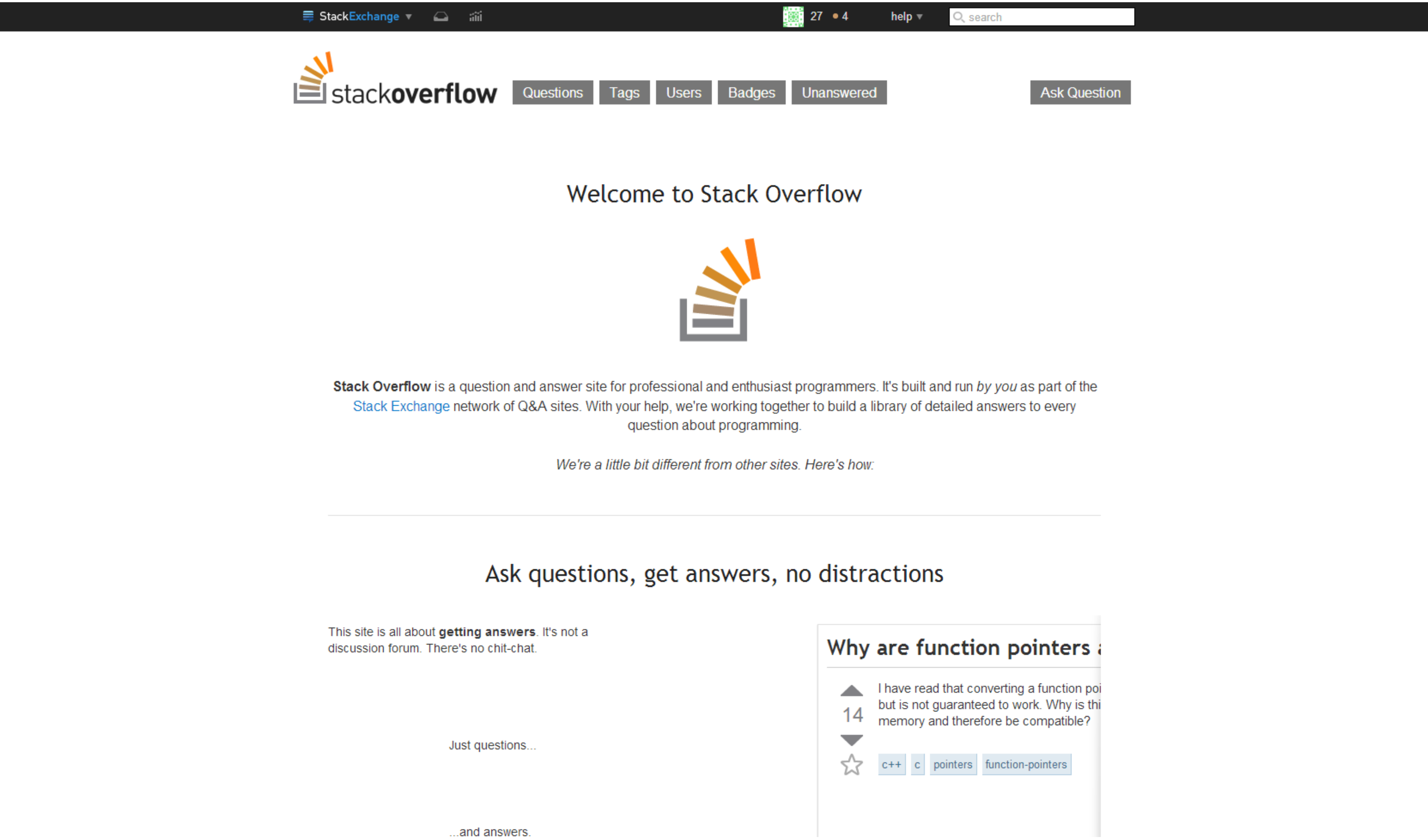
WickyNilliams/headroom.js ★ 1,519 54
Give your pages some headroom. Hide your header until yo...

kikinteractive/app ★ 1,253 106
Instant mobile web app creation

venmo/synx ★ 1,174 30
A command-line tool that reorganizes your Xcode project fol...

schneiderandre/popping ★ 917 73

strongloop/loopback ★ 770 34



Welcome to Stack Overflow

Stack Overflow is a question and answer site for professional and enthusiast programmers. It's built and run *by you* as part of the Stack Exchange network of Q&A sites. With your help, we're working together to build a library of detailed answers to every question about programming.

We're a little bit different from other sites. Here's how:

Ask questions, get answers, no distractions

This site is all about **getting answers**. It's not a discussion forum. There's no chit-chat.

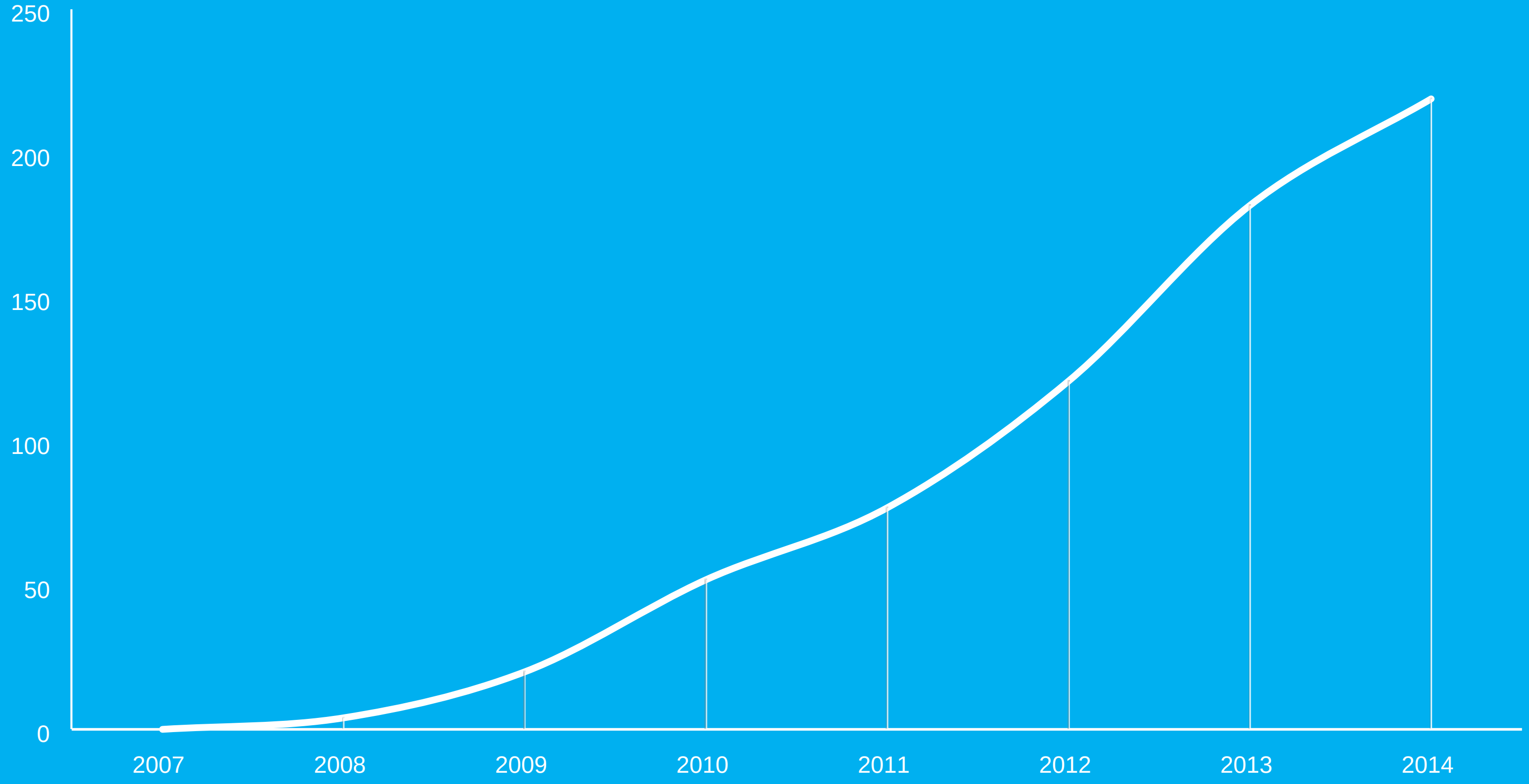
Just questions...

