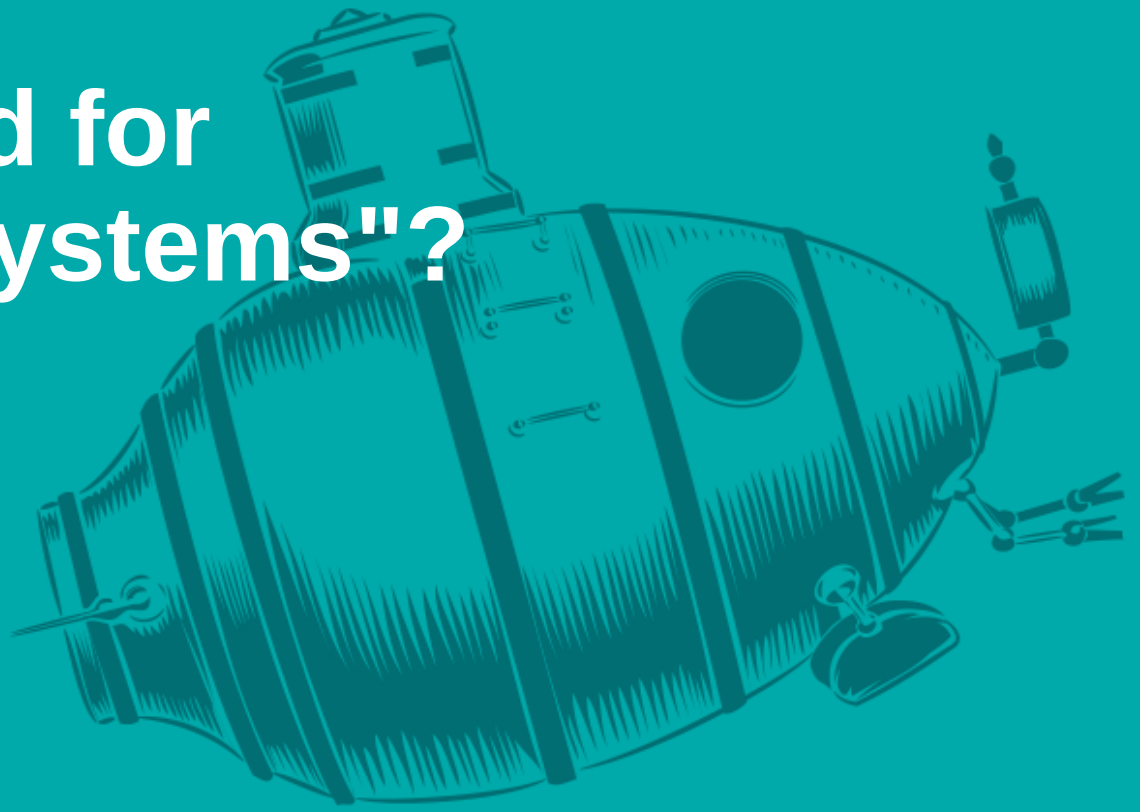
ALEF

Wait, ICS doesn’t stand for "Internet-Connected Systems"?



Jan Kopřiva

jan.kopriva@alef.com | @jak0pr

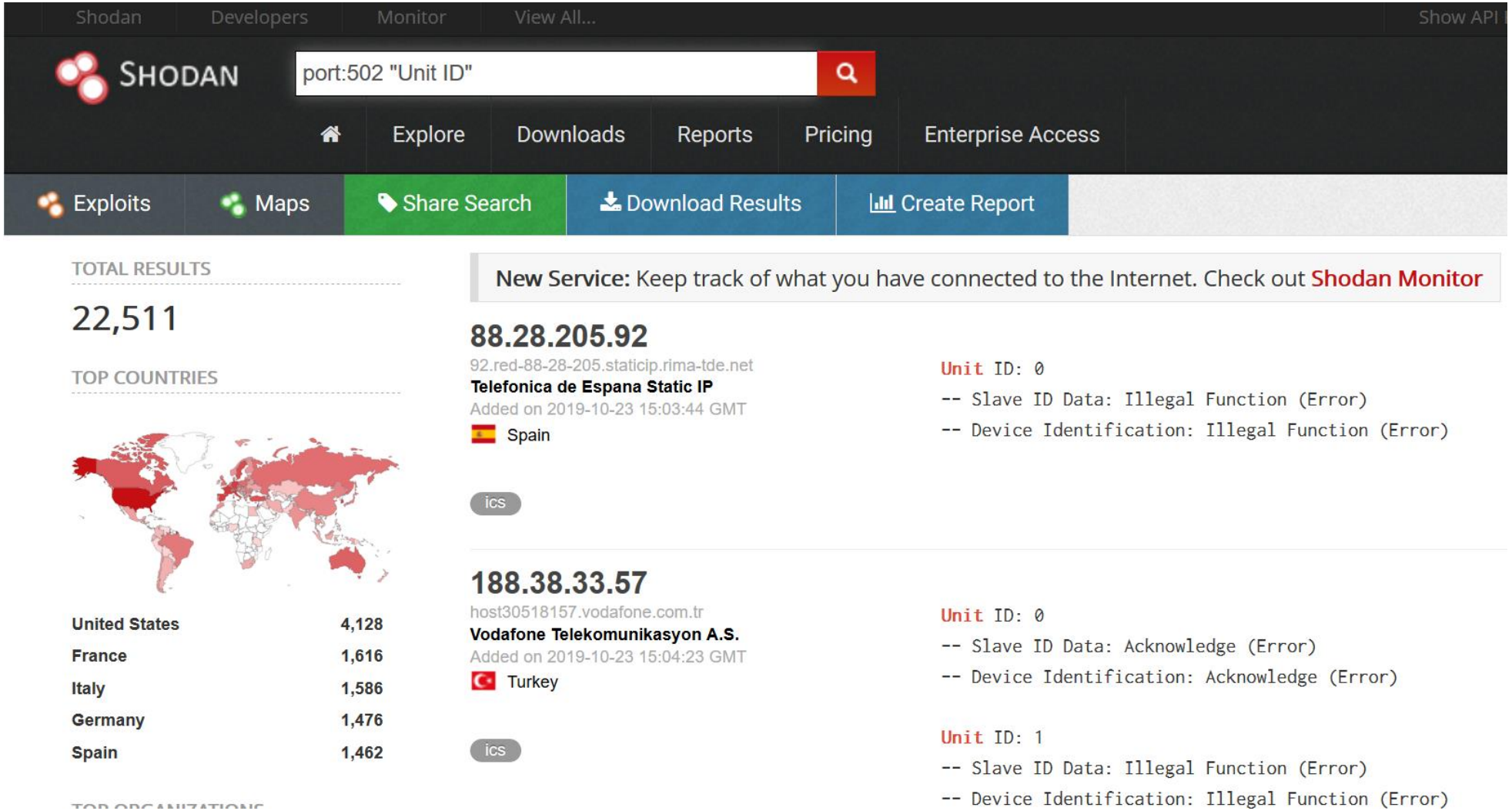
ALEF CSIRT

TLP: WHITE

Are ICS connected to the internet common?

