

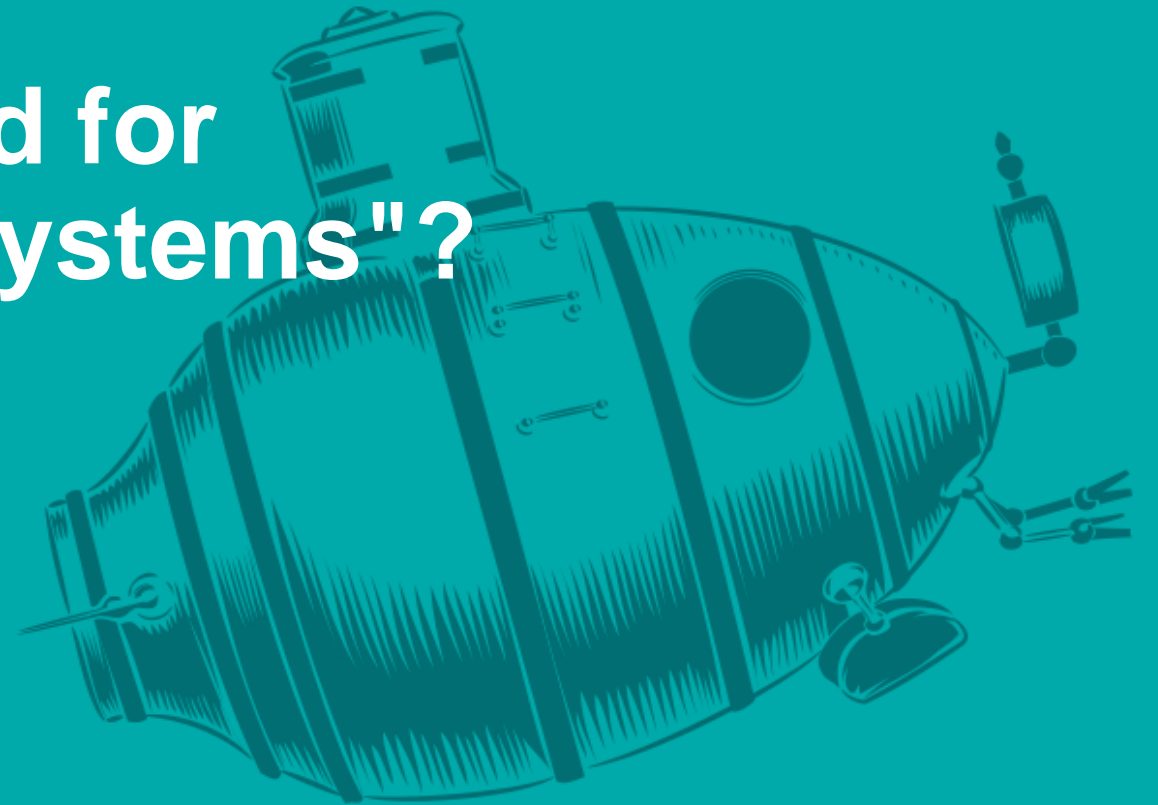


Wait, ICS doesn't stand for "Internet-Connected Systems"?

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?

Shodan Developers Monitor View All... Show API

SHODAN port:502 "Unit ID" 🔍

Home Explore Downloads Reports Pricing Enterprise Access

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS
22,511

TOP COUNTRIES

United States	4,128
France	1,616
Italy	1,586
Germany	1,476
Spain	1,462

TOP ORGANIZATIONS

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

88.28.205.92
92.red-88-28-205.staticip.rima-tde.net
Telefonica de Espana Static IP
Added on 2019-10-23 15:03:44 GMT
🇪🇸 Spain

ics

Unit ID: 0
-- Slave ID Data: Illegal Function (Error)
-- Device Identification: Illegal Function (Error)

188.38.33.57
host30518157.vodafone.com.tr
Vodafone Telekomunikasyon A.S.
Added on 2019-10-23 15:04:23 GMT
🇹🇷 Turkey

ics

Unit ID: 0
-- Slave ID Data: Acknowledge (Error)
-- Device Identification: Acknowledge (Error)

Unit ID: 1
-- Slave ID Data: Illegal Function (Error)
-- Device Identification: Illegal Function (Error)