...and answers.

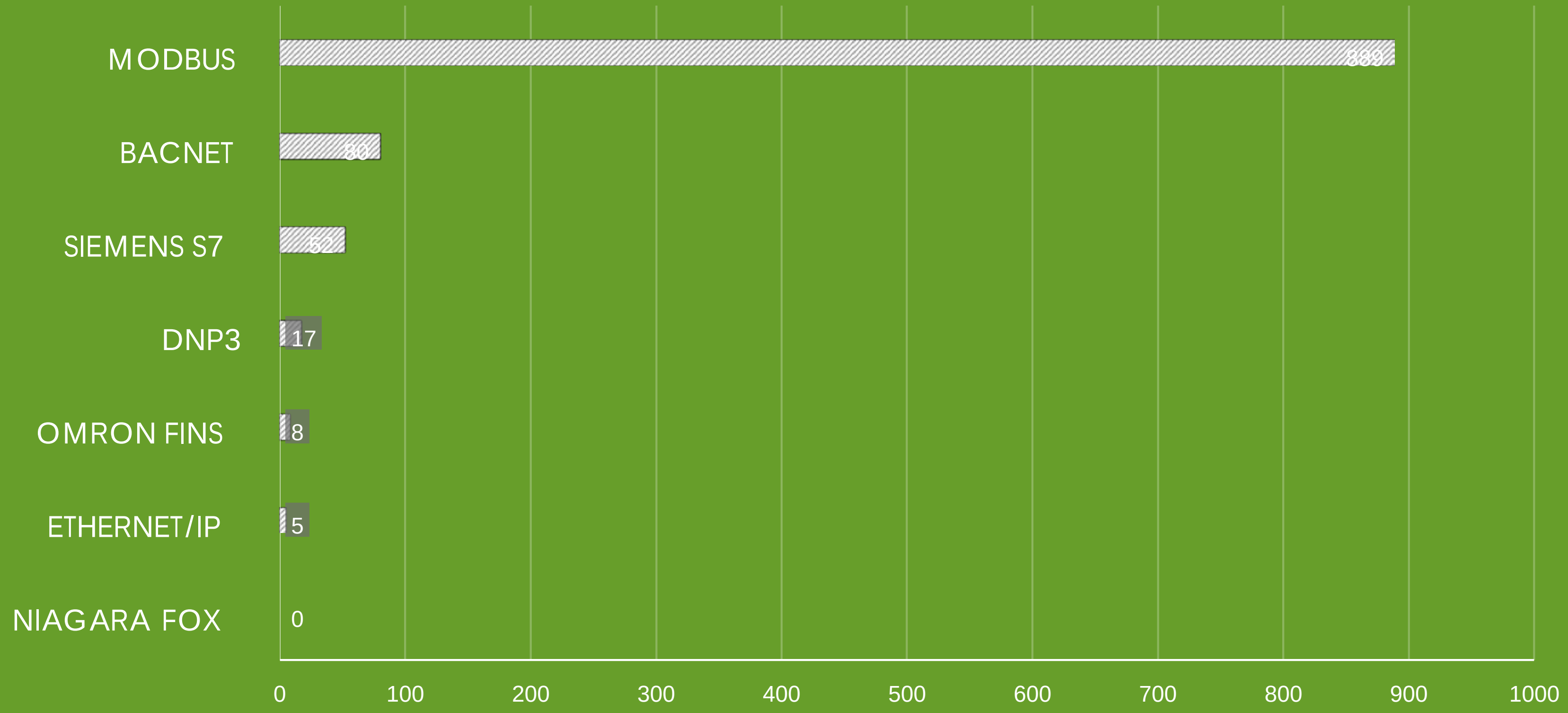
Why are function pointers a

I have read that converting a function poi but is not guaranteed to work. Why is thi memory and therefore be compatible?

