

Digital Leviathan

Nation-State Big Brothers (from huge to little ones)

Eduardo Izycki and Rodrigo Colli

Las Vegas, August 11th 2018

AGENDA

- INTRO
- SOURCES
- OUTCOMES
- CONCLUSION

INTRO

INTRO

“We should give our obedience to an unaccountable sovereign otherwise what awaits us is a ‘state of nature’ that closely resembles civil war – a situation of universal insecurity”.

Thomas Hobbes

?

The claim

Terrorism, cybercrime, foreign espionage, among other are examples that support politicians claims for increase state power over online life.

!

Opposing evidence

The current use of cyber offensive tools are aimed to political objectives rather than public safety

INTRO

1 Espionage

Stealing of information and/or personal data (for achieving political purposes, i.e. opposition party, NGO, ethnic minorities)

2 Surveillance / Eavesdropping

Untargeted violations of privacy (monitoring of behavior, activities, or other changing information of people online)

3 Censorship

Block specific applications or technologies; filtering and blocking of websites; manipulation of content or traffic manipulation; violations of user rights.

SOURCES

SOURCES

1 APT Reports

- *Total of 758 reports/blog posts from vendors, NGO, CSIRT and universities,*
- *The dataset has bias from a western perspective (close to 80%)*

- *Focus on attacks targeting NGO, political groups, media outlets, or opposition was considered as an indicator of state misbehavior*

2 Leaks from spyware providers

- *Two big providers of surveillance solutions Hacking Team and Gamma Group,*
- *Data is available from multiple sources (Wikileaks has a good search platform)*

- *It was possible to identify who acquired it (LEA, military, intelligence, etc)*

3 Acquisition of technology

- *Surveillance and/or intrusion technologies reported from multiple sources*
- *Purchases made by different countries (potential cyber capabilities)*

- *Buggedplanet.info and Surveillance Industry Index (SII) were helpful sources*

SOURCES

4 Censorship

- *Freedom House, OONI, Google, Reporters without Borders and OpenNet provide evidence of some level online censorship,*
- *Blocking applications, technologies, traffic; filtering and blocking of websites; violations of user rights*

- *Based on a western view of freedom of speech (an individual or a community to articulate their opinions and ideas without fear of retaliation, censorship or sanction)*

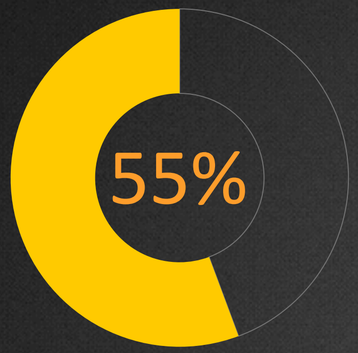
5 Transparency Reports

- *Transparency Reports issued by major social networks and content providers*
- *Facebook, Twitter, Google, Yahoo, Apple, LinkedIn, Snapchat, Tumblr, Dropbox, Wiki,Microsoft, and WordPress*

- *Provides extra detail on the intent of Nation-States use of social media for surveillance*

OUTCOMES

OUTCOMES – STATE CYBER ATTACK



Documents had some level of attribution



Single APT Groups and/or Campaigns



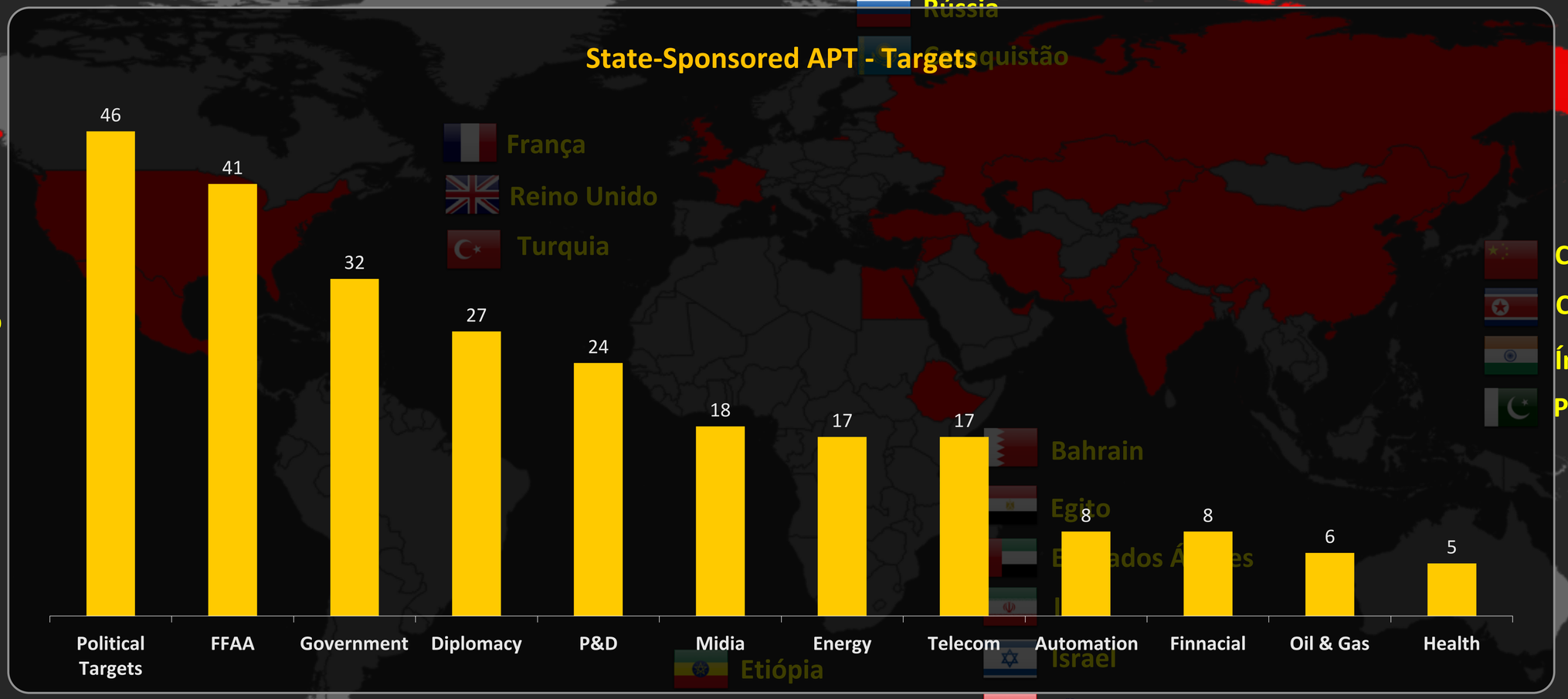
Considered state-sponsored attacks



Countries attributed with a state-sponsored APT

\+ Extensive use of Python3 (NLTK) and regular expressions for processing documents / posts