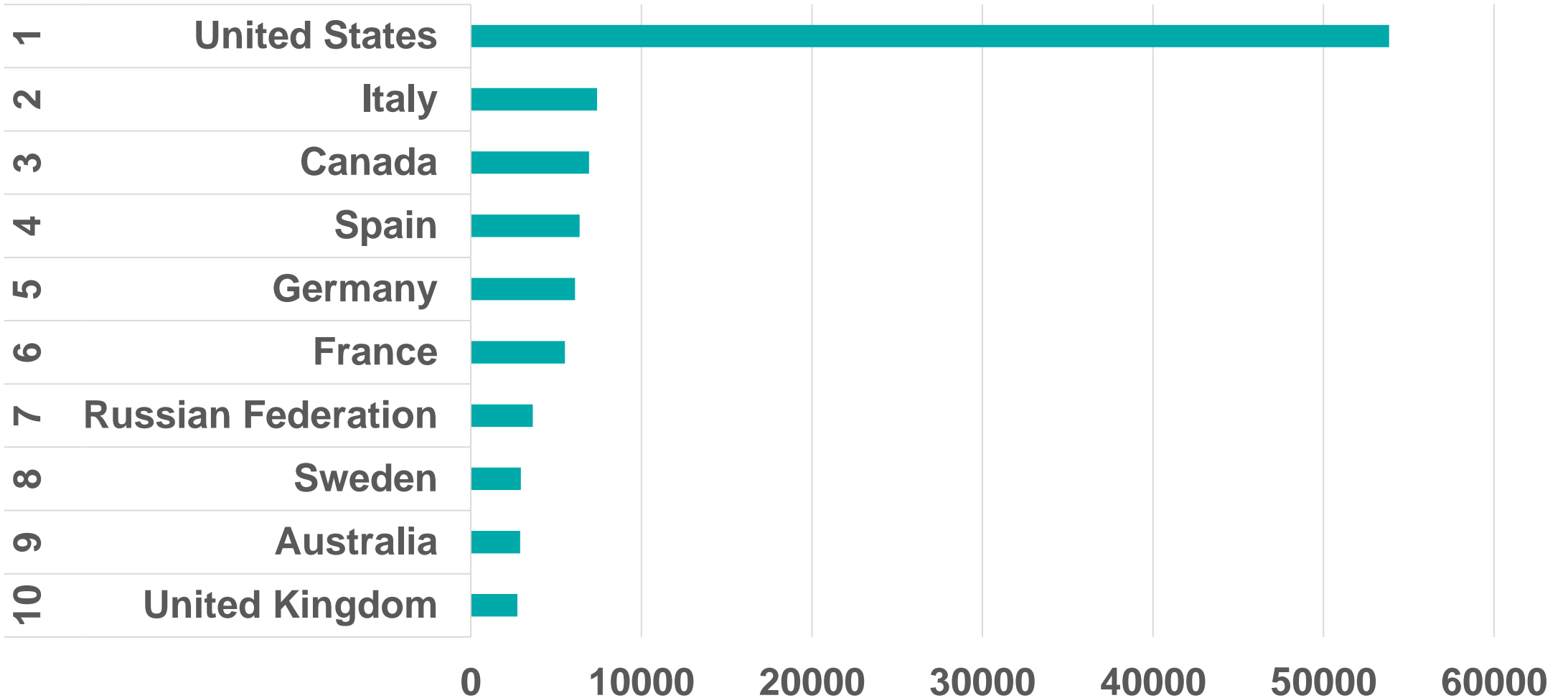
Is ICS connected to the internet dangerous?

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

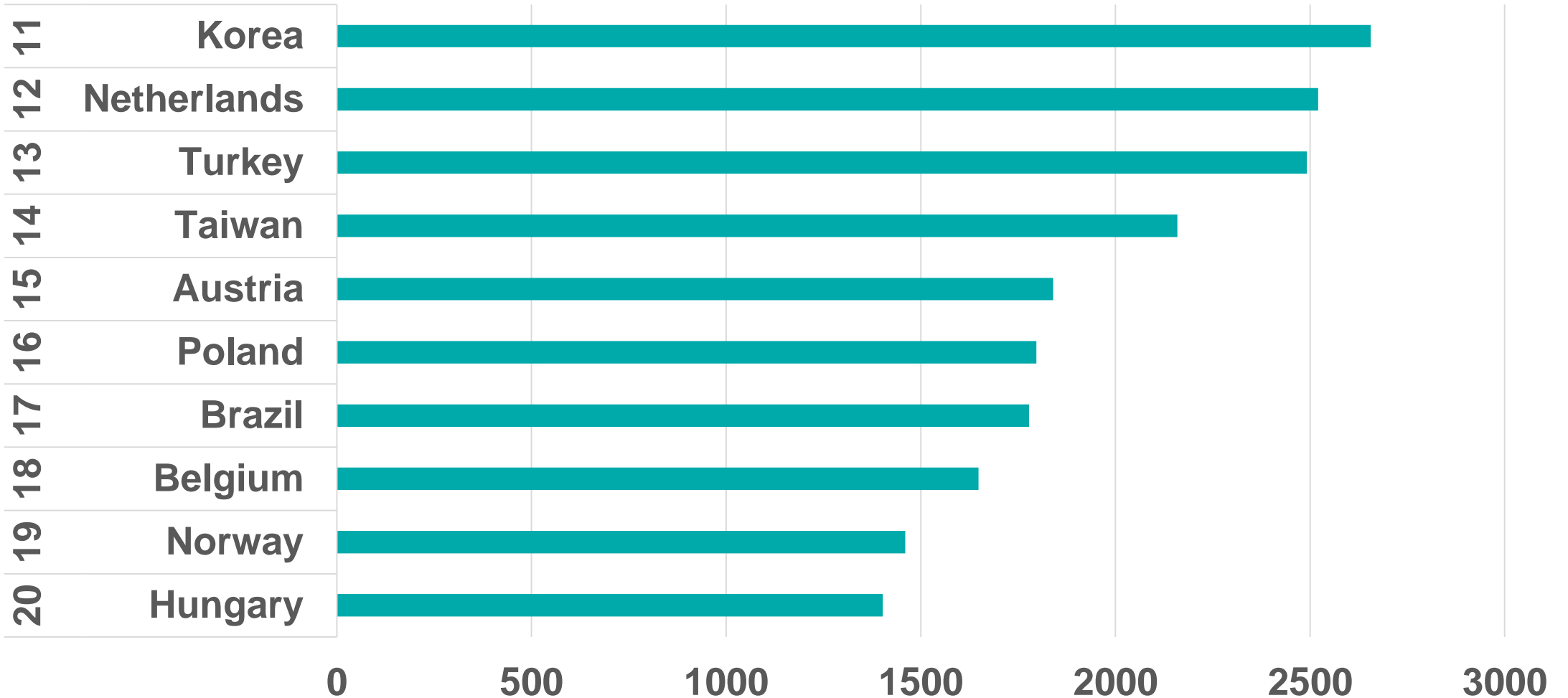
What did we do?