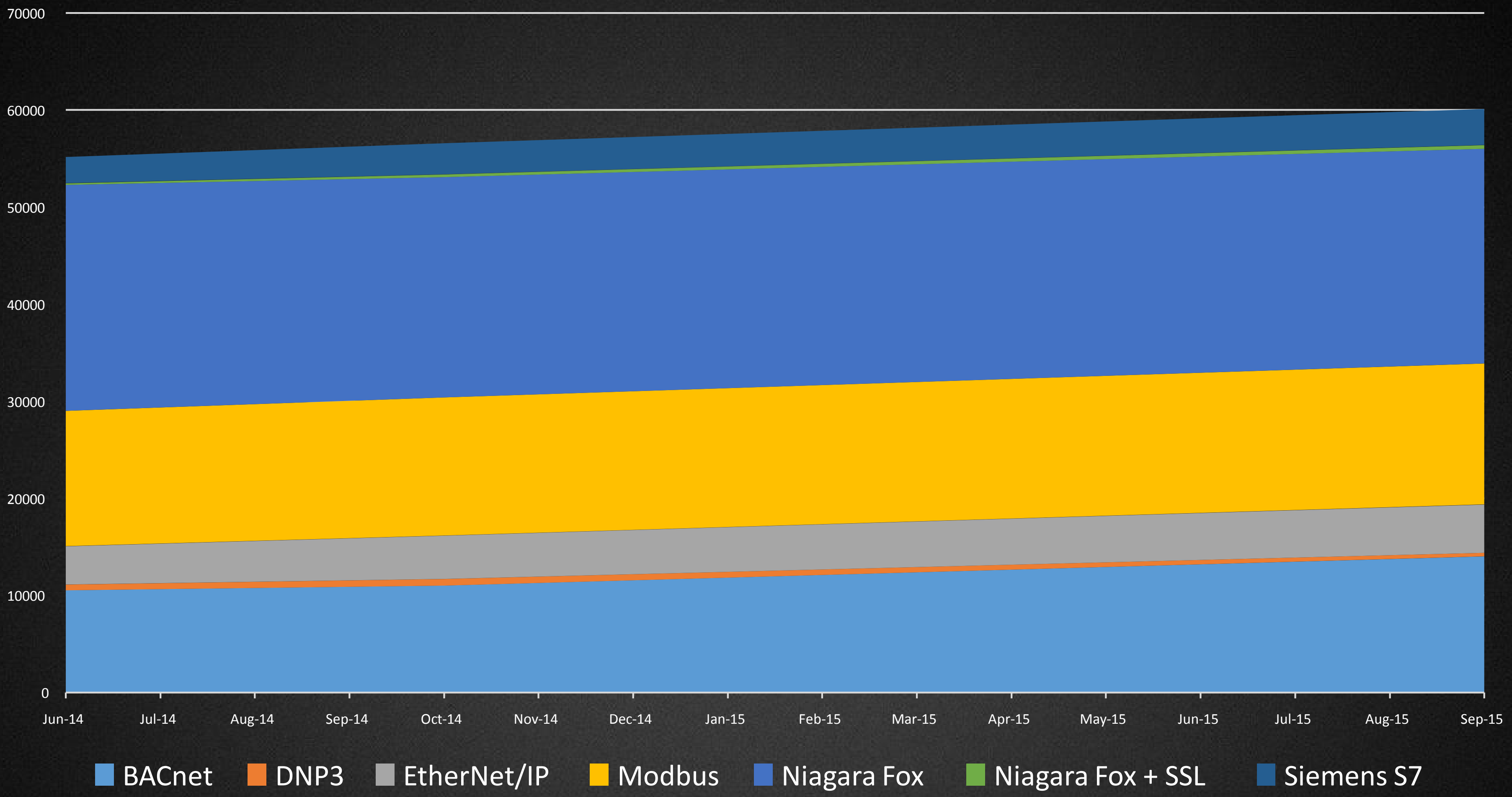
MODBUS QUESTIONS PER YEAR



POPULARITY ON STACKOVERFLOW



ICS Protocol Growth



#16 Australia

#17 Hungary

#18 China

#19 Malaysia

#20 Finland

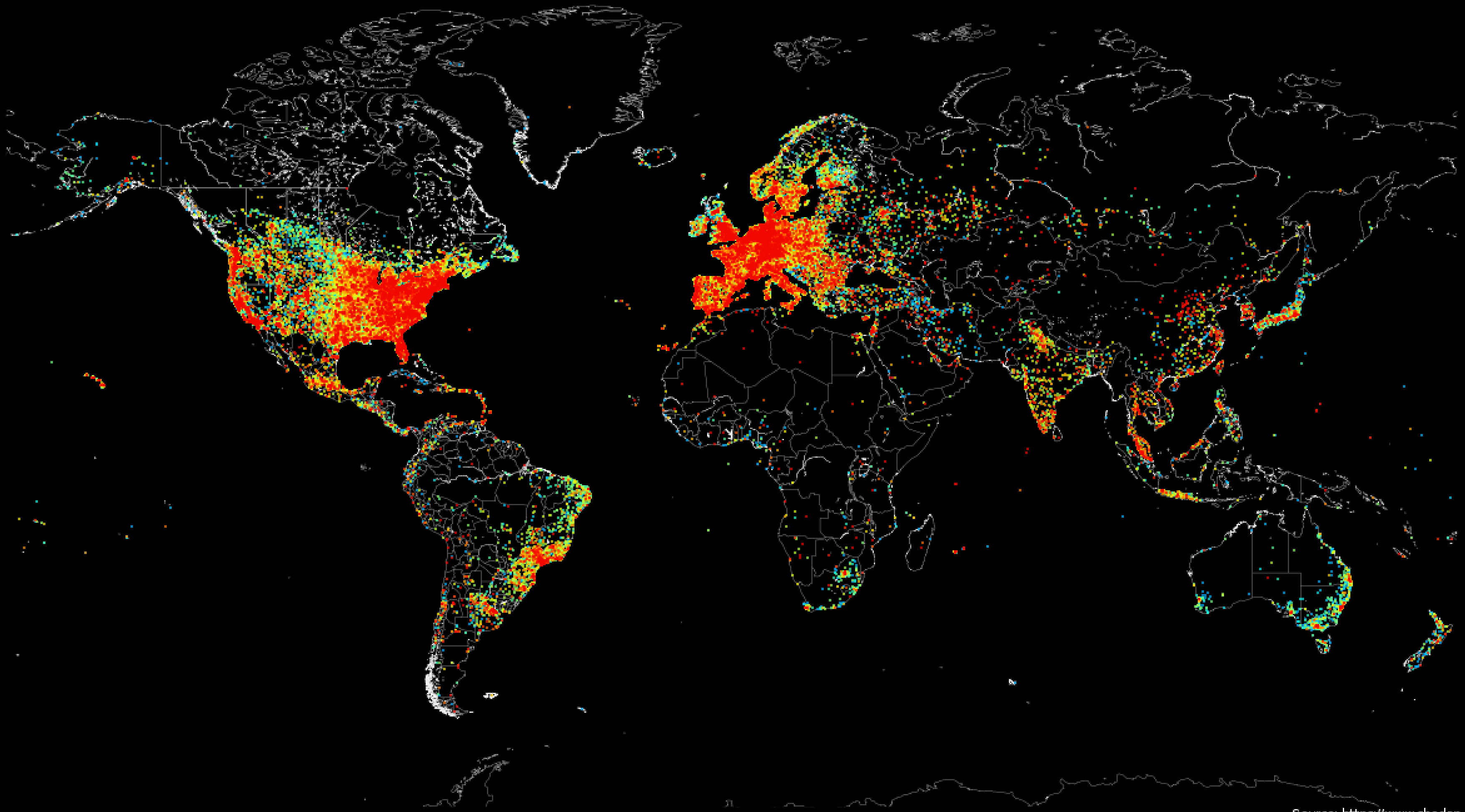