- Only few cases a year make it to mainstream media
- We tend to assume there is a lot more, but very few studies on the topic exist

How would an attacker find connected ICS?



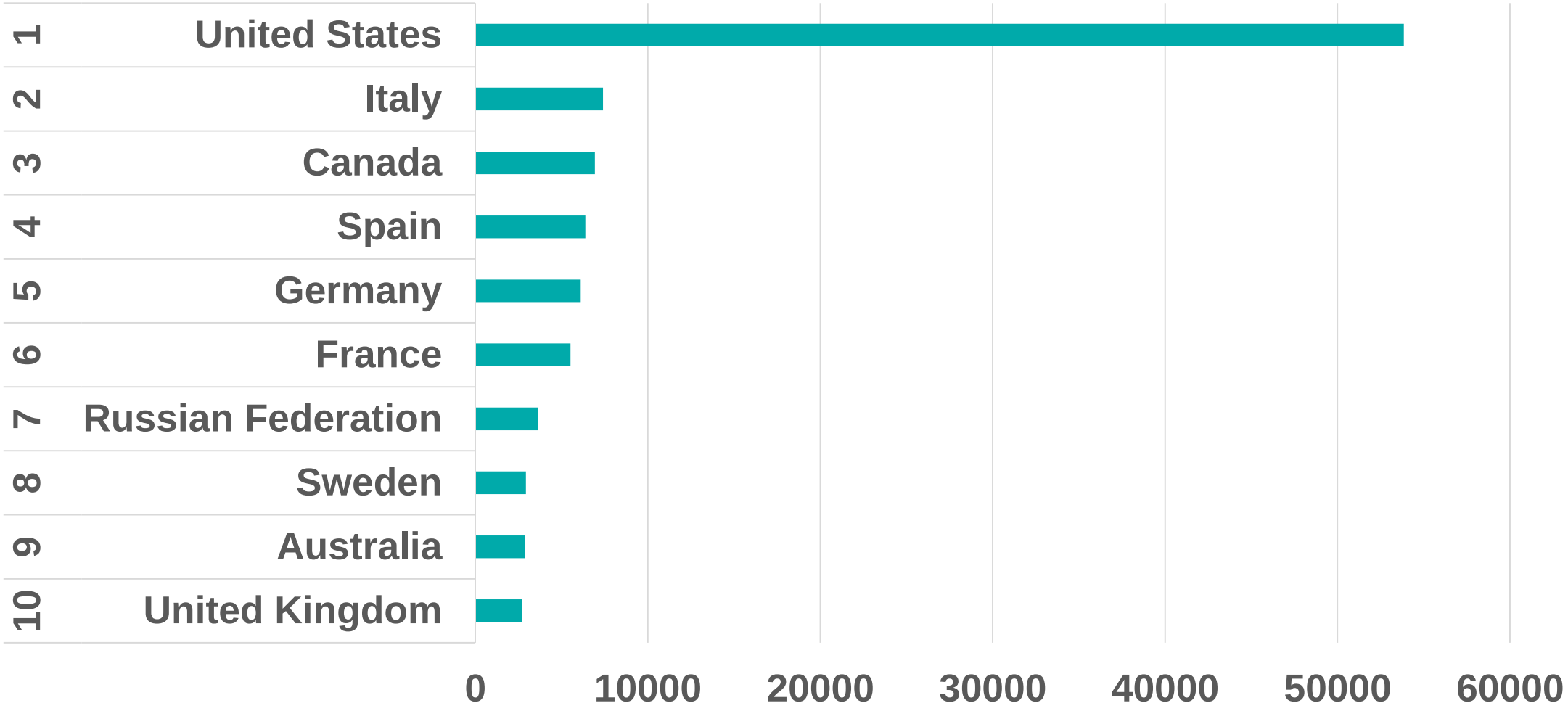
Is ICS connected to the internet dangerous?

- Many industrial protocols lack any security functionalities…
- …so the short answer is „yes“

What did we do?