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

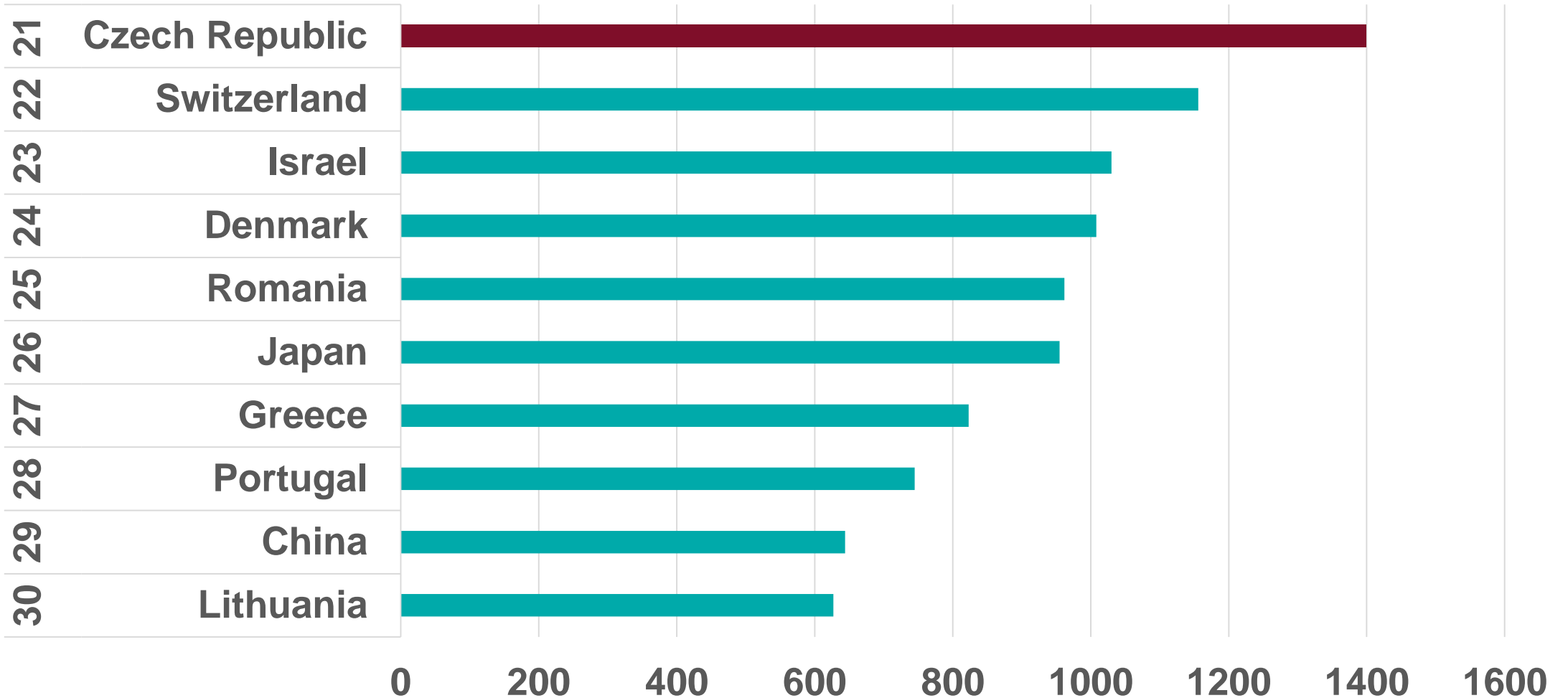
How many ICS are out there?



How many ICS are out there?