#21 Switzerland

#22 Russia

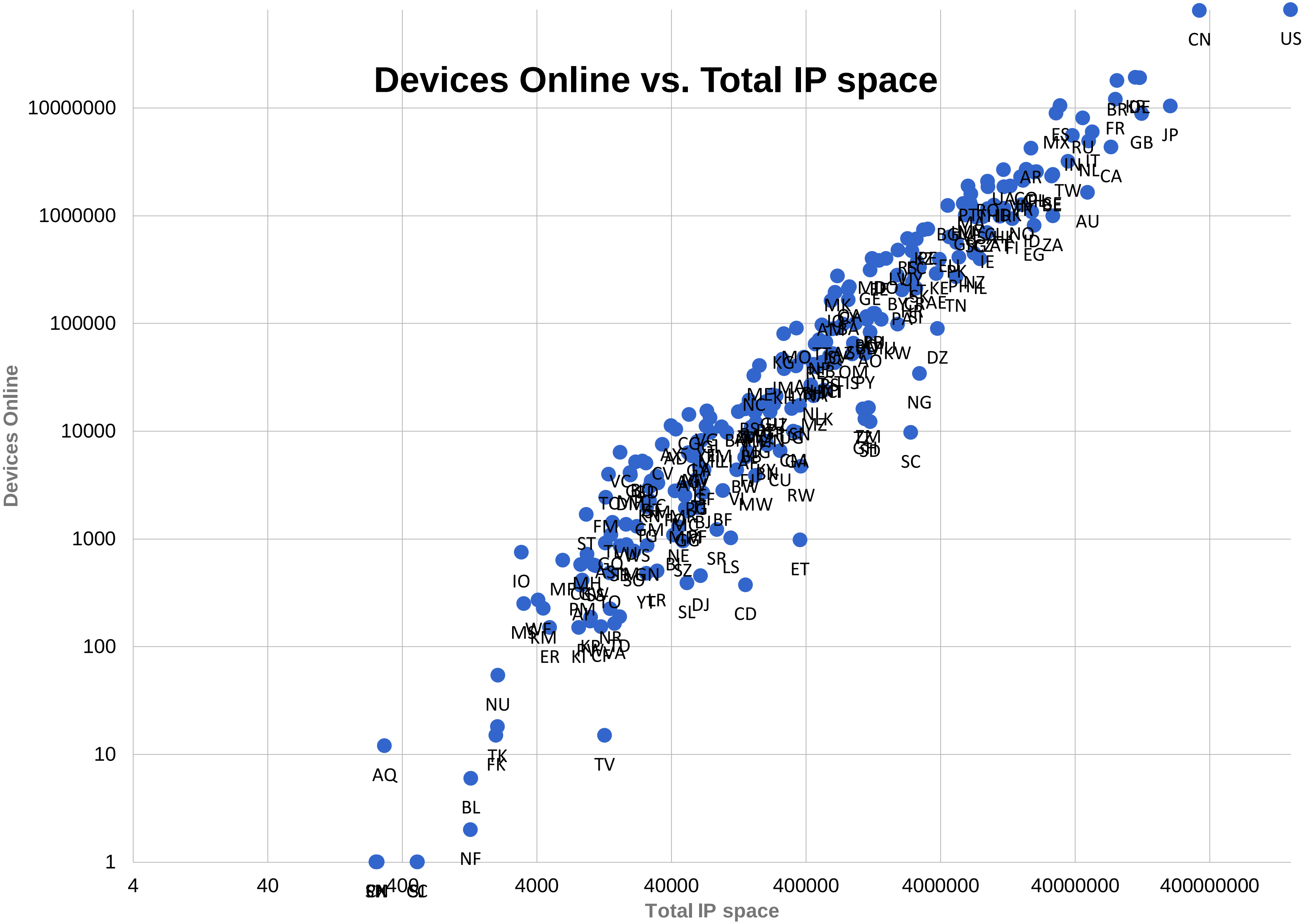
#23 Lithuania

#14 Brazil
#15 Czech Republic
#16 China
#19 Lithuania
#20 Romania
#21 Russia
#22 Austria
#23 Switzerland