OUTCOMES – STATE CYBER ATTACK



Rússia

Paquistão

França

Reino Unido

Turquia

EUA

México

China

Coreia do Norte

Índia

Paquistão

Bahrain

Egito

Etiópia

Israel

Líbano

Síria

STATE SPONSORED APT

Legenda

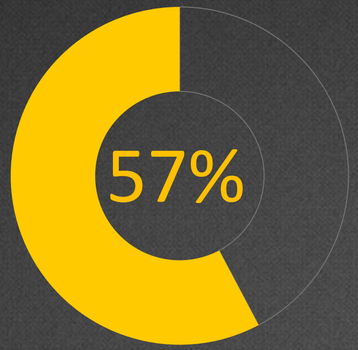
STATE SPONSORED

N/A

OUTCOMES – CYBER OFFENSIVE CAPABILITIES

71

Countries acquired offensive solutions from private vendors



In 41 cases it was possible to identify the user/buyer

19

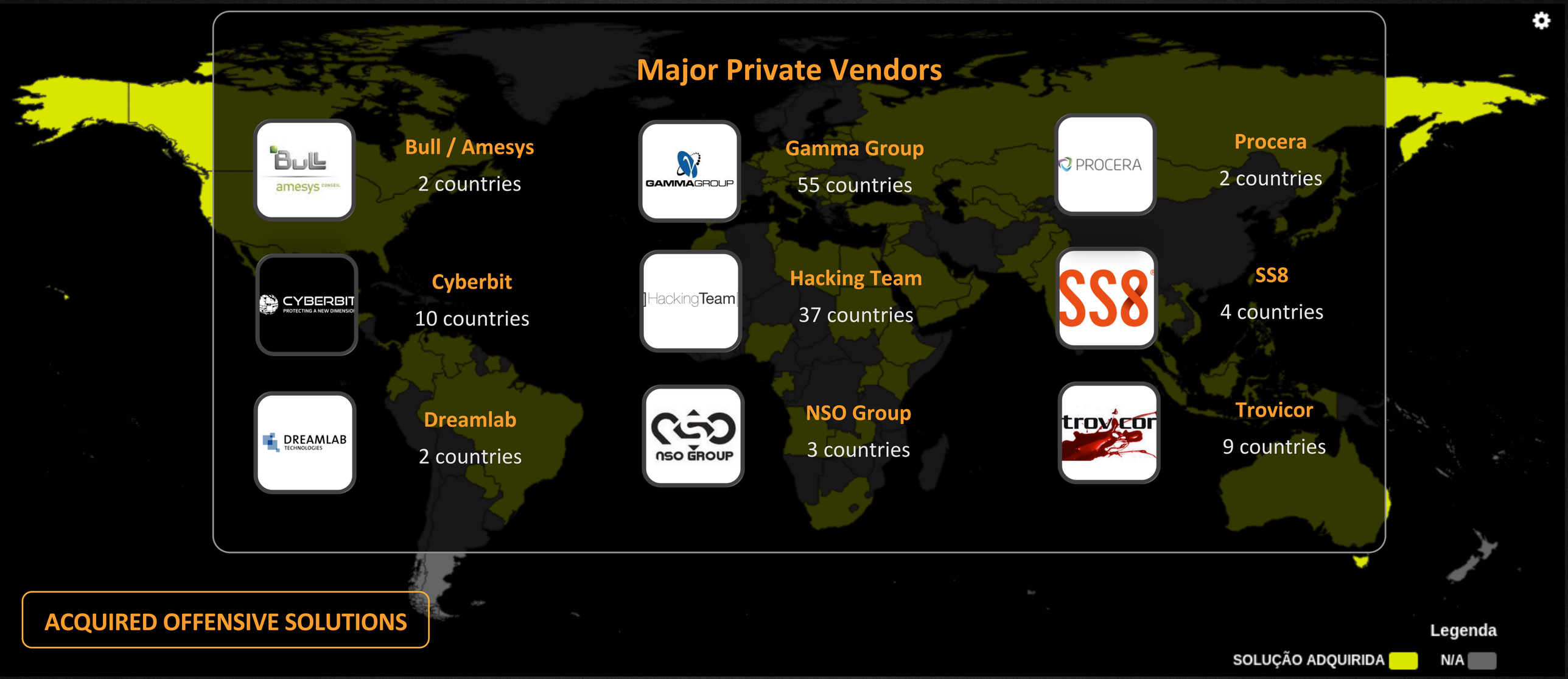
User/buyer was an intelligence agency and/ or armed forces

29

Countries that acquired more than one offensive solution

\+ Wikileaks' search platform, Buggedplanet.info, Surveillance Industry Index, and reports from Citizen Lab / Privacy International / Freedom House

OUTCOMES – CYBER OFFENSIVE CAPABILITIES



OUTCOMES – CYBER OFFENSIVE CAPABILITIES

Users / Buyers



Saudi Arabia
GIP / GID / MD



Spain
CNI



Mongolia
SSSD



Singapore
IDA SGP



Azerbaijan
Azerbajan NS



Hungary
SSNS



Malasya
MACC / MALMI / PMO



Thailand
Royal Thai Army



Bangladesh
(DGFI)