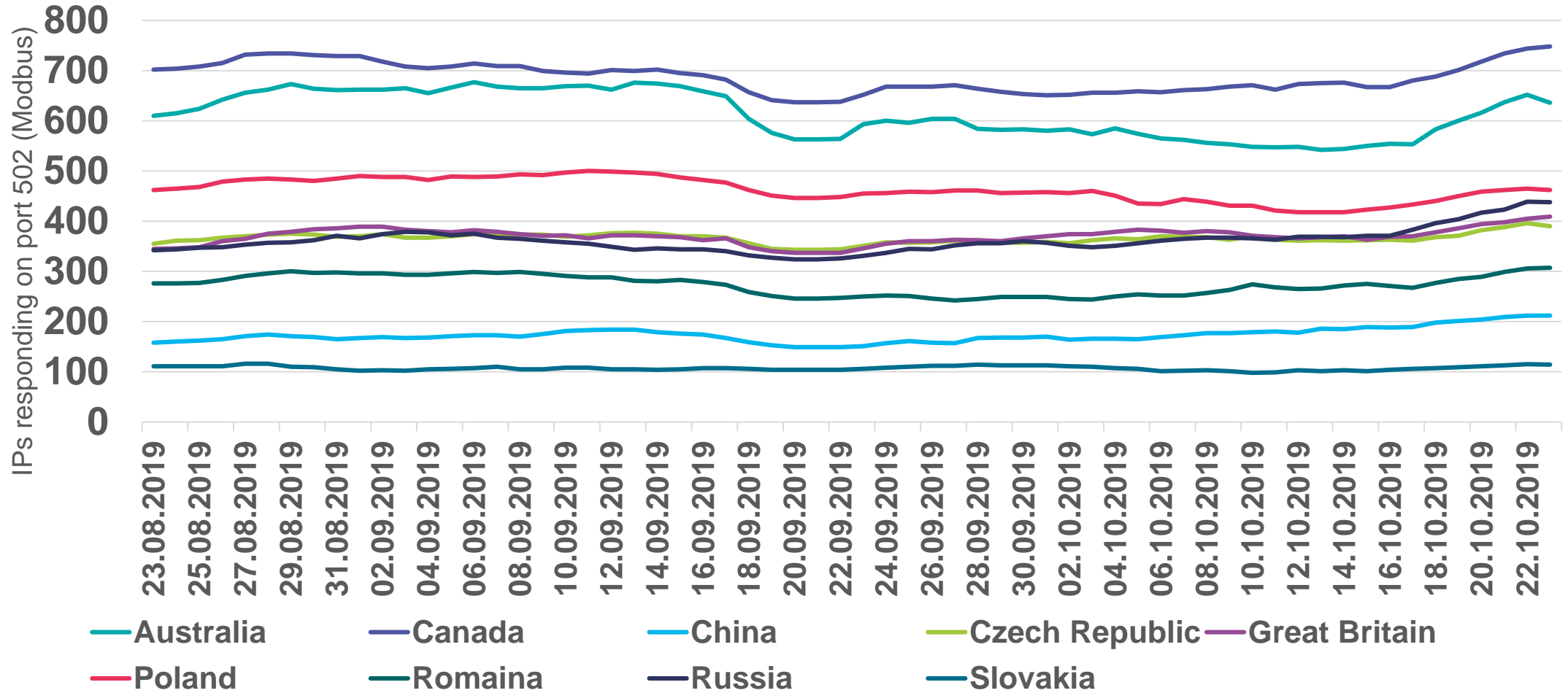
How many ICS are out there?



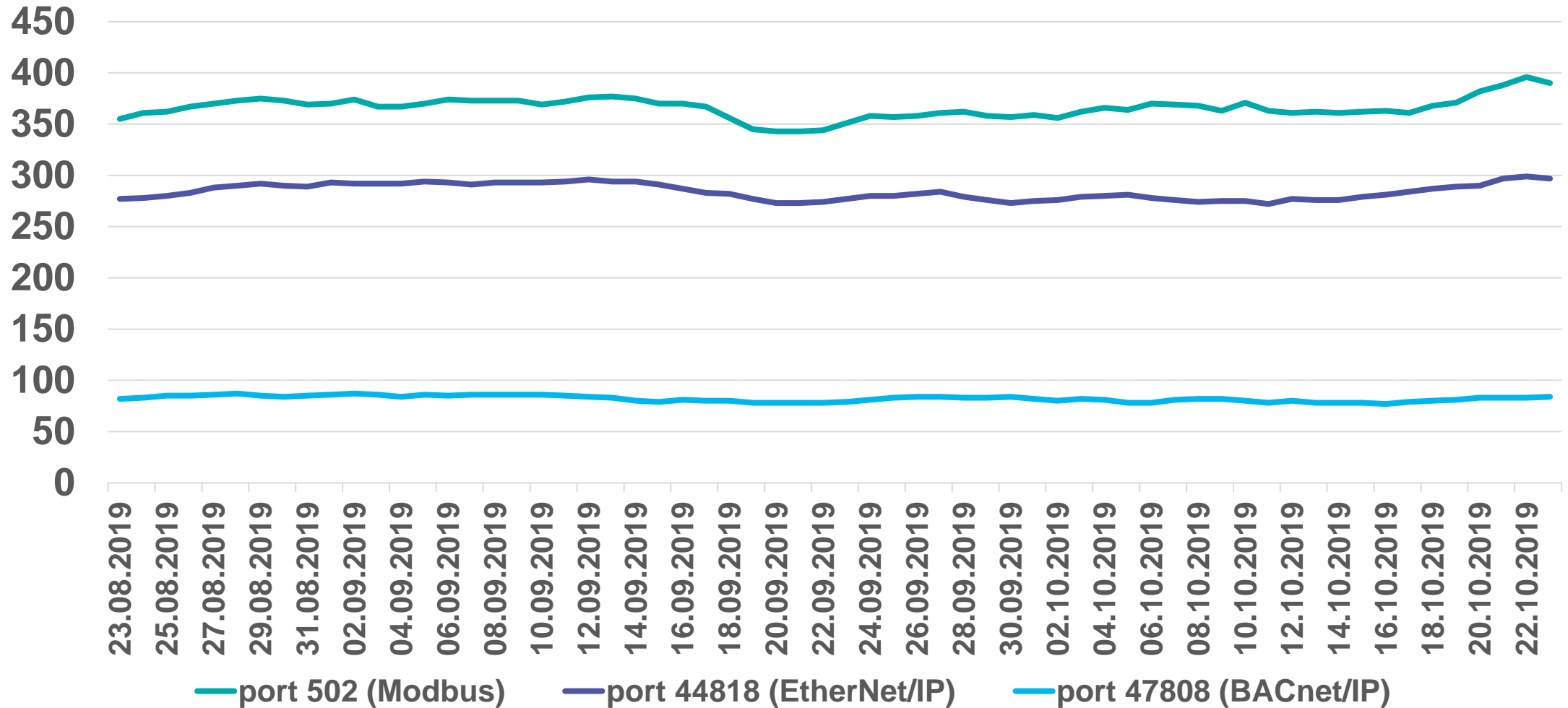
That's not great...