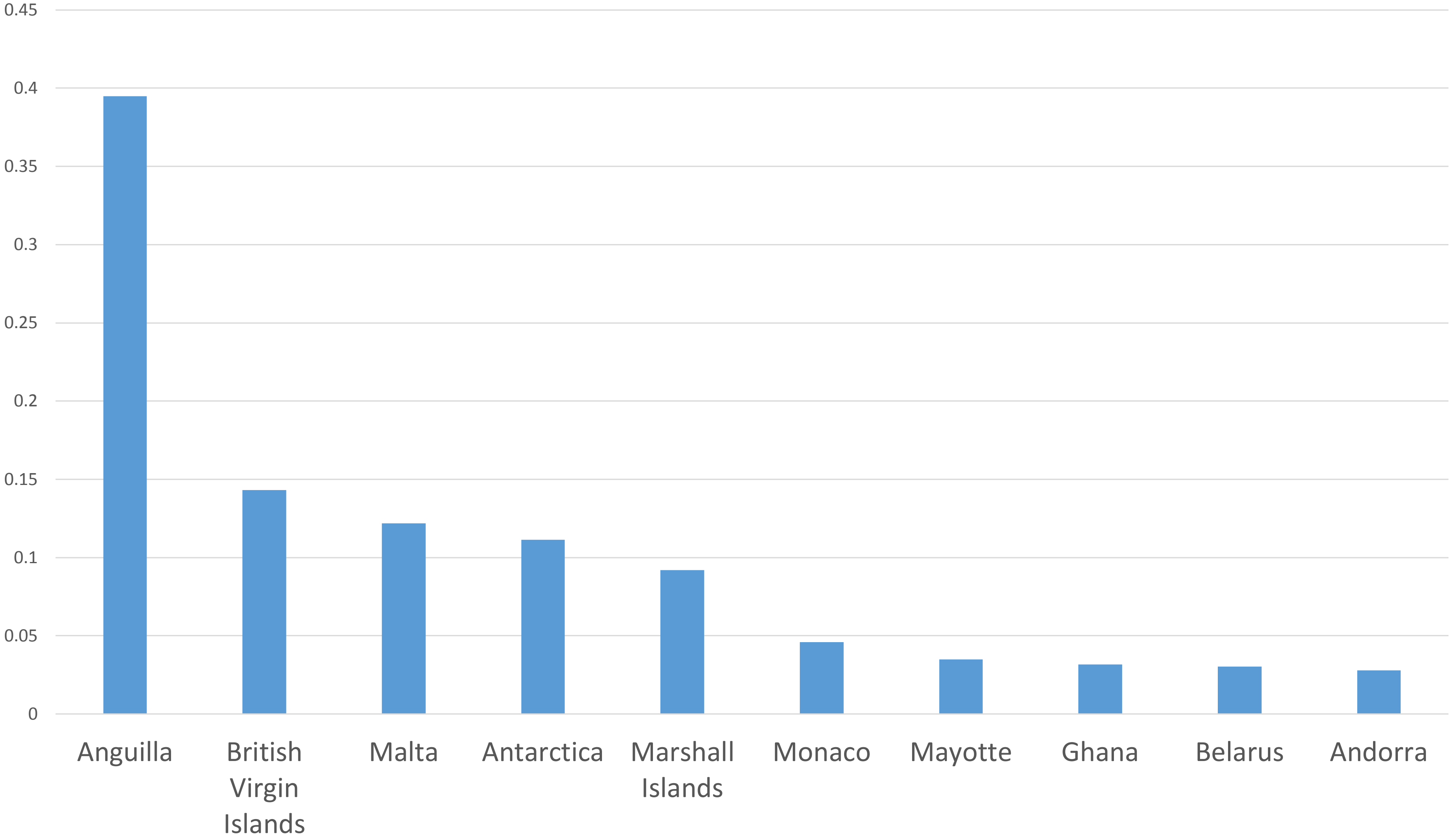
SHODAN

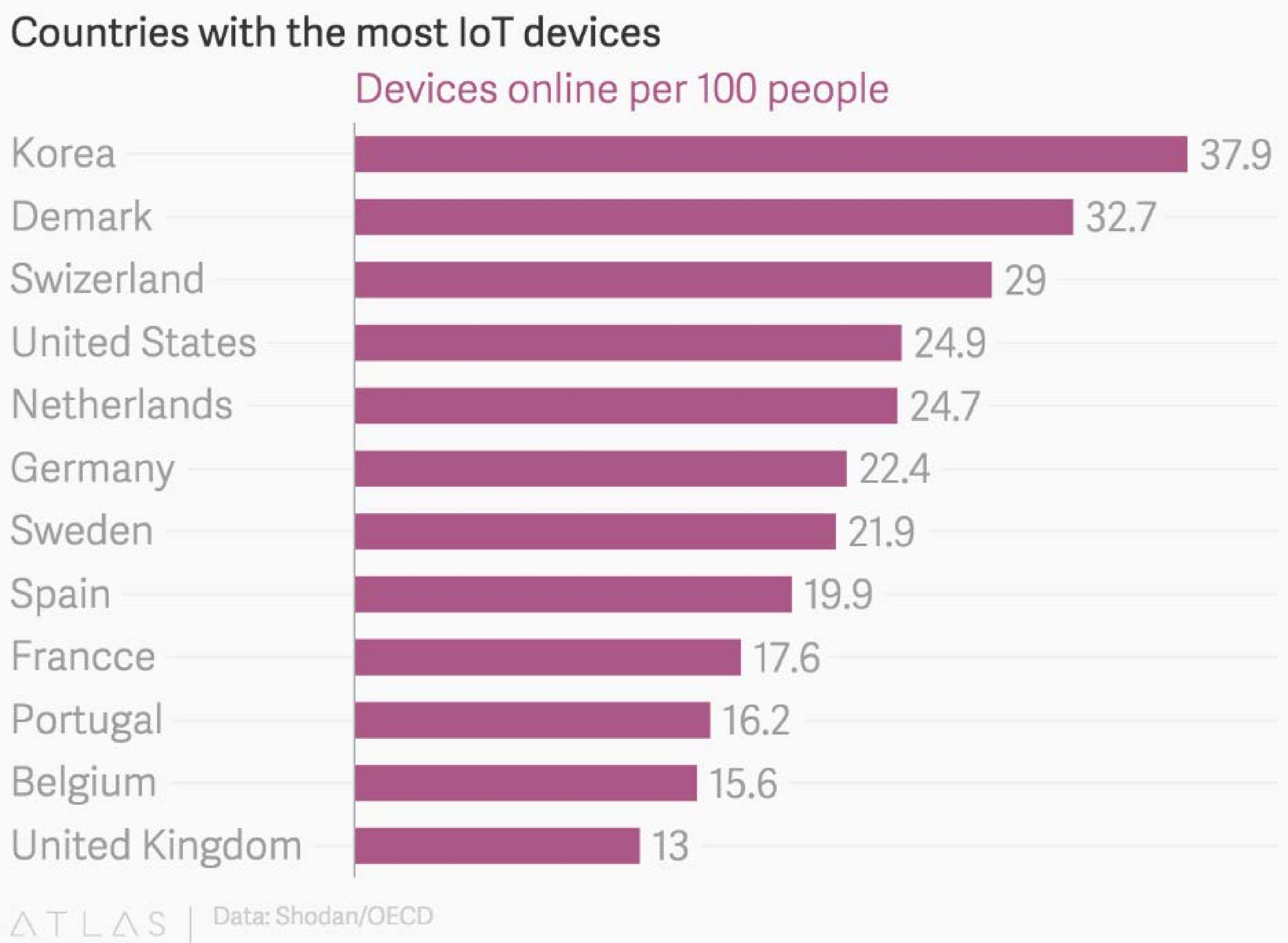


Source: https://www.shodan.io


Devices Online vs. Total IP space
Devices Online
Total IP space
10000000
1000000
100000
10000
1000
100
10
1
4
40
400
4000
40000
400000
4000000
40000000
400000000
CN
US
JP
GB
FR
CA
AU
ZA
EG
TW
AR
IN
IT
NL
MX
RU
ES
IE
NZ
TN
DZ
NG
SC
KW
AO
RW
MW
ET
CD
SL
DJ
LS
SR
SZ
NE
BF
TV
TK
FK
NU
BL
NF
AQ
IO
ER
KI
NR
MS
KM
WF
PM
AI
YT
TO
ST
FM
VC
CV
VI
CU
BW
KY
BN
CM
CG
NC
KG
MK
GE
PA
SI
MO
ZM
GH
SD
PY
OM
NL
UZ
KE
PH
BY
ZA
FI
NO
ID
TH
DK
UA
CL
SE
BR
DE
KR
SN
SC

Top Gainers


0.45
0.4
0.35
0.3
0.25
0.2
0.15
0.1
0.05
0
Anguilla
British Virgin Islands
Malta
Antarctica
Marshall Islands
Monaco
Mayotte
Ghana
Belarus
Andorra