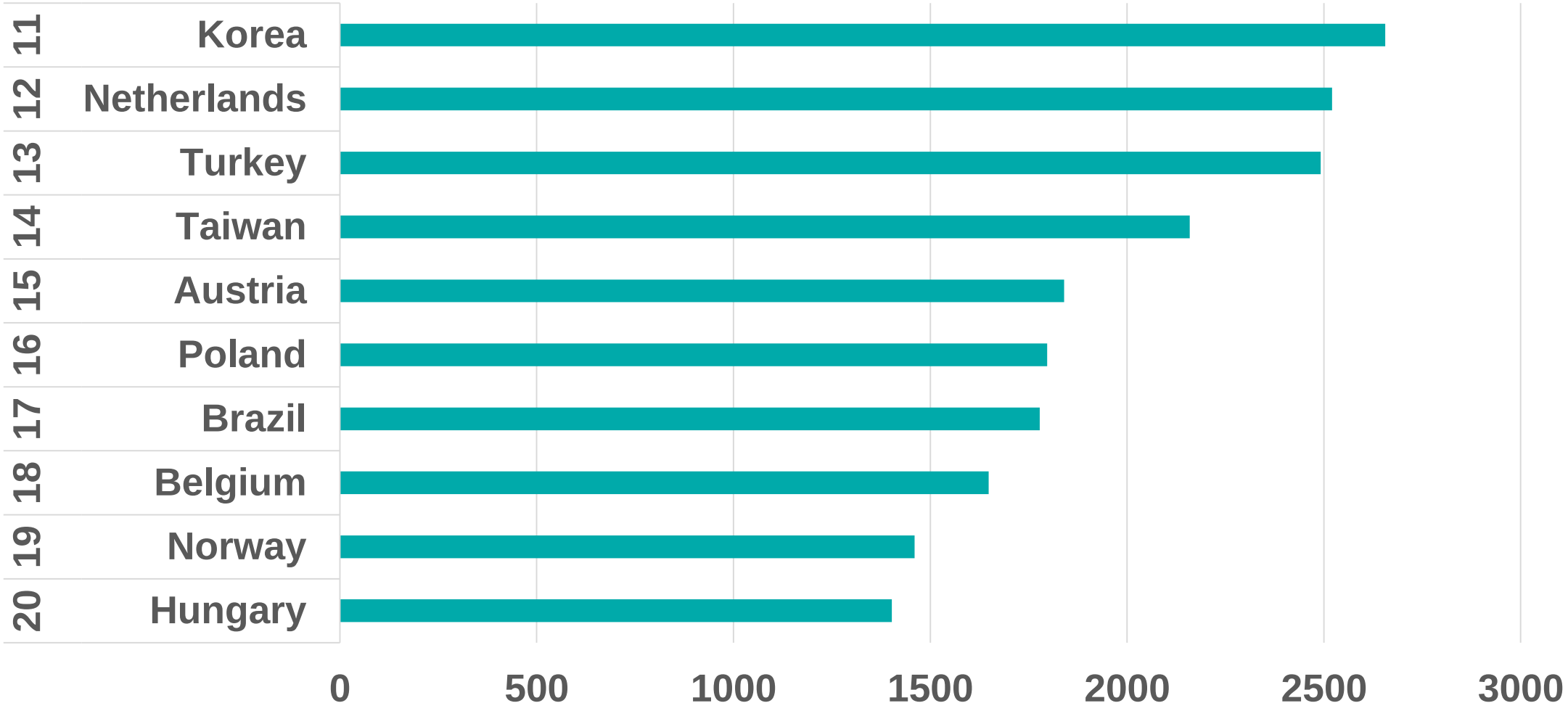
- 21st – 22nd October 2019
- Look at commonly used industrial ports/protocols (mostly using using TriOp toolkit)
- Some limited manual verification of results

How many ICS are out there?



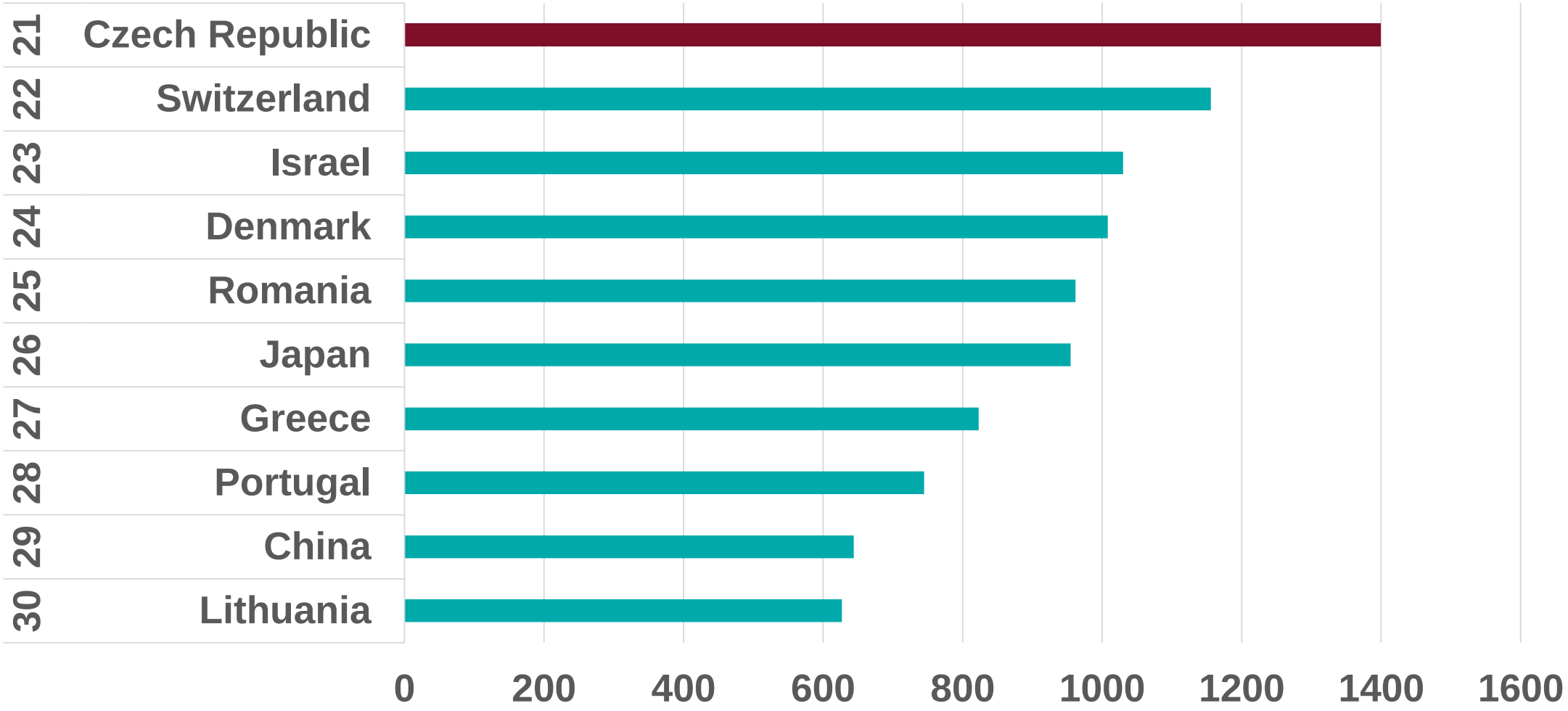
ALEF

How many ICS are out there?



ALEF

How many ICS are out there?