Indonesia
Lembaga Sandi Negara



Oman
Intelligence Agency



Uganda
CMI



Cyprus
Intelligence Agency



Kenya
NIS



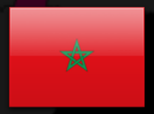
Panama
Presidency Cabinet



Uzbequistan
NSS



Ecuador
SENAIN



Marroco
CSDN / DST



Serbia
BIA

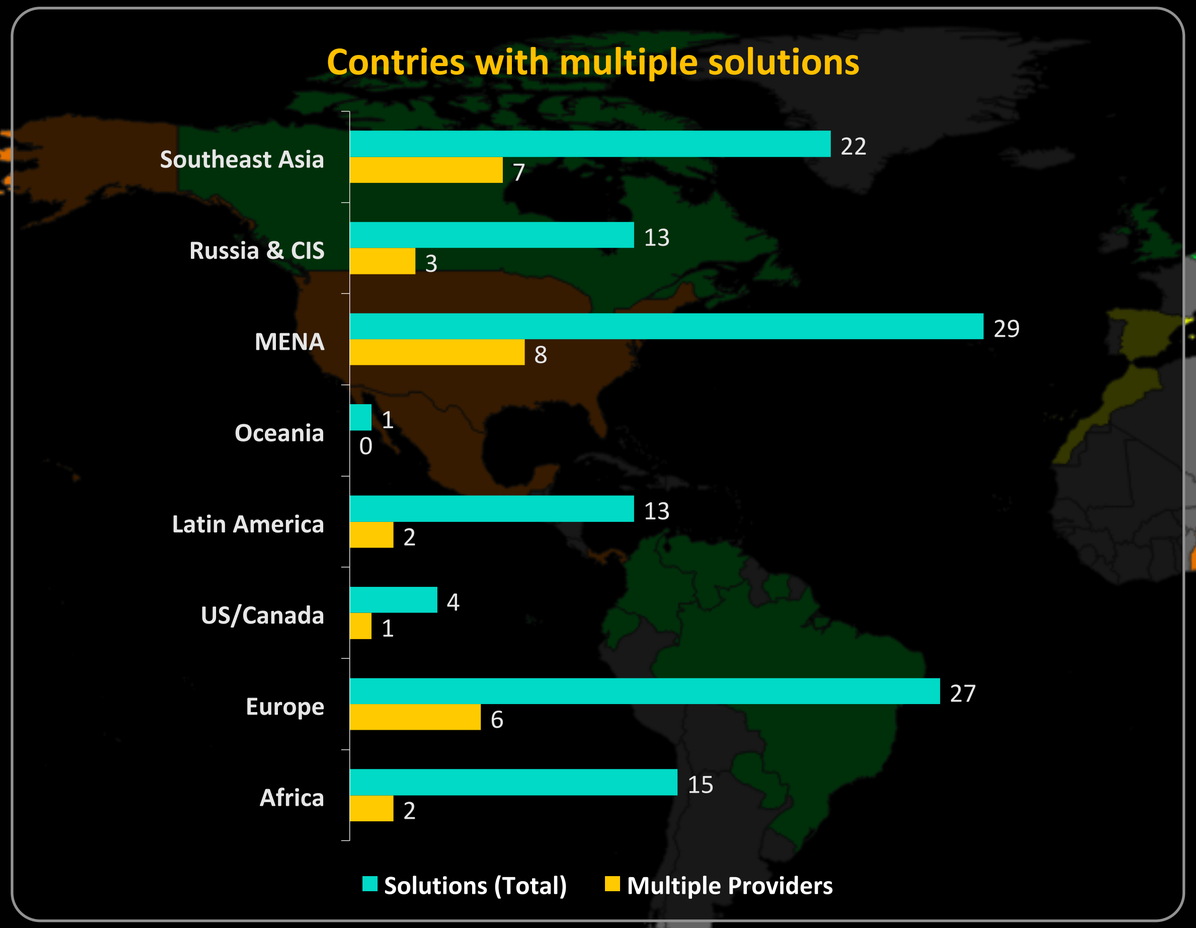
NEW THREATS

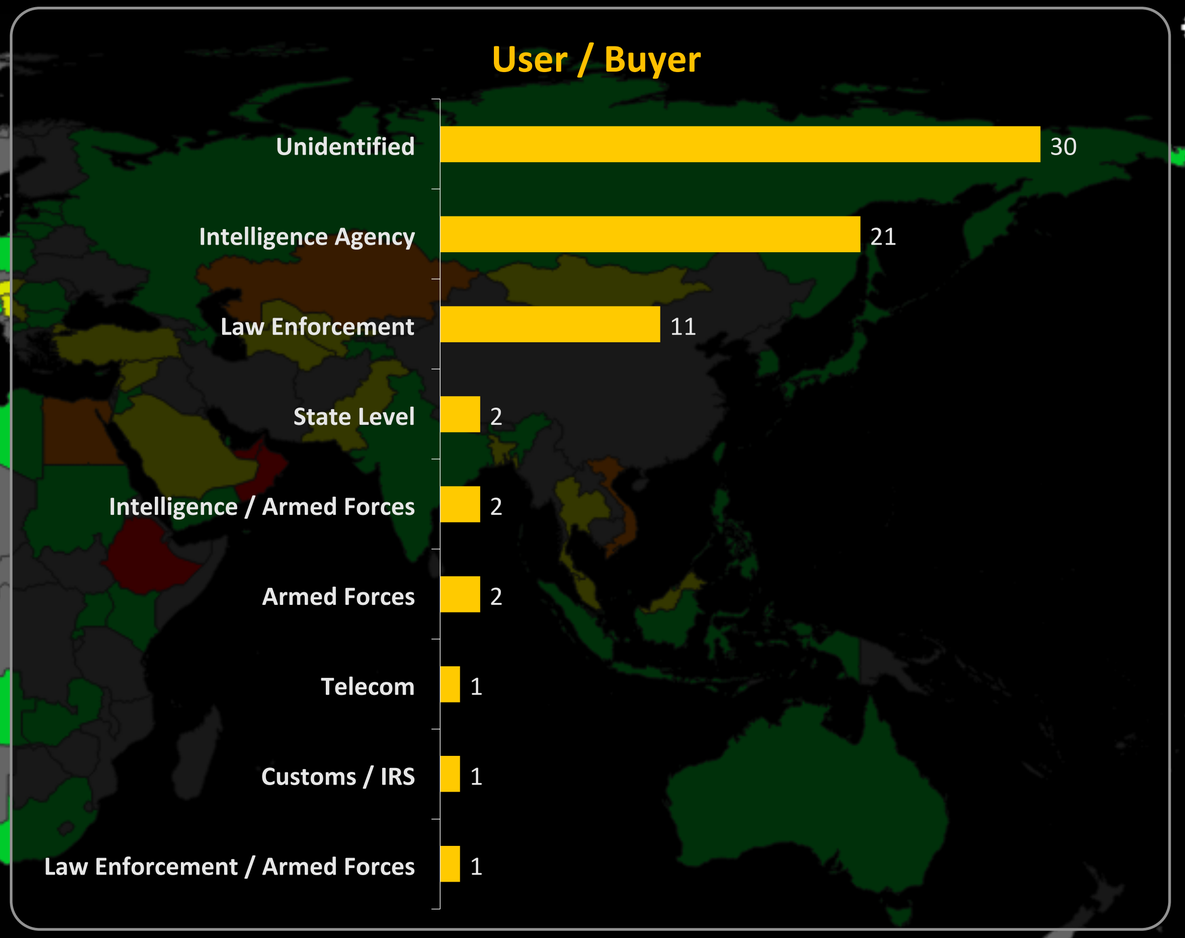
Legenda

NOVA AMEAÇA

N/A

OUTCOMES – CYBER OFFENSIVE CAPABILITIES





MULTIPLE OFFENSIVE SOLUTIONS

Legenda