Countries with the most IoT devices

Data: Shodan/OECD

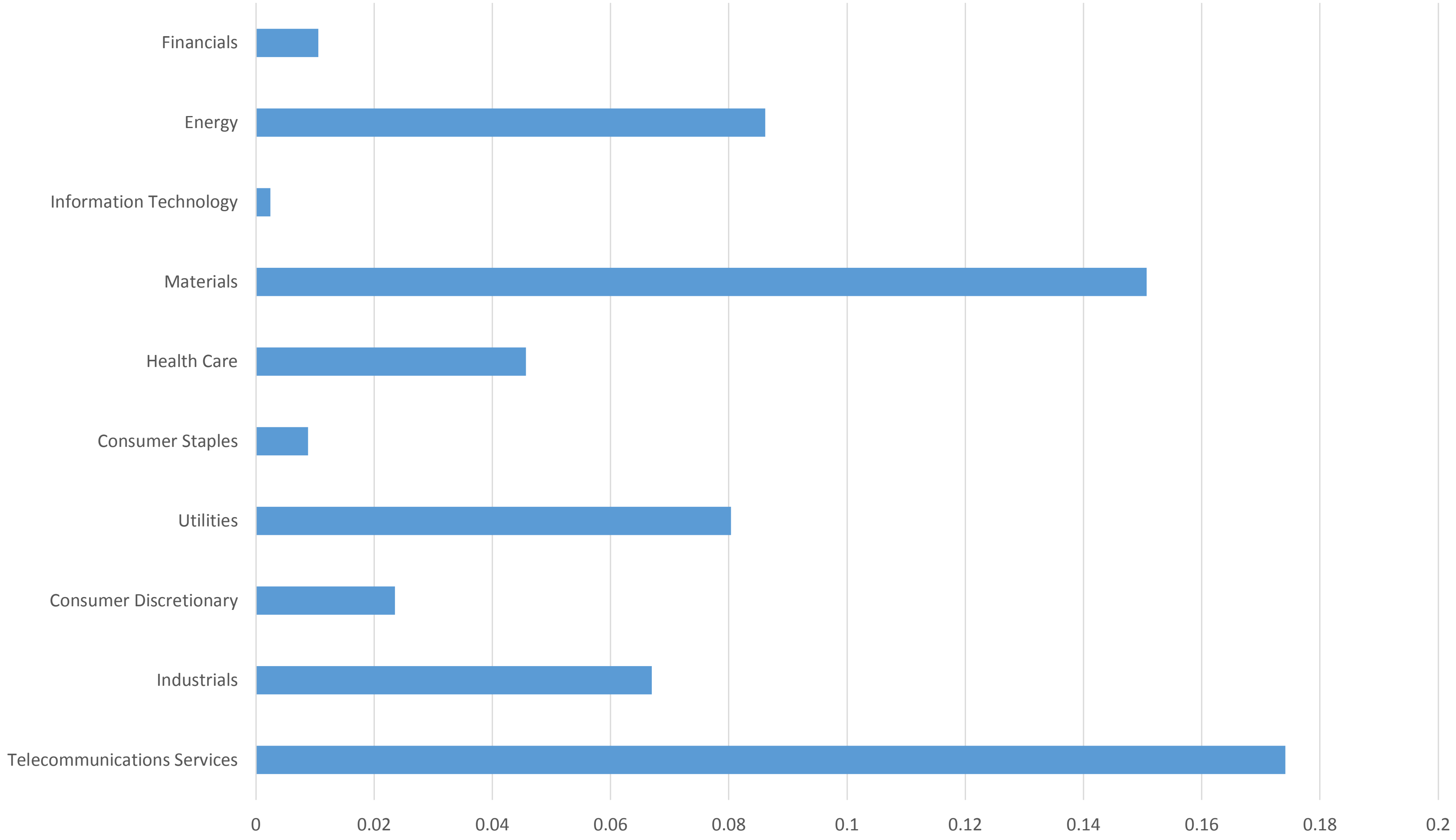
UNITED NATIONS GLOBAL PULSE

Harnessing big data for development and humanitarian action

SSL/TLS by sector

Sector	Heartbleed	Count	SSLv2	SSLv3	TLSv1	TLSv1.1	TLSv1.2
Telecommunications Services	2550	14357795	494756	663929	3041207	224645	229355
Industrials	3	11009	352	2176	4347	2498	3019
Consumer Discretionary	7014	8234391	40276	290888	1491892	1265697	1272378
Utilities	0	881	40	157	351	253	261
Consumer Staples	0	6679	43	202	3246	2974	2977
Health Care	3	10338	232	1433	4759	3520	3755
Materials	0	2563	104	291	659	398	478
Information Technology	223	6619025	7592	149568	2721123	2684986	2697873
Energy	0	2064	62	339	855	630	638
Financials	0	16338	93	1568	7334	5203	5791

% SSLv2


Financials
Energy
Information Technology
Materials
Health Care
Consumer Staples
Utilities
Consumer Discretionary
Industrials
Telecommunications Services
0
0.02
0.04
0.06
0.08
0.1
0.12
0.14
0.16
0.18
0.2

SSH/People

SEYCHELLES	0.040536105
IRELAND	0.030029077
SINGAPORE	0.028632523
SAINT VINCENT	0.025676664
KYRGYZSTAN	0.021243156
ANTIGUA	0.017359736
SAINT KITTS	0.017144729
NETHERLANDS	0.016761866
GUAM	0.013781537
USA	0.012438426
HONG KONG	0.011747104

SSL/People

NETHERLANDS	0.072849
IRELAND	0.047603
USA	0.040362
LIECHTENSTEIN	0.037387
SINGAPORE	0.034396
LUXEMBOURG	0.028766
MONACO	0.026845
ISLE OF MAN	0.025939
CAYMAN ISLANDS	0.022291
GERMANY	0.01987
ITALY	0.019628

Telnet/People

GUAM	0.06082
ANTIGUA	0.030176
SAINT VINCENT	0.0281
NEW CALEDONIA	0.022068
SAINT KITTS	0.021567
TRINIDAD & TOBEGO	0.017805
DOMINICAN REPUBLIC	0.01733
CAYMAN ISLANDS	0.015599
NORWAY	0.015157
GRENADA	0.014603
SOUTH KOREA	0.014176