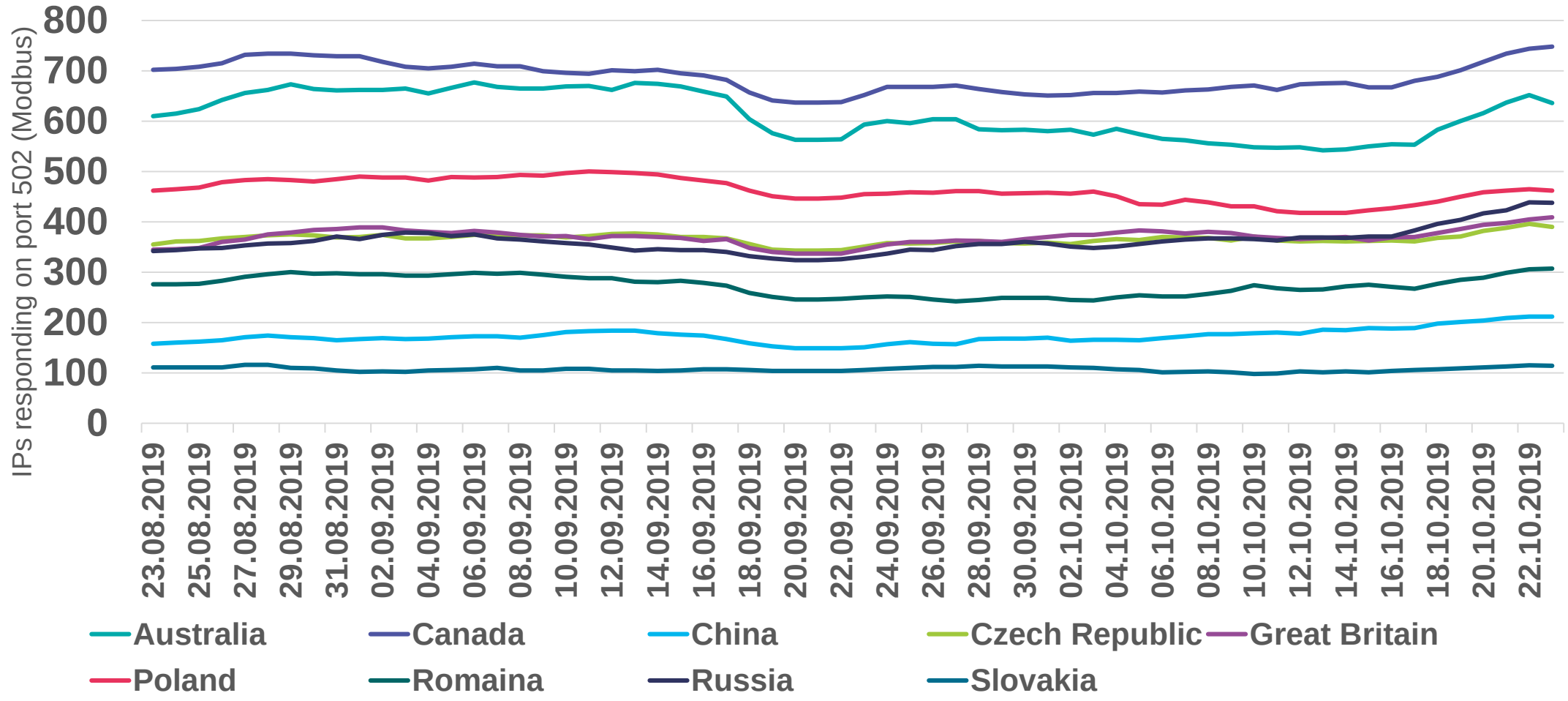


ALEF

That‘s not great…

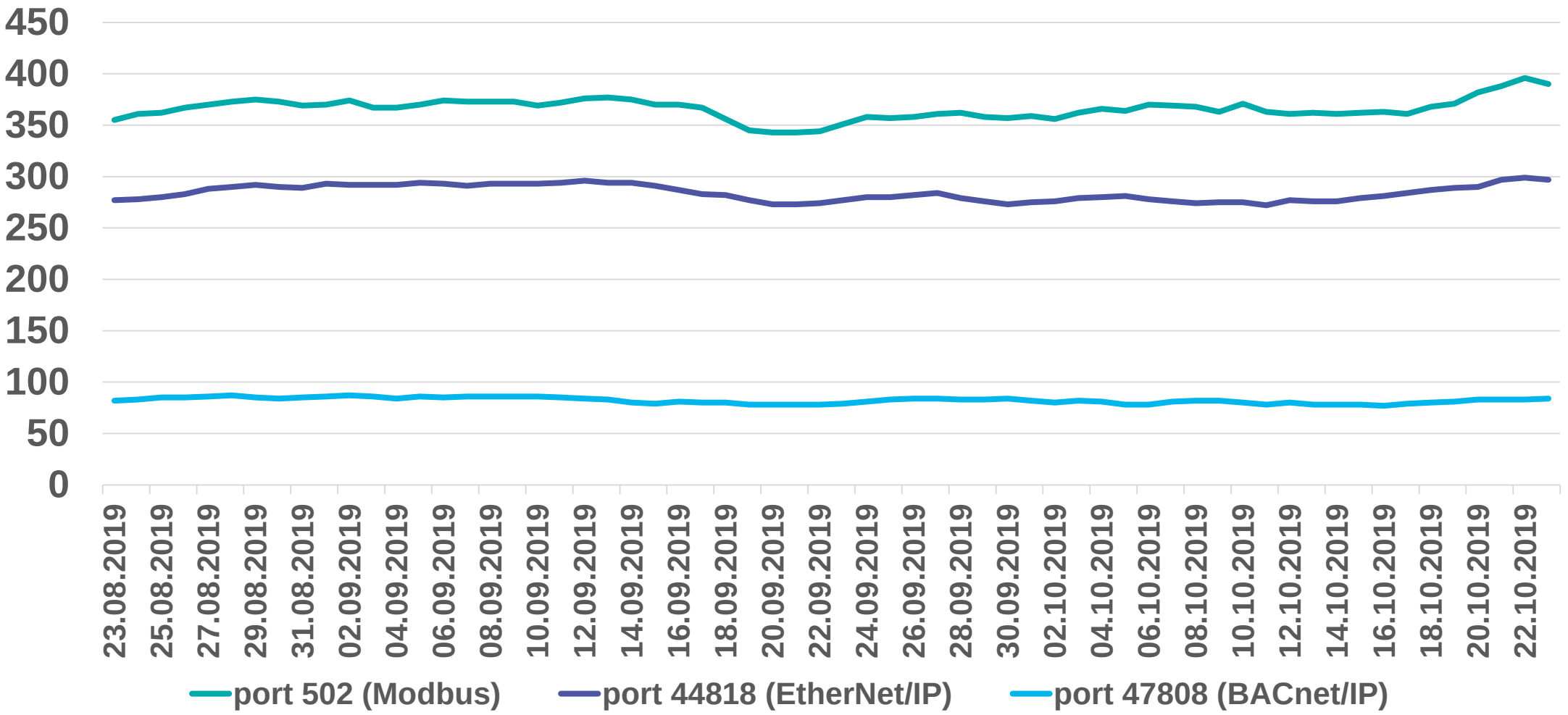
- If Shodan data were representative for all IPs in a country
  - Czech Republic ~ 0,1% IPs
  - Russia ~ 0,03% IPs
  - United States ~ 0,02% IPs
  - China ~ 0,002% IPs

…but is this normal?