UMA SOLUÇÃO | DUAS SOLUÇÕES | TRÊS SOLUÇÕES | QUATRO SOLUÇÕES | N/A

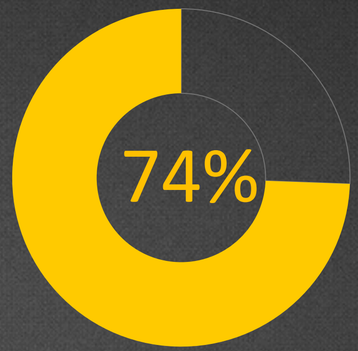
OUTCOMES - CENSORSHIP



Countries with evidence of online censorship



Countries with evidence of some level of internet shutdown



In 32 countries the shutdown reached national level

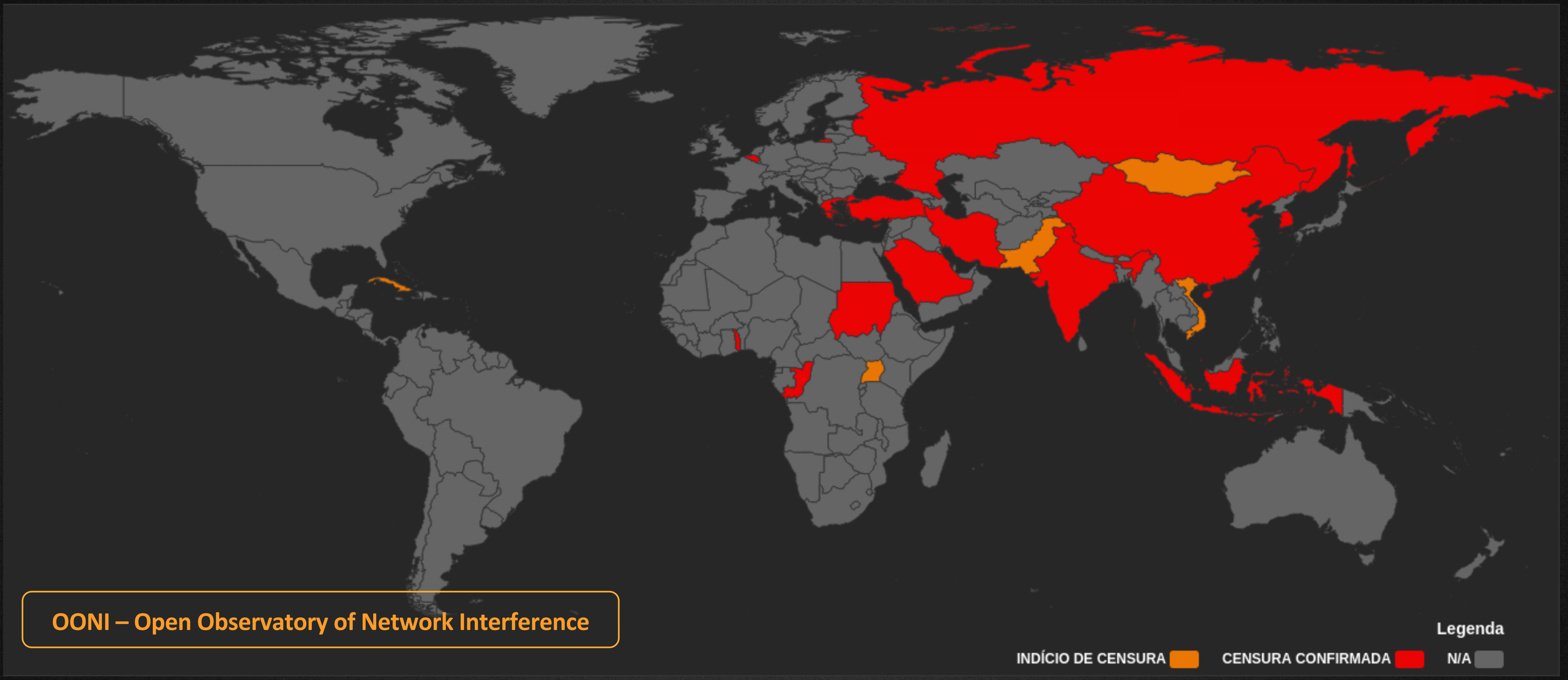


Countries with evidence from two or more sources

\+

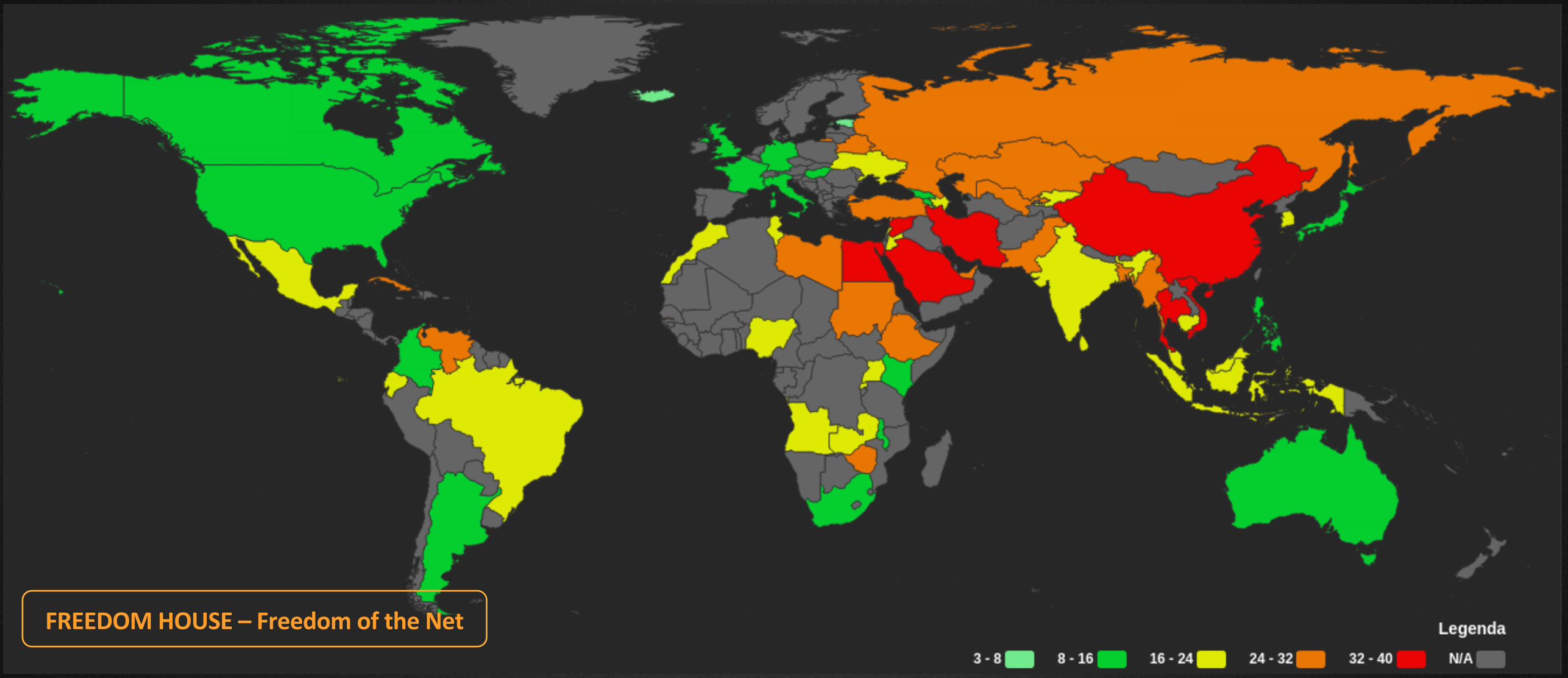
Reports from *Freedom House, OONI, Google, Reporters without Borders and OpenNet Initiative*