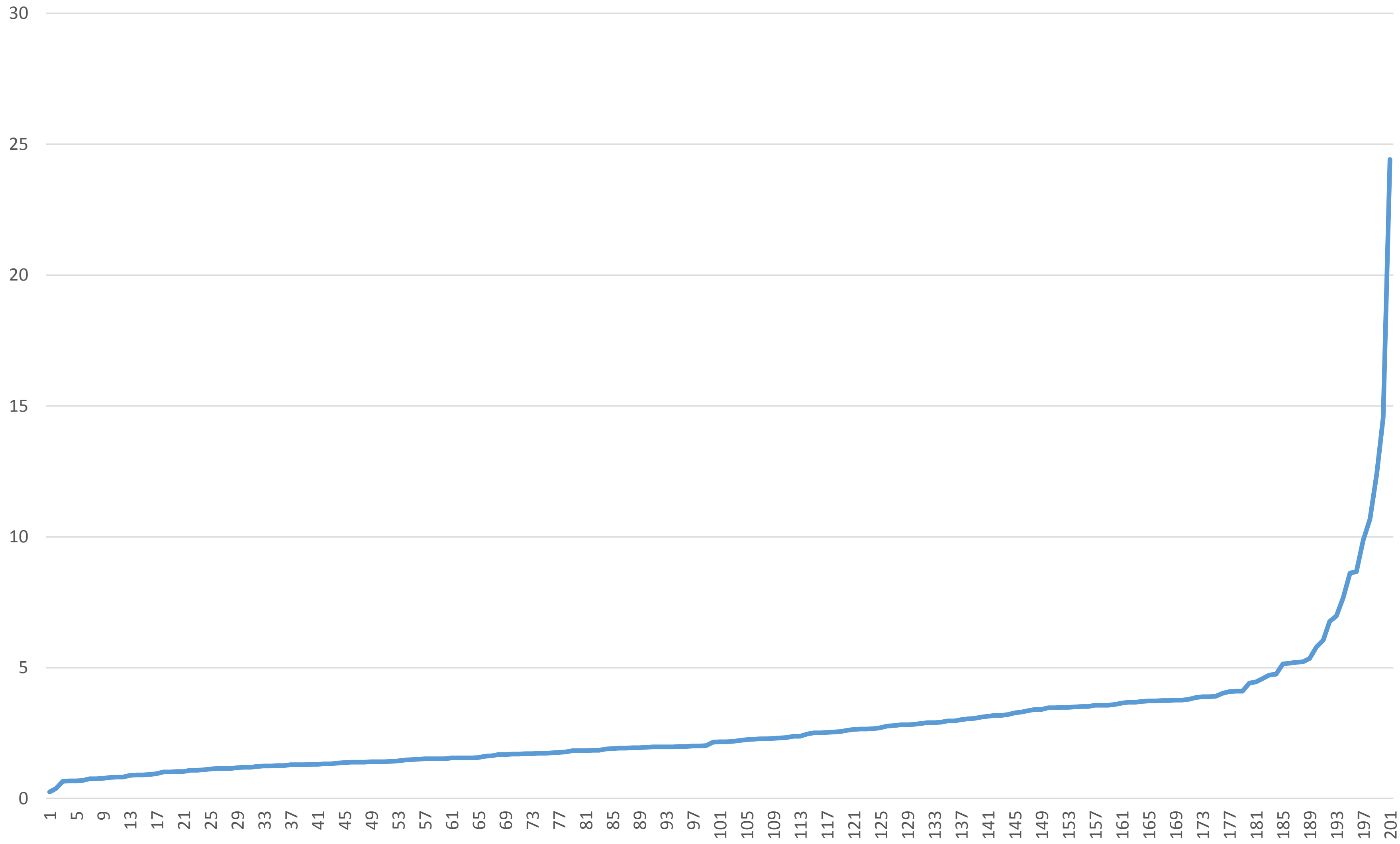
IPv6

1. 80
2. 443
3. 8080
4. 53
5. 81
6. 20000
7. 9080
8. 8888
9. 9100
10. 9000

IPv4

1. 7547
2. 80
3. 443
4. 5060
5. 4567
6. 22
7. 23
8. 8080
9. 53
10. 21

HTTP vs HTTPS



HTTP vs HTTPS

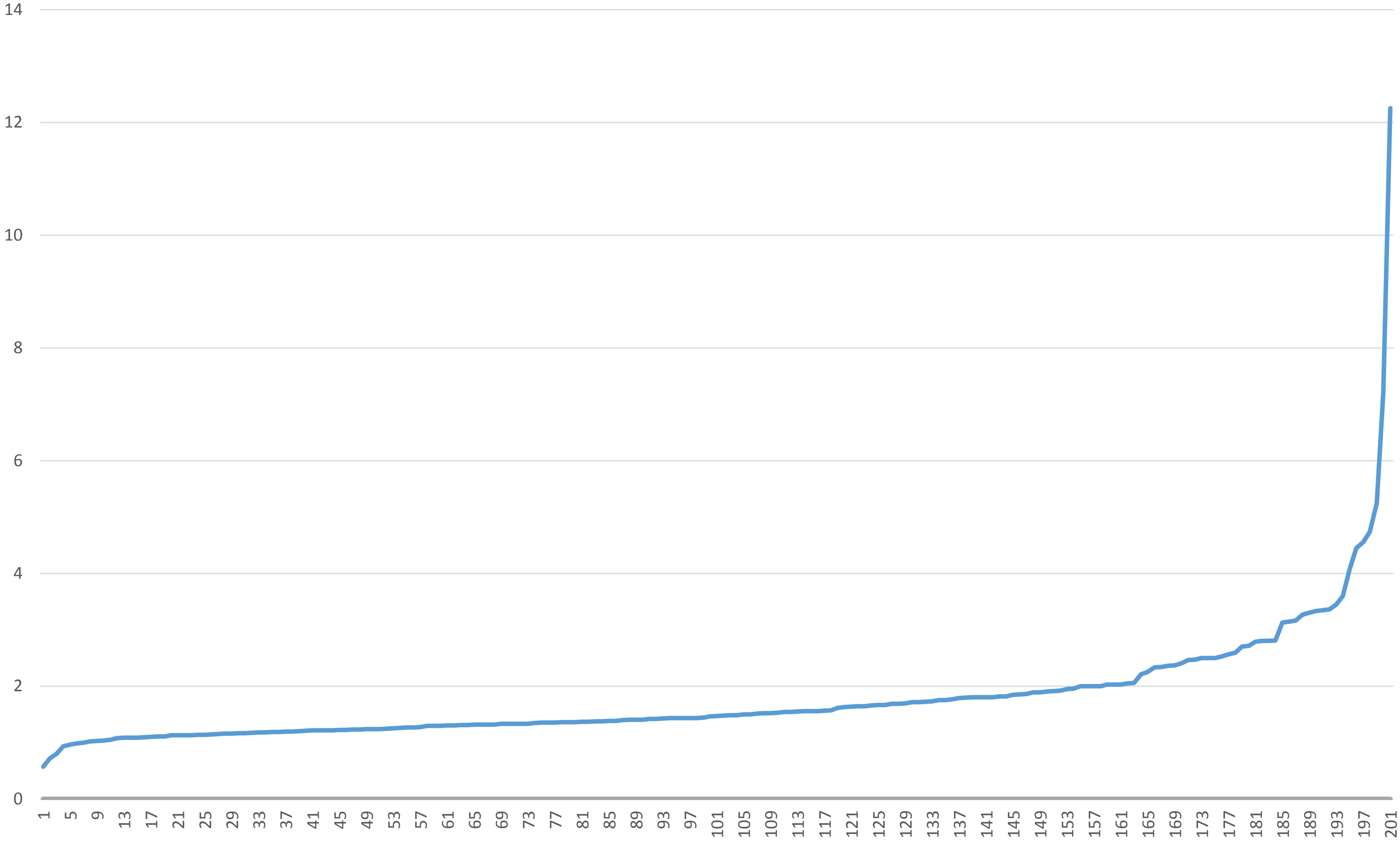
Most Encrypted

1. Cuba
2. Italy
3. Singapore
4. Guyana
5. Jersey

Least Encrypted

197. Saint Kitts
198. Egypt
199. Syria
200. Saint Vincent
201. Seychelles

Unencrypted vs Encrypted (POP)