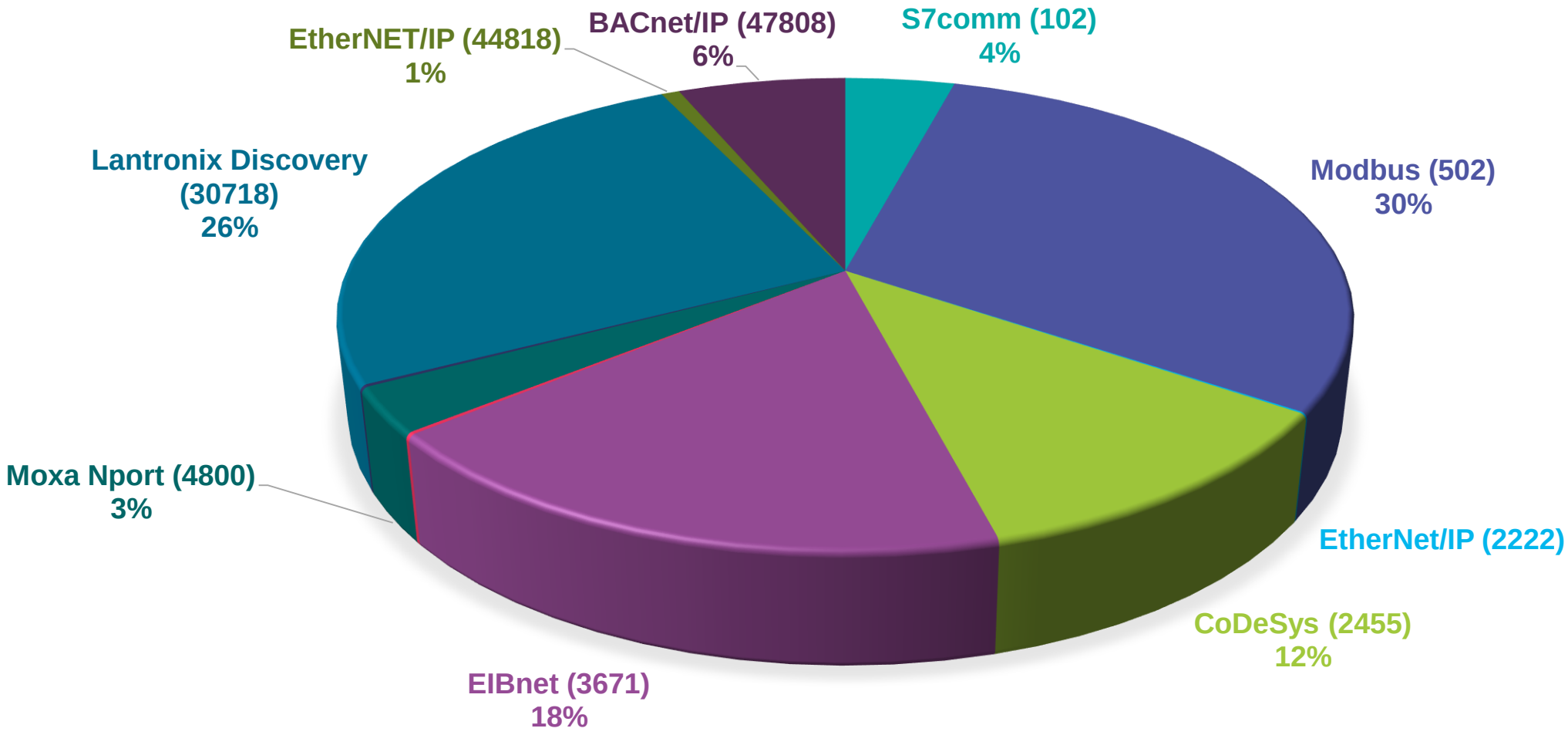
ALEF

Let‘s take a look at the Czech Republic…



ALEF

What is/was out there?