OUTCOMES - CENSORSHIP



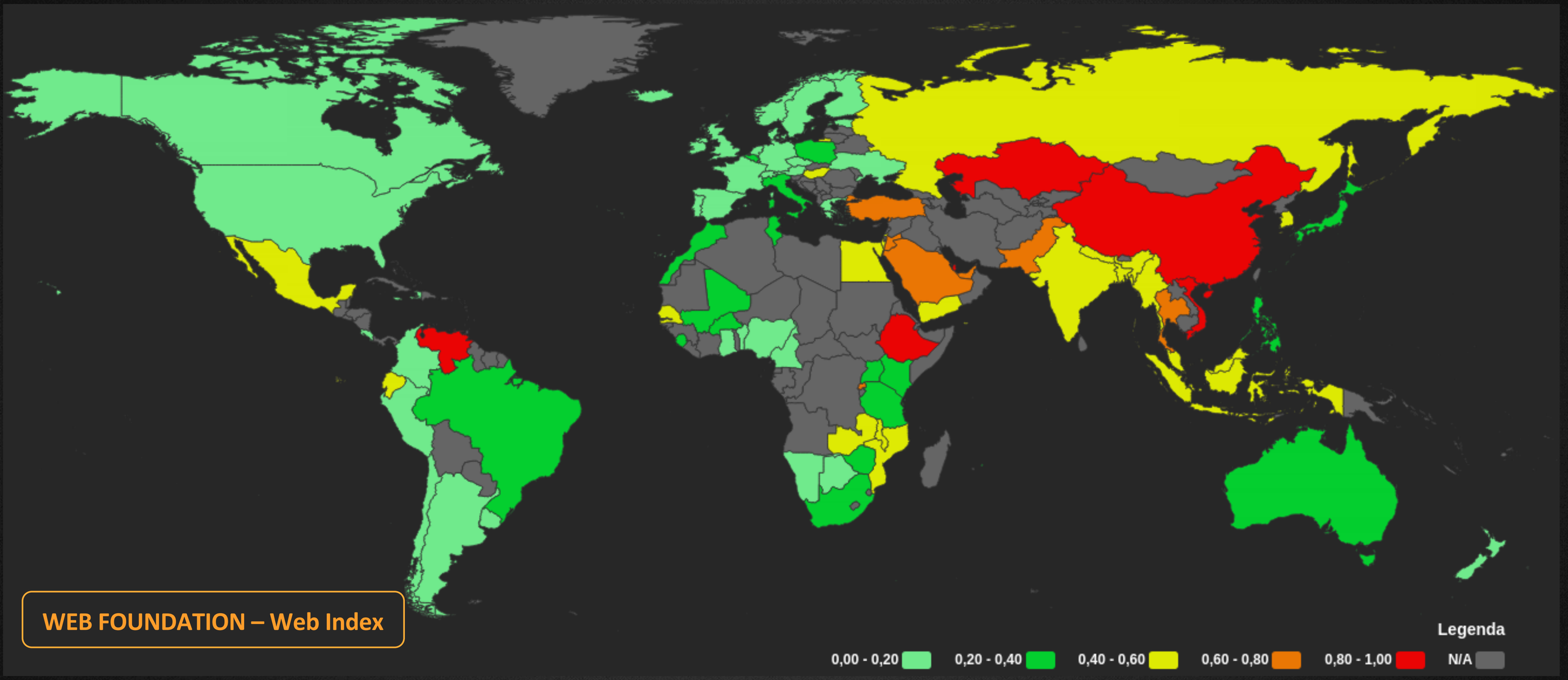
OONI – Open Observatory of Network Interference