Unencrypted vs Encrypted (POP)

Most Encrypted

1. Dominica
2. Antarctica
3. South Sudan
4. Turkmenistan
5. Myanmar

Least Encrypted

197.Botswana

198.Angola

199.South Korea

200.Mali

201.Swaziland

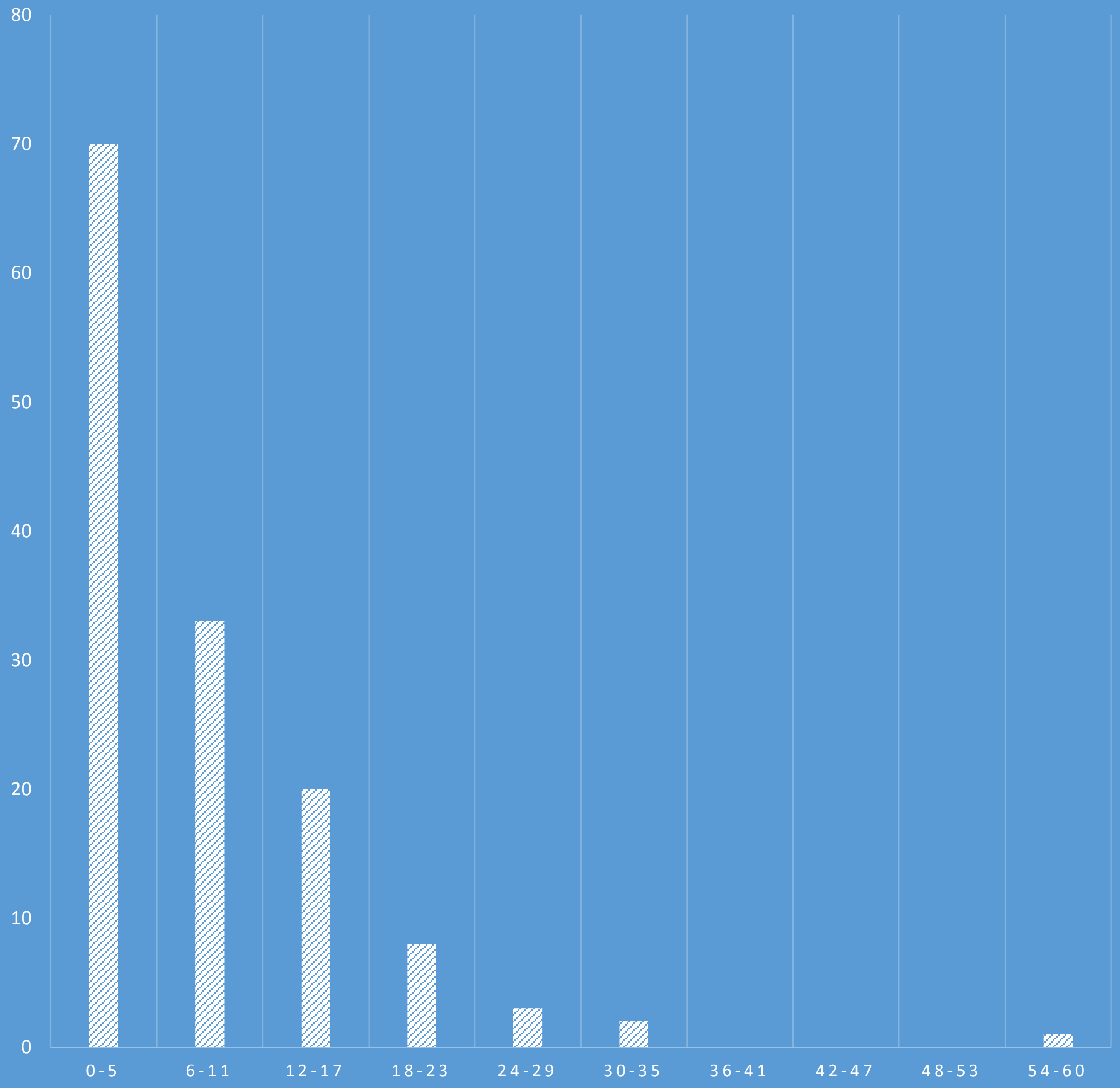
1.3% Novelty Plates

hp
VASES - TEAPOTS - STRAINERS - BOWLS - POTS - AND MORE
Greene Leaf Gift Haus
LOCATED IN THE MALL IN THE HISTORIC DEPOT DISTRICT - STORE #231

Universities Needing Toner

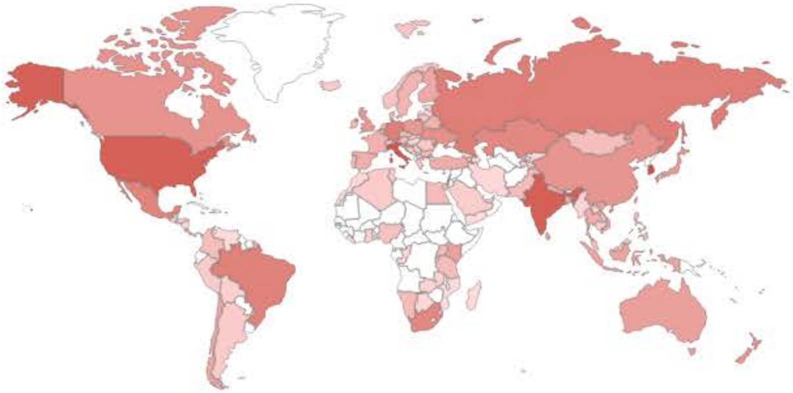
#1	Minnesota	89
#2	Hawaii	75
#3	Austin	60
#4	San Francisco	60
#5	Toronto	56
#6	Santa Cruz	55
#7	South Florida	55
#8	Boston	55
#9	Washington	54
#10	Pennsylvania	48

NUMBER OF TURBINES



Open BGP

Search for port:179 open returned 119,548 results on 15-06-2016



Top Countries

1. Korea, Republic of	26,065
2. Italy	19,932
3. India	14,802
4. United States	14,205
5. Russian Federation	4,549
6. Germany	4,446
7. Brazil	3,890
8. Mexico	3,529
9. South Africa	2,939
10. Kazakhstan	2,833

Recursive DNS

Search for port:53 recursion enabled returned 3,636,849 results on 15-06-2016

Top Countries

1. China	1,141,763
2. Taiwan, Province of China	
3. United States	255,129308,662
4. Korea, Republic of	255,000
5. Russian Federation	174,062
6. India	164,970
7. Brazil	158,099
8. Turkey	98,795
9. Japan	59,360
10. Italy	46,037

<10 Abuse Emails

(for ICS/ IoT)

Questions?