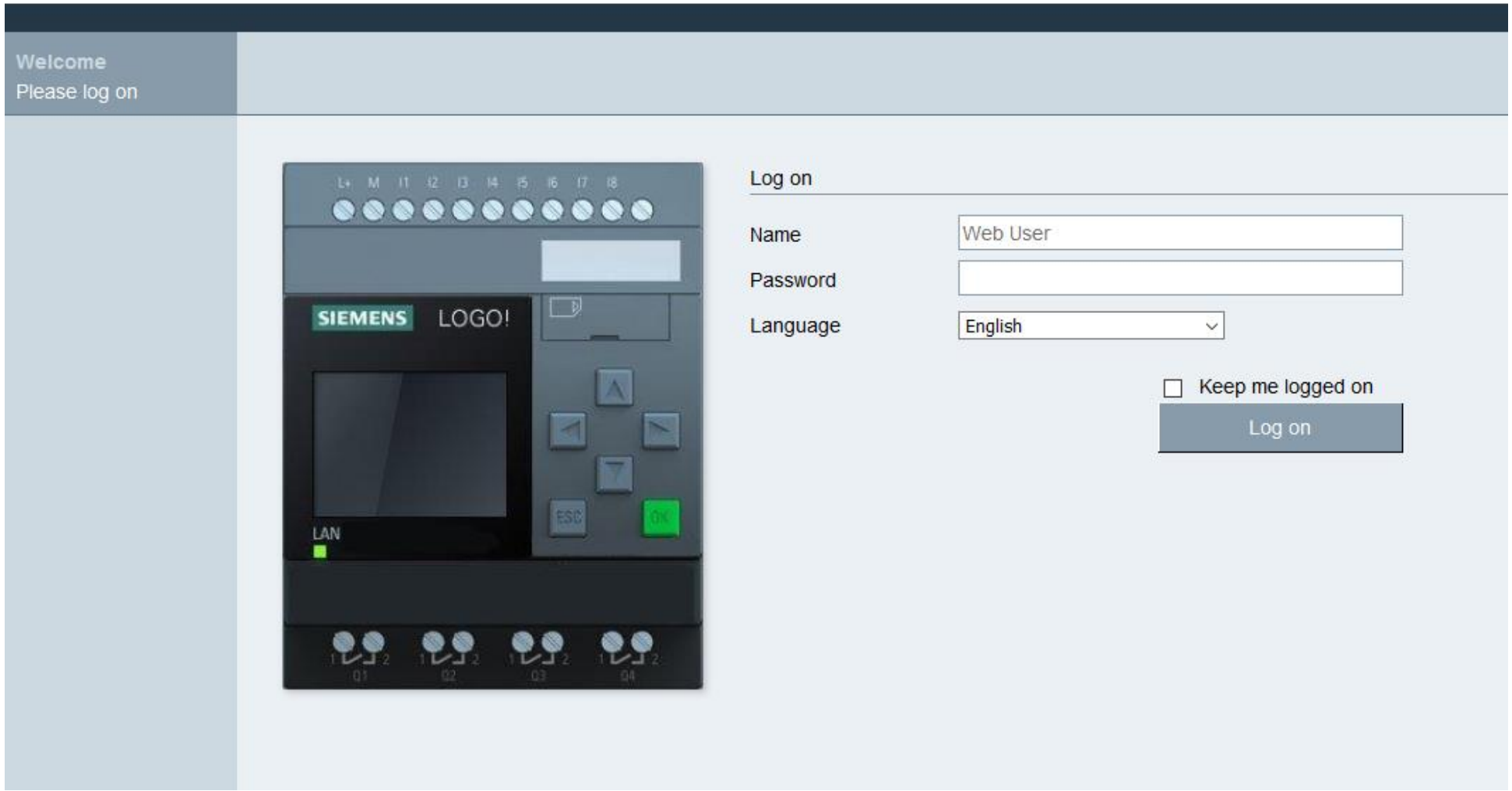
ALEF

What is/was (probably) out there?

- HVAC and temperature controllers
- „Smart“ buildings
- Solar power plants
- Biogas plant
- Local power grid controller
- General use PLCs
- Elevator controller
- Camera systems controller
- Physical security systems
- Industrial processes controllers
- Industrial measuring equipment

Some control panels required authentication…

SIEMENS



ALEF

…others didn‘t

Climatix - BACnet Communication Card
by Siemens Building Technologies

Image Version: 10.30
HW_2.00_20140811_1508

- Server Config
- BACnet Config
- Error Log
- History Log
- deviceRMS Overview
- File Manager
- Process Manager
- Registry Manager

BACnet Config

With this form you can setup the Climatix's BACnet configuration.

Save internal COV-Values | Shutdown BACnetServer | Start BACnet Server

Description	Actual Value
enable BACnet	☑
Language	COM1 (-1, COM1, COM2, 0, 1, 2, 3, ...)
BACnet DeviceID	
BACnet DeviceName	
UDPPort	47808 (Decimal 47808 = BAC0 Hexadecimal...)
Use UniCode	☐
RecipientDevice1	0
RecipientDevice2	0
RecipientDevice3	0

Initial Configuration for BACnet COV Handling

COV File	
Limit <= 1	0.0001
Limit > 1	0.001
Limit > 10	0.1
Limit > 100	0.3
Limit > 1000	1.0
Limit > 10000	3.0

Save all Values

Foreign Device Settings

enable Foreign Device ☐ Update FD

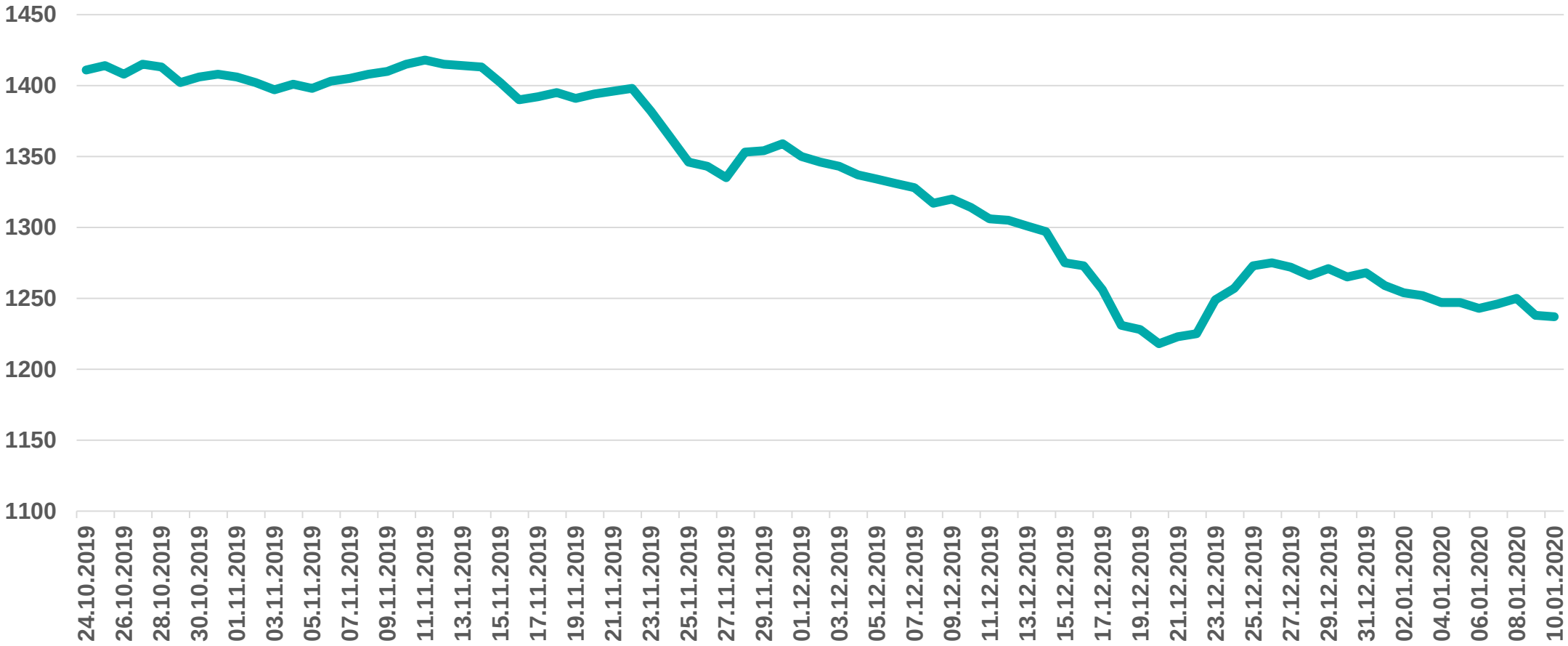
IP Address	UDP Port	Time To Live	
0.0.0.0	47808	1800	Update