OUTCOMES - CENSORSHIP



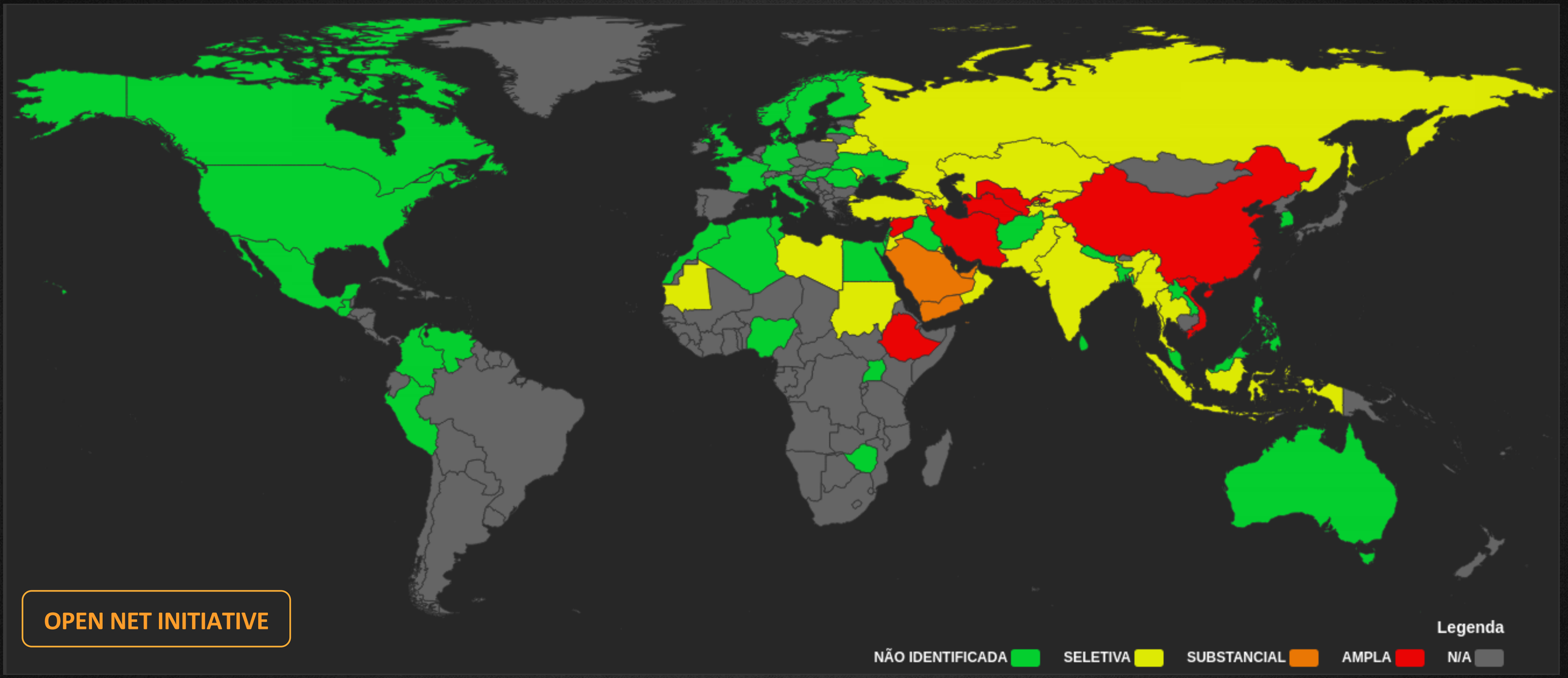
FREEDOM HOUSE – Freedom of the Net

OUTCOMES - CENSORSHIP



WEB FOUNDATION – Web Index

OUTCOMES - CENSORSHIP



OPEN NET INITIATIVE

OUTCOMES - CENSORSHIP

#OpStopBlocking – Brazil 2016







Censorship and Shutdowns – Multiple Sources

Saudi Arabia
All sources

China
All sources

Vietnam
All sources

Bahrain
4 sources

Turkey
4 sources

Pakistan
4 sources

Iran
4 sources

Ethiopia
4 sources

United Arab Emirates
3 sources

ACCESSNOW.ORG – SHUTDOWN TRACKER

Legenda

1 - 32 | 32 - 64 | 64 - 95 | 95 - 127 | 127 - 159 | N/A

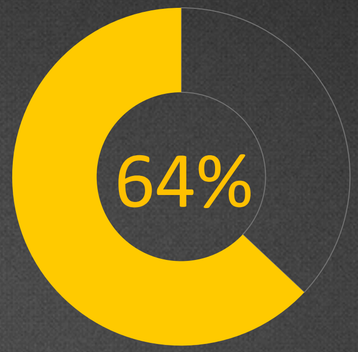
OUTCOMES – TRANSPARENCY REPORTS

70

Companies worldwide publish transparency reports

10

Major content providers covered in this analysis



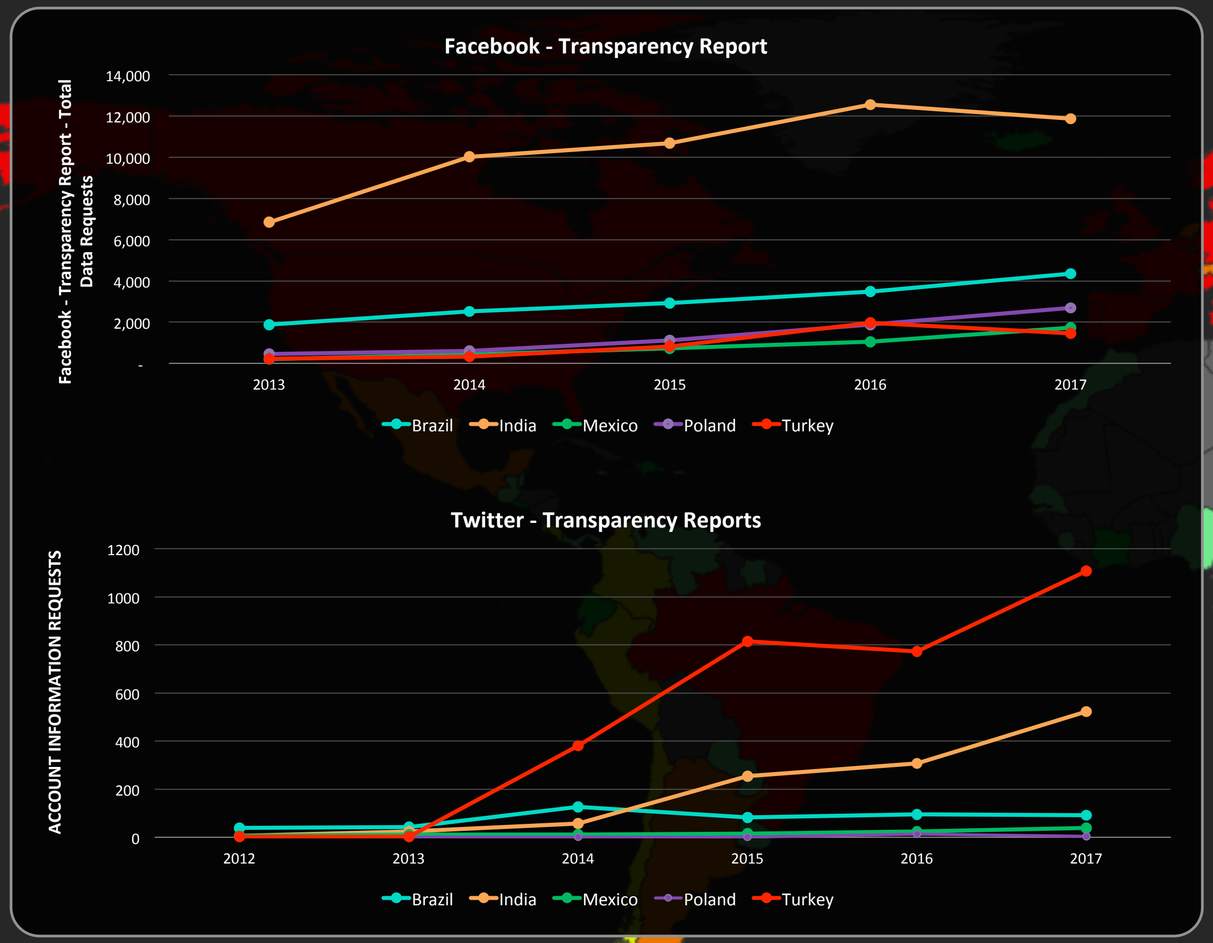
World average requests where some data was produced (2017)