- 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

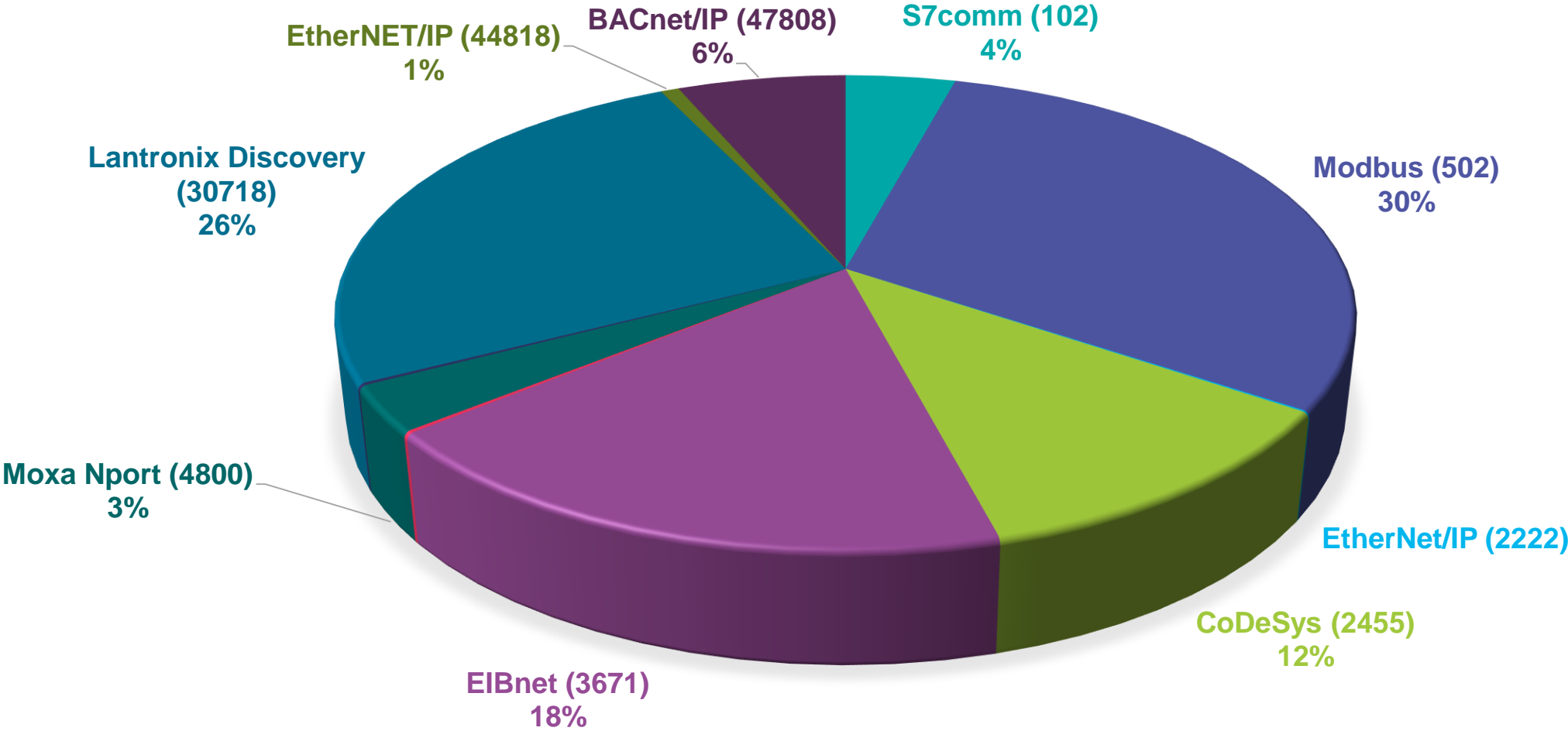
...but is this normal?



Let's take a look at the Czech Republic...



What is/was out there?




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

Welcome
Please log on



Log on

Name

Password

Language

Keep me logged on

...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.