ALEF

Informing interested parties

- Big help from (and big thanks to)
  - CZ.NIC – National Registrar for CZ TLD
  - NCISA/NÚKIB – National Cyber and Information Security Agency

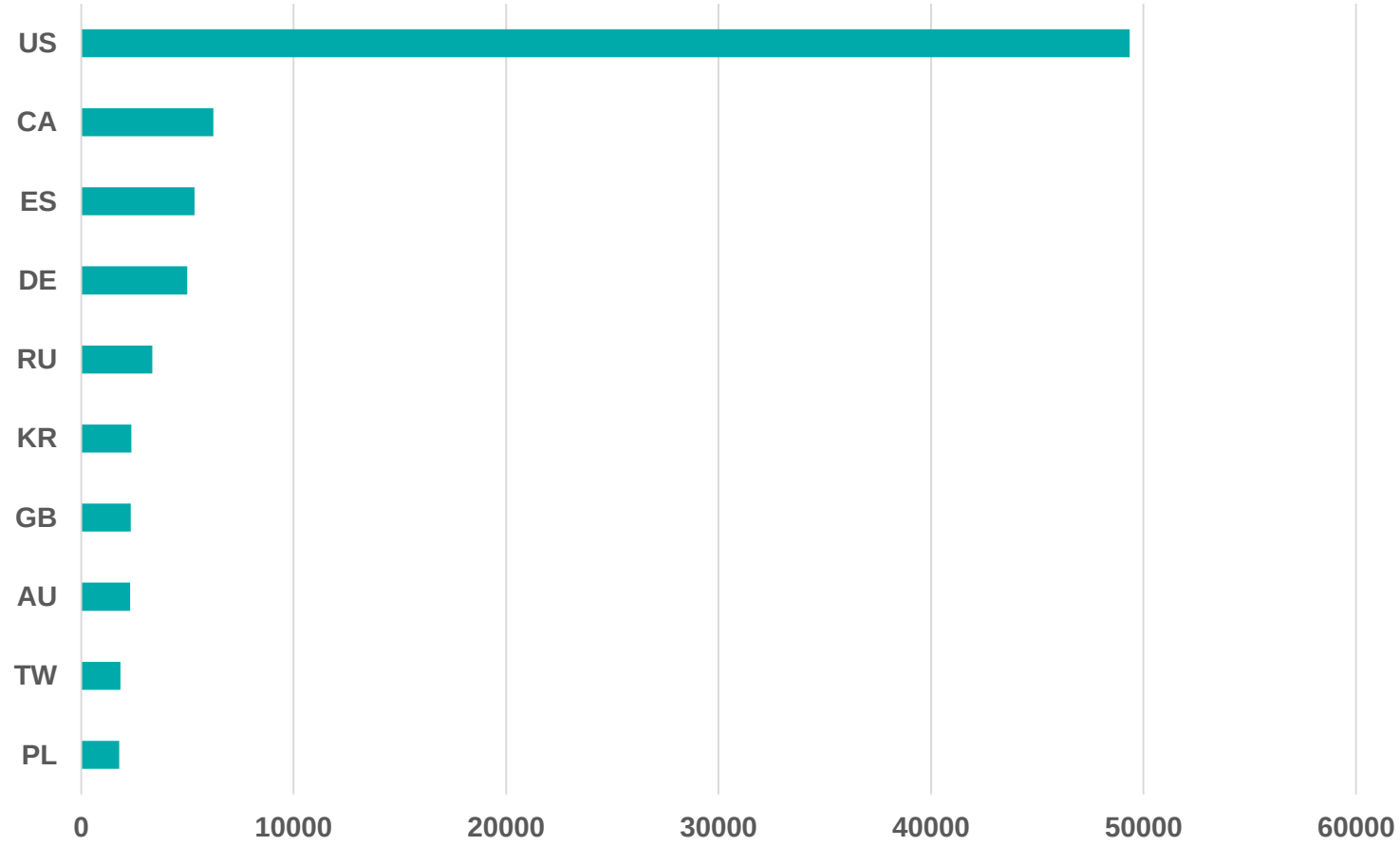
That was then…



ALEF