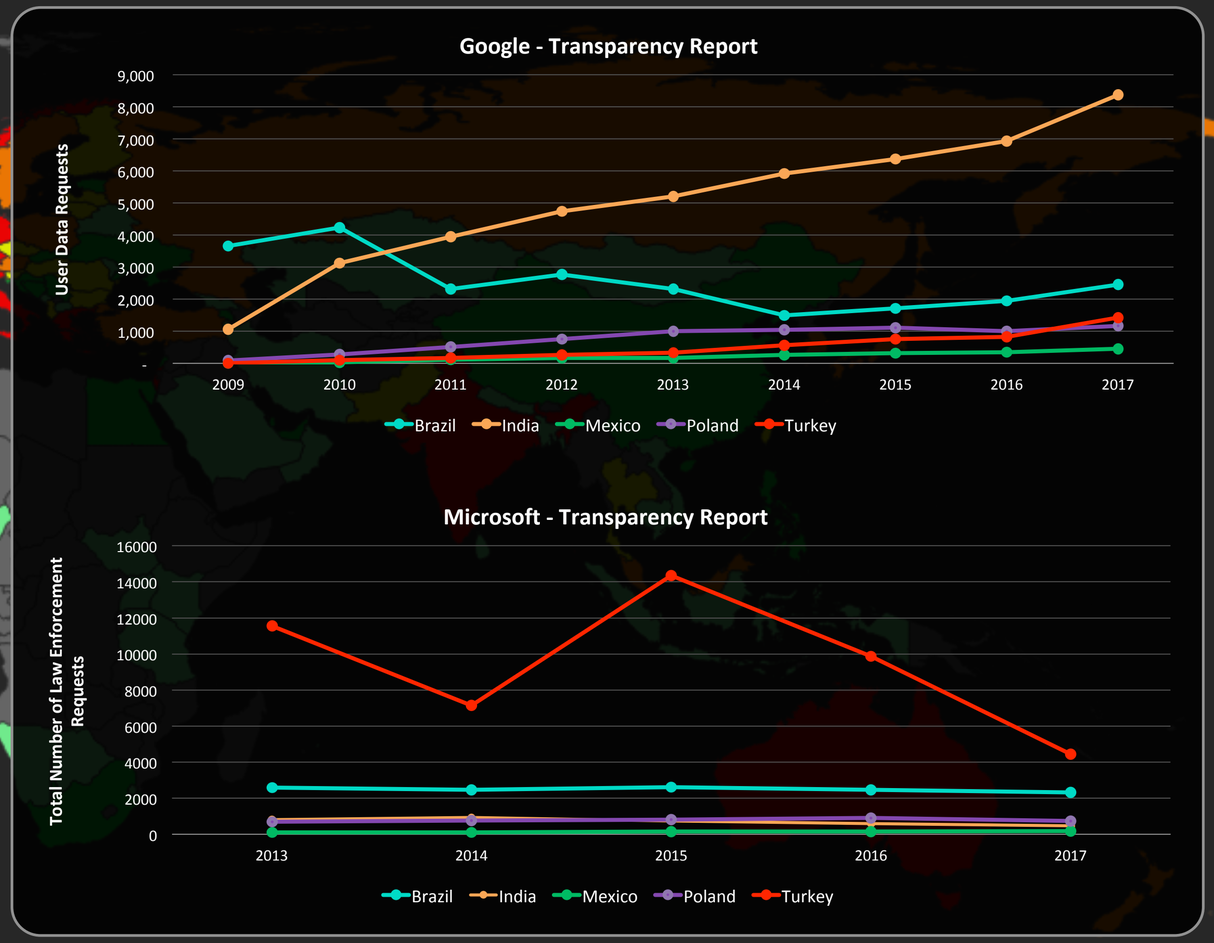
125

Countries have requested information or to remove content

\+ Most transparency reports data are available in csv/json formats, unfortunately some only PDF