Description	Actual Value
enable BACnet	<input checked="" type="checkbox"/>
Language	<input type="text" value="COM1"/> (-1, COM1, COM2, 0, 1, 2, 3, ...)
BACnet DeviceID	<input type="text" value=""/>
BACnet DeviceName	<input type="text" value=""/>
UDPPort	<input type="text" value="47808"/> (Decimal 47808 = BAC0 Hexadecimal...)
Use UniCode	<input type="checkbox"/>
RecipientDevice1	<input type="text" value="0"/>
RecipientDevice2	<input type="text" value="0"/>
RecipientDevice3	<input type="text" value="0"/>

Initial Configuration for BACnet COV Handling

COV File	<input type="text" value=""/>
Limit <= 1	<input type="text" value="0.0001"/>
Limit > 1	<input type="text" value="0.001"/>
Limit > 10	<input type="text" value="0.1"/>
Limit > 100	<input type="text" value="0.3"/>
Limit > 1000	<input type="text" value="1.0"/>
Limit > 10000	<input type="text" value="3.0"/>

Foreign Device Settings

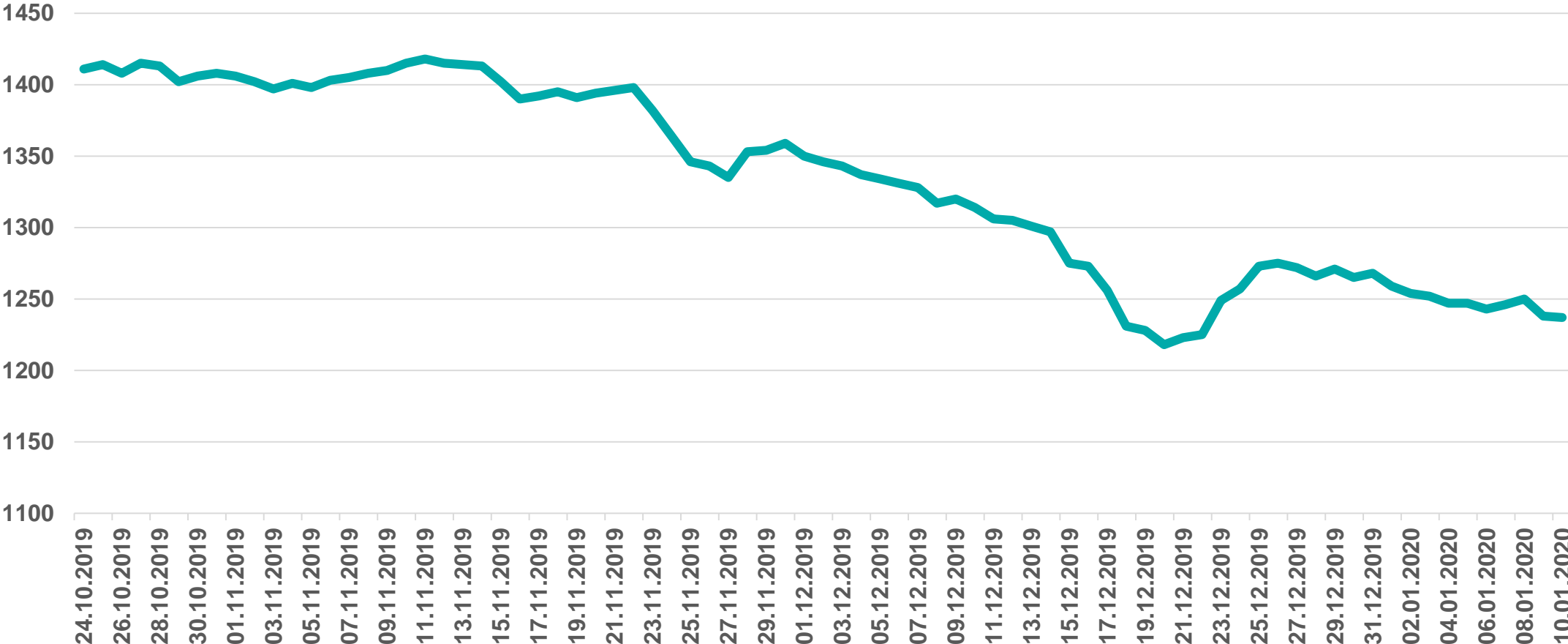
enable Foreign Device

IP Address	UDP Port	Time To Live
<input type="text" value="0.0.0.0"/>	<input type="text" value="47808"/>	<input type="text" value="1800"/>