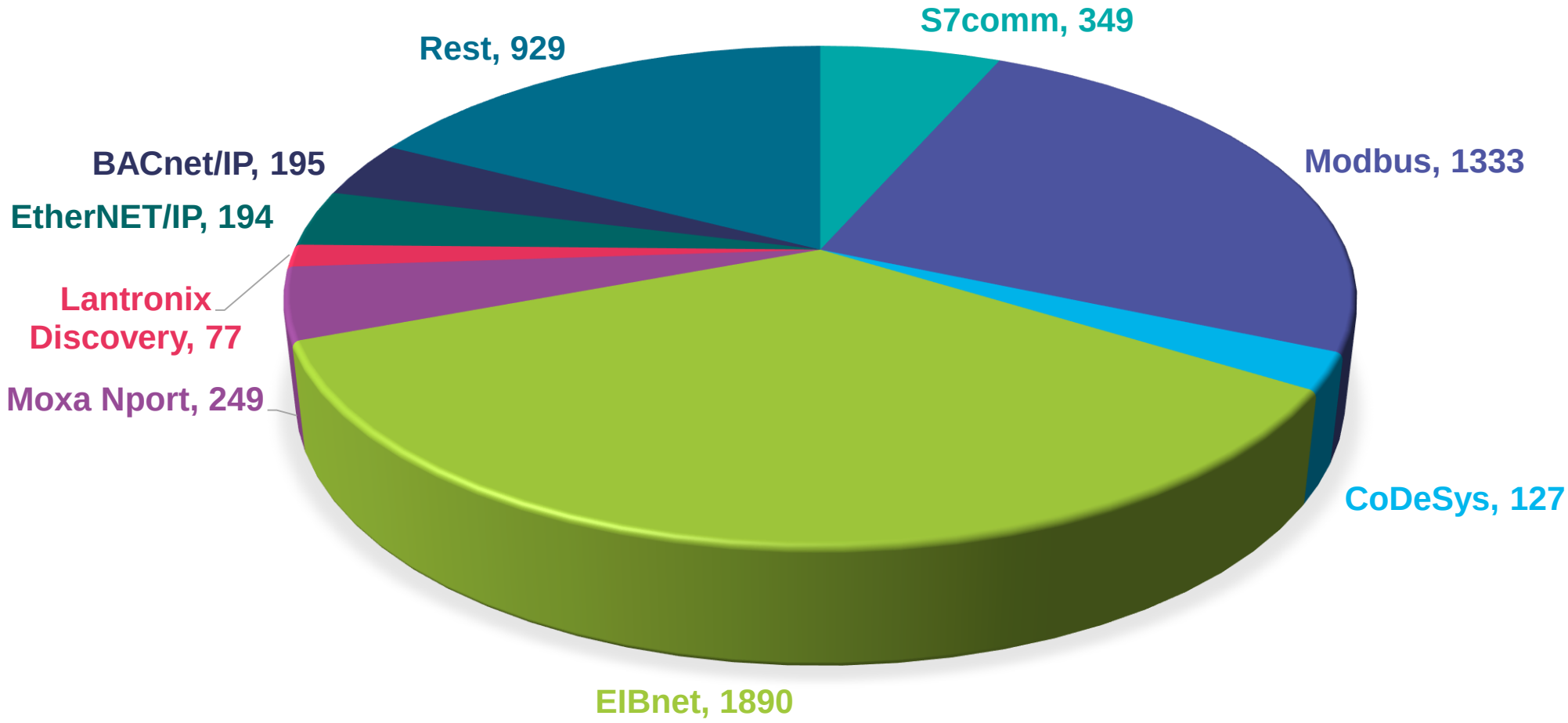
…this is now

- 122,784 ICS systems on Shodan - January 10th



ALEF

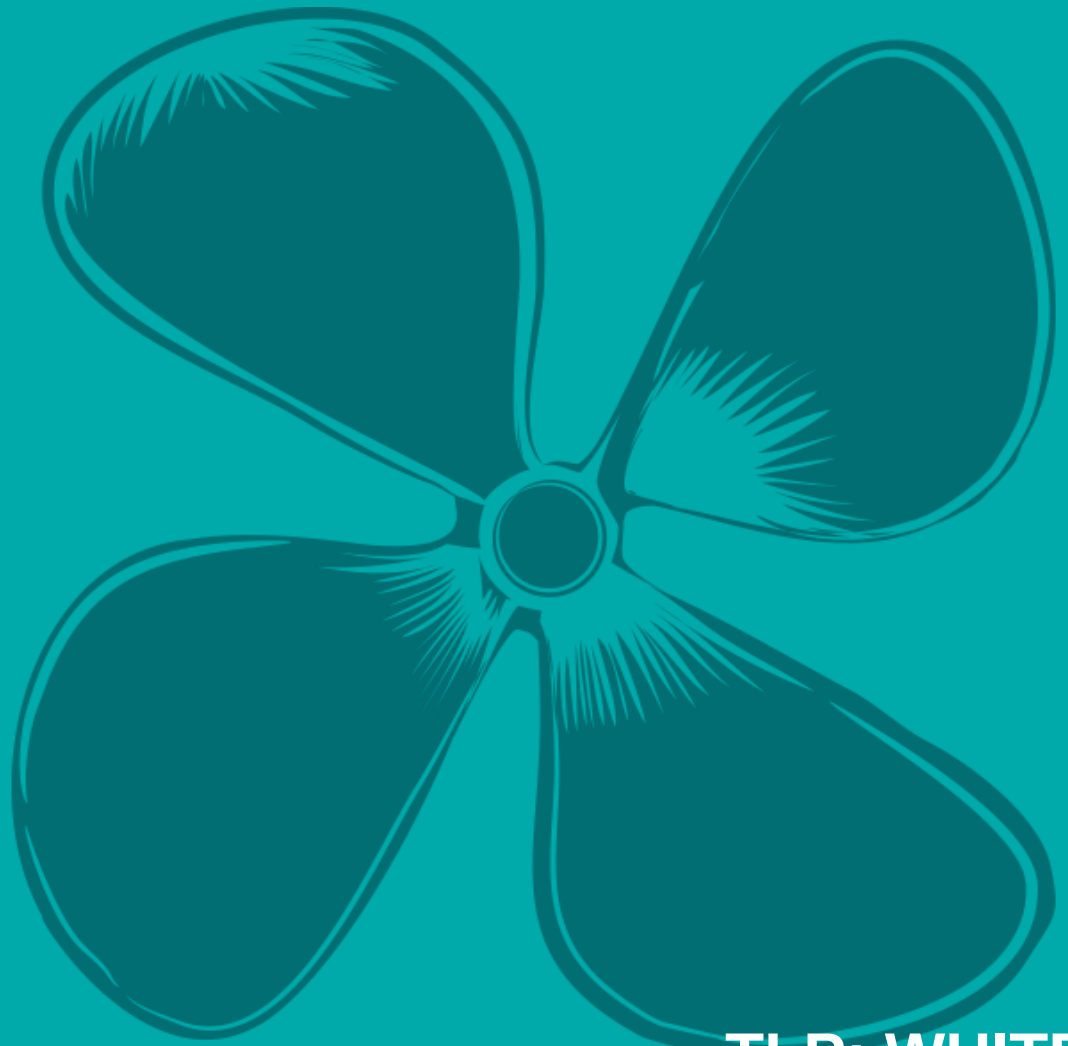
A look at current situation in Spain



ALEF

ALEF

Thank you for your attention



TLP: WHITE