OUTCOMES – TRANSPARENCY REPORTS



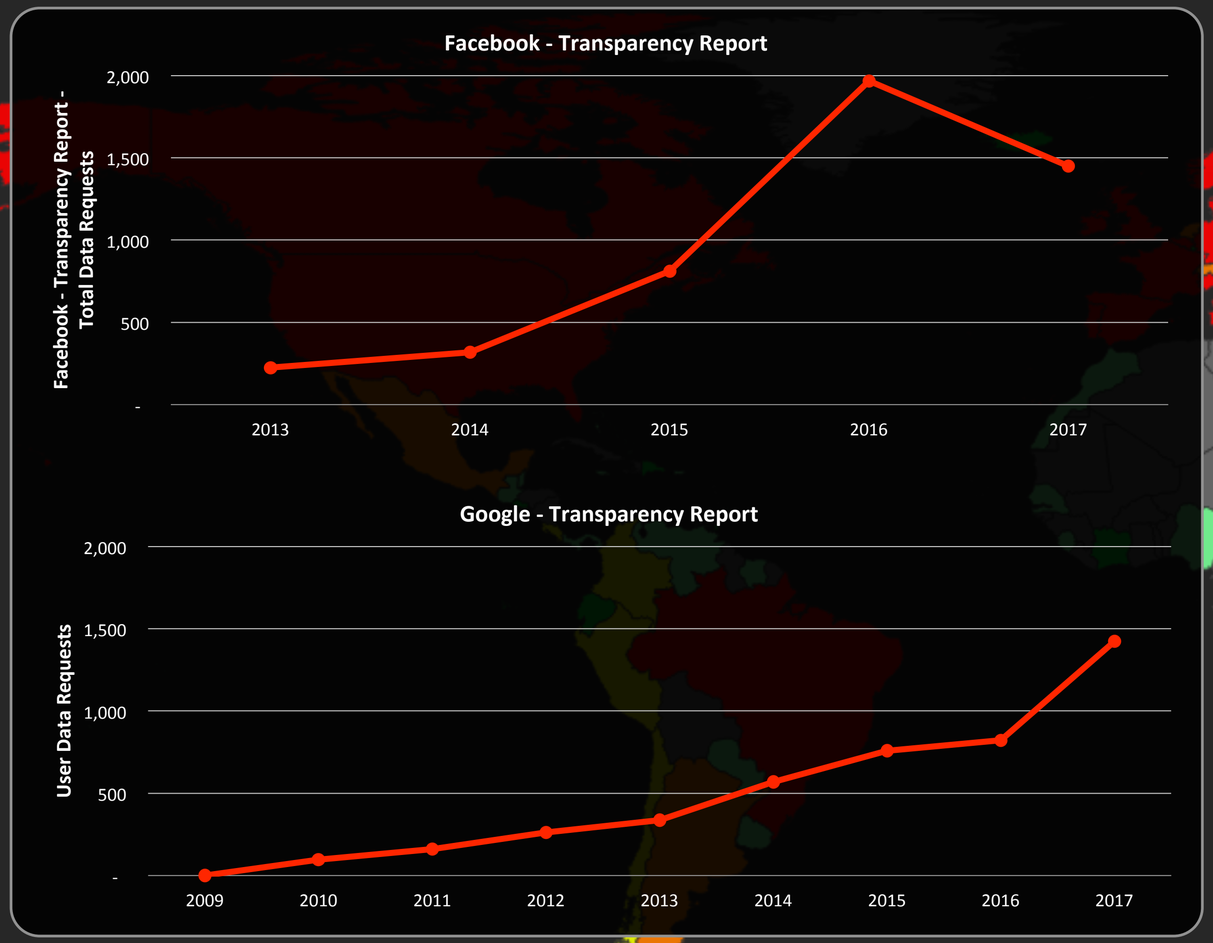


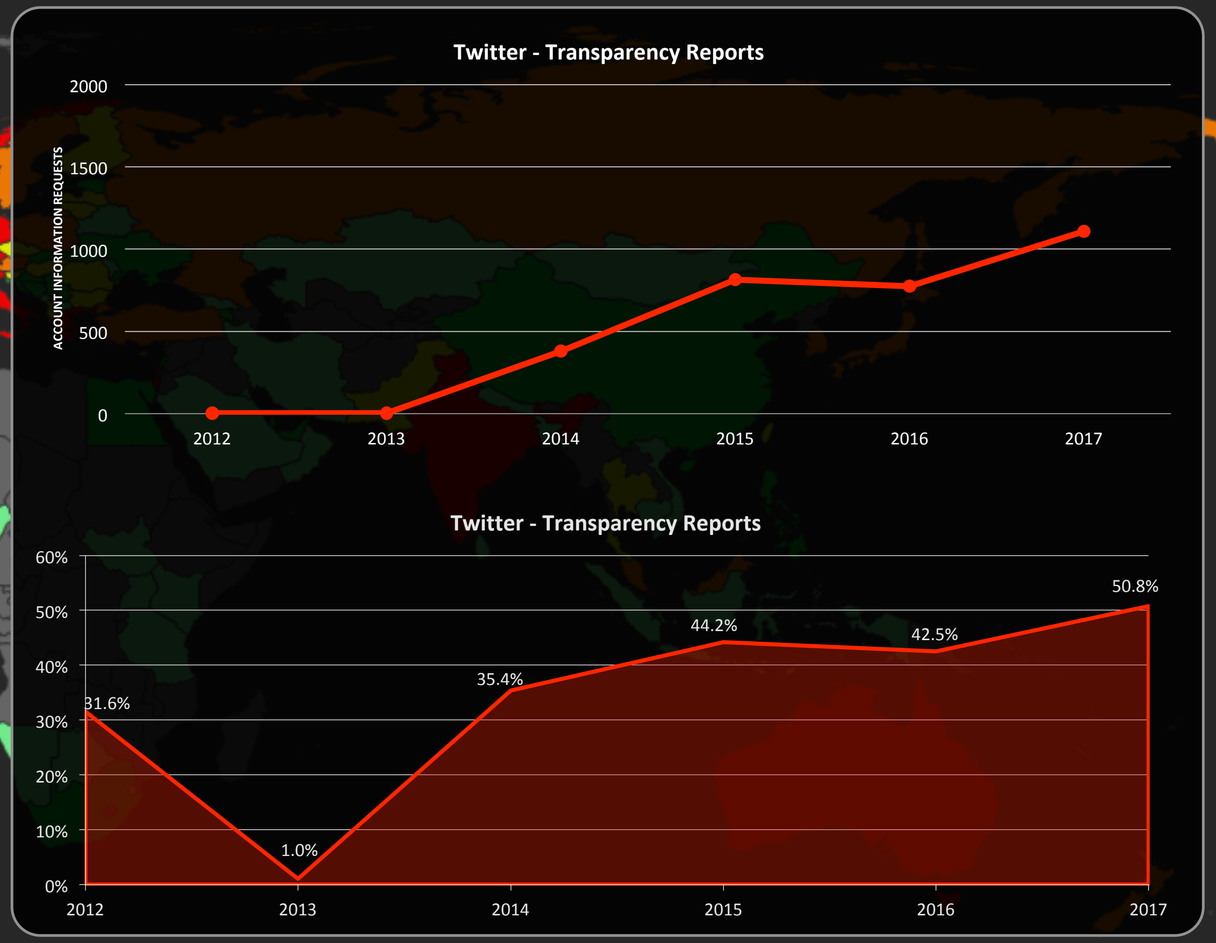
Transparency Reports

Legenda

1 - 2 | 2 - 4 | 4 - 6 | 6 - 8 | 8 - 10 | N/A

OUTCOMES – TRANSPARENCY REPORTS





Transparency Reports - Turkey

Legenda

1 - 2 | 2 - 4 | 4 - 6 | 6 - 8 | 8 - 10 | N/A

CONCLUSION

CONCLUSION

1

Cyber offensive tools being used against political targets

85 countries attacked and/or possess cyber weapons

There are evidence that 19 countries were attributed as authors/sponsors of cyber attacks.
Another 18 countries possess cyber weapons with Intelligence Agencies
At last, 34 countries acquired cyber weapons but the user/buyer is not known

All Cyber Offensive Capabilities



92,2% Worldwide

OFFENSIVE CAPABILITIES

Legenda

FFAA | INTELLIGENCE | STATE SPONSORED APT | LEA | CIVILIAN | UNKNOWN | N/A

CONCLUSION

2

Online Censorship and Internet Shutdowns

The two are strongly correlated

Out of 57 countries that engaged in censorship or shutdowns, 26 did both.
Concerning social media such as Facebook, Twitter and Google, all countries have increased its yearly number of requests

Censorship/Shutdowns – Internet Users



56,7 % Worldwide

CENSORSHIP & BLOCKING

Legenda

SOCIAL MEDIA | SHUTDOWNS | BOTH | CENSORSHIP | N/A

Thanks!

Eduardo Izycki

Independent Researcher


linkedin.com/in/eduardoizycki


@dudarthur


eduizycki@protonmail.com