Informing interested parties

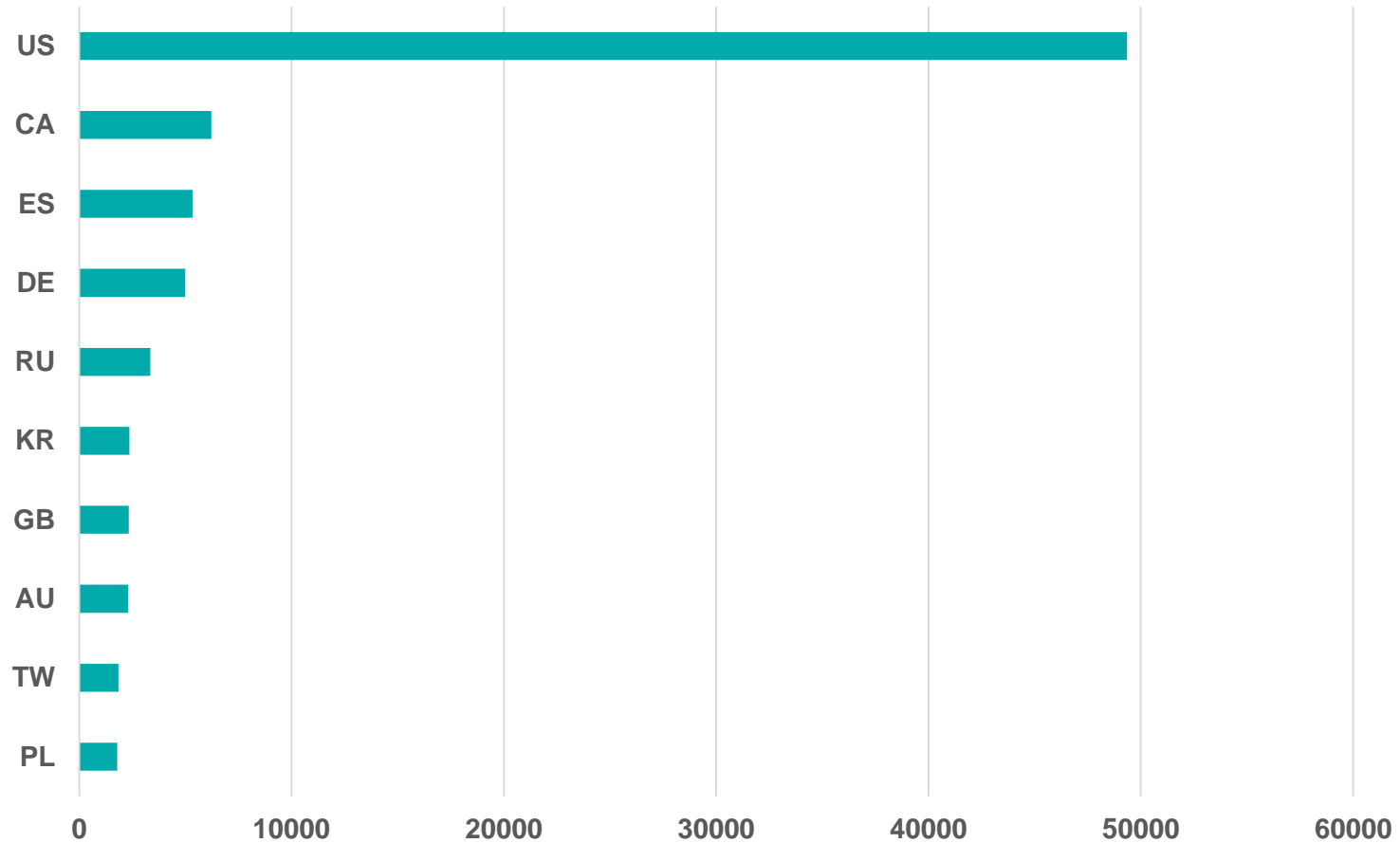
- Big help from (and big thanks to)
 - CZ.NIC – National Registrar for CZ TLD
 - NCISA/NÚKIB – National Cyber and Information Security Agency

That was then...

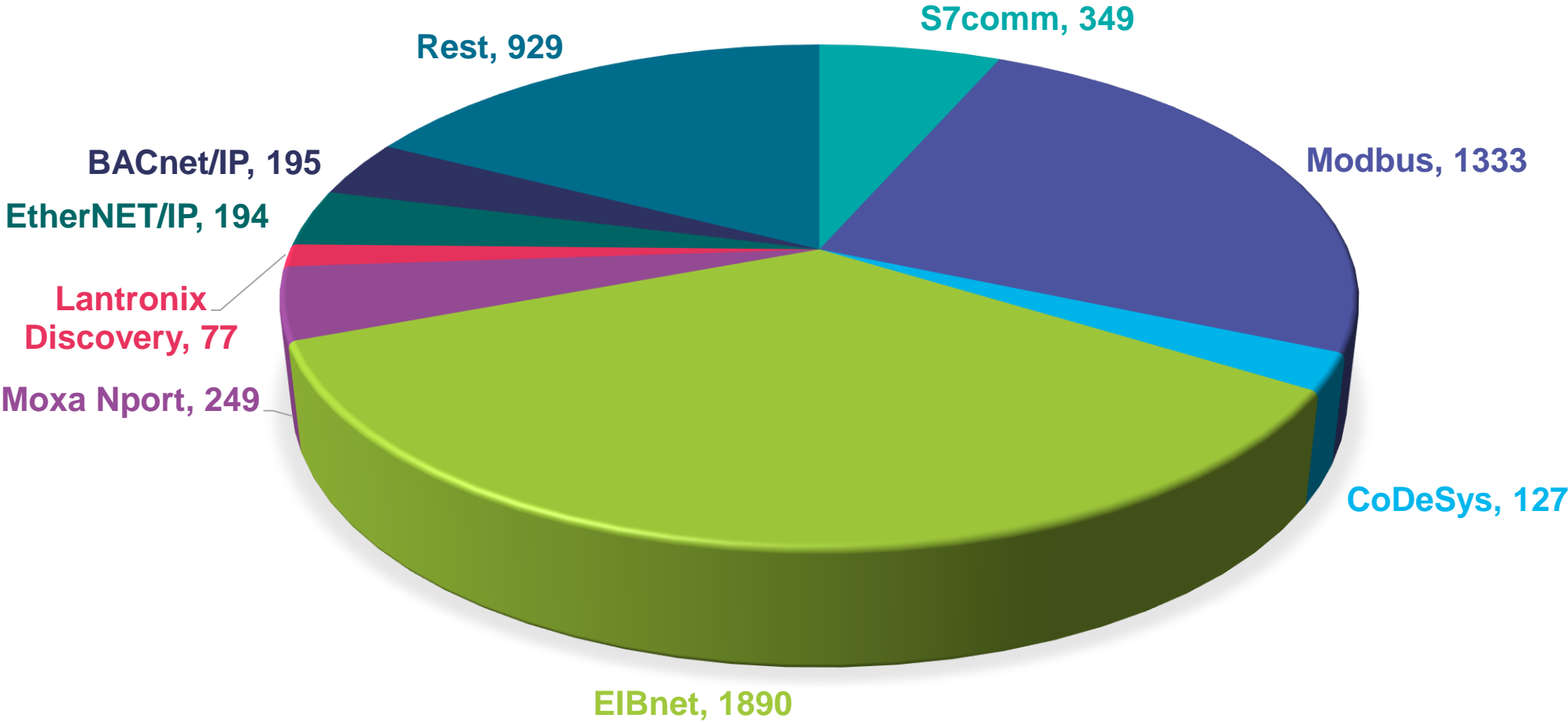


...this is now

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

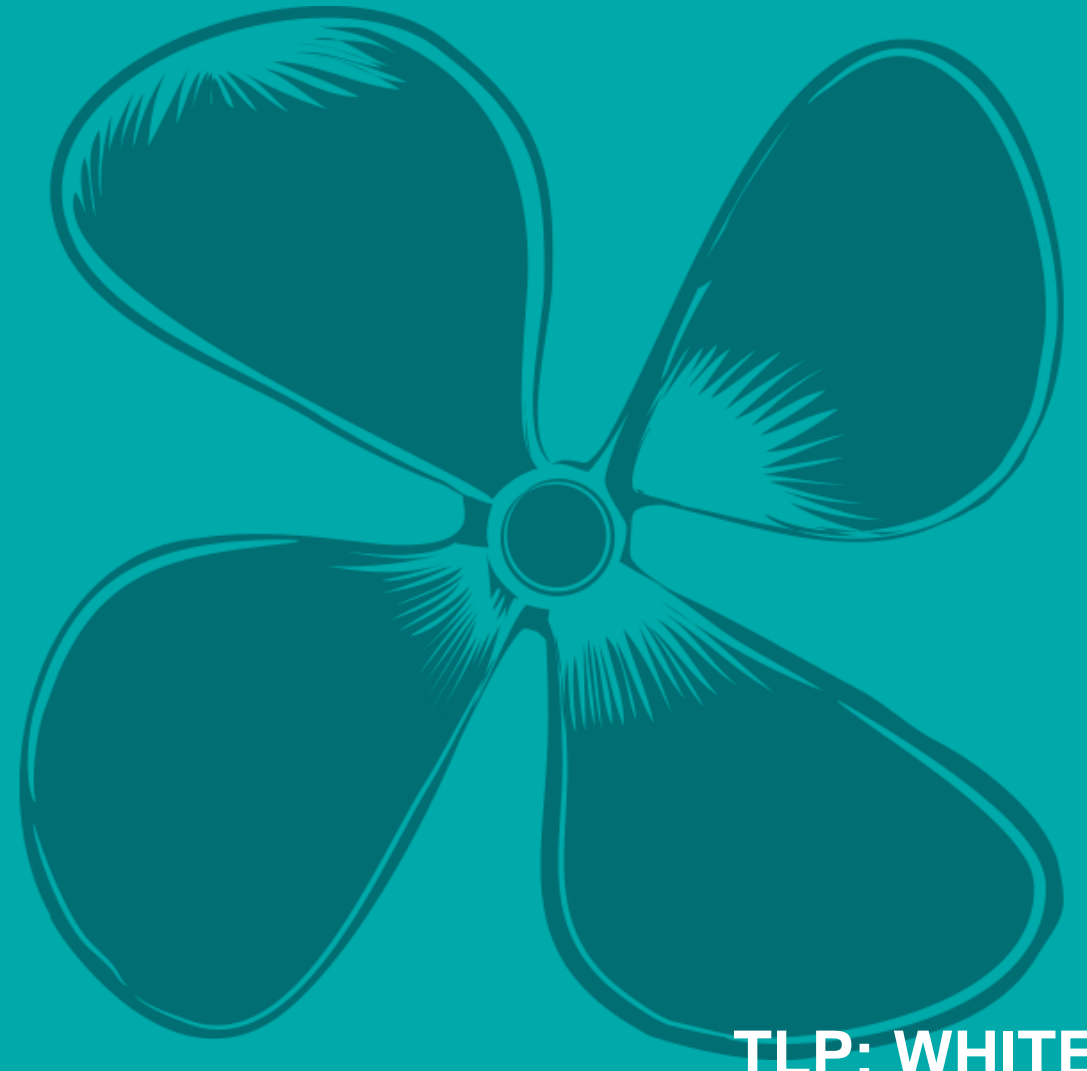


A look at current situation in Spain



X ALEF

**Thank you for
your attention**



TLP: WHITE