



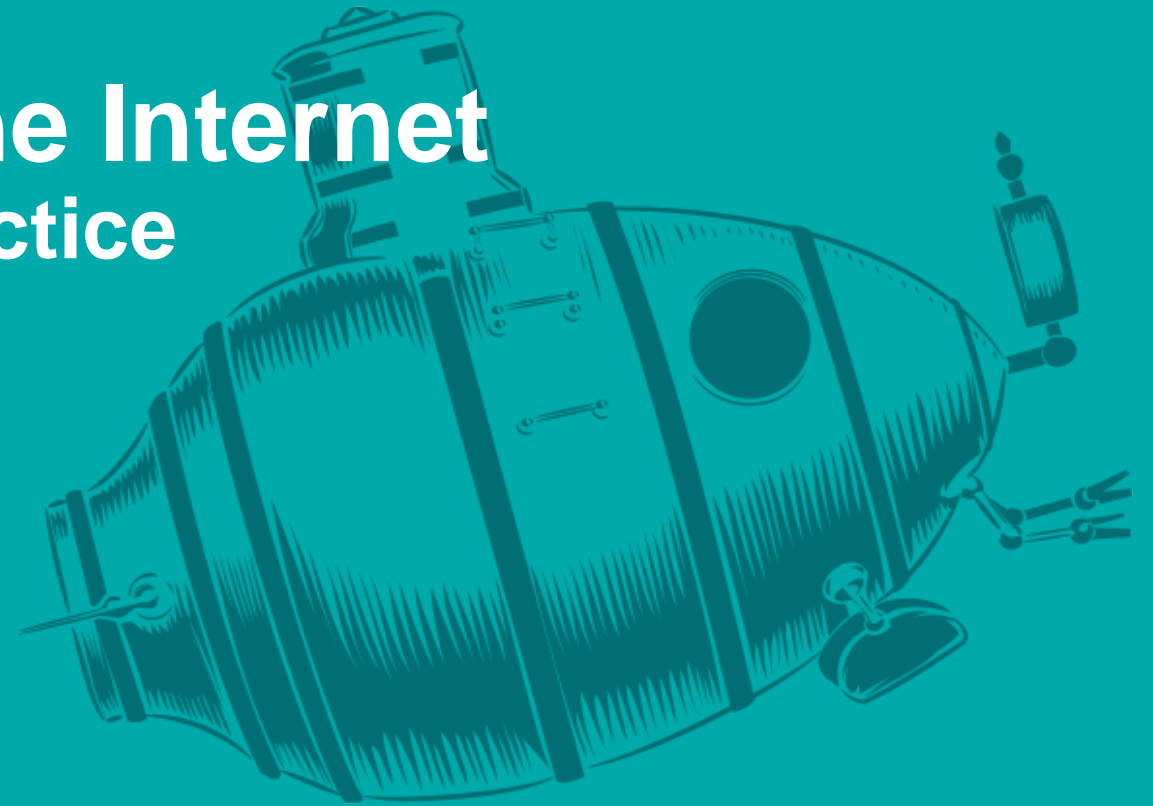
**ALEF**

# ICS accessible from the Internet bad (and very common) practice

**Jan Kopřiva**

jan.kopriva@alef.com

ALEF CSIRT



**TLP: GREEN**



# 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

**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: Illegal Function (Error)  
-- Device Identification: Illegal Function (Error)

**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“



```
Command Prompt
C:\Tools\TriOp\scada>python3 triop.py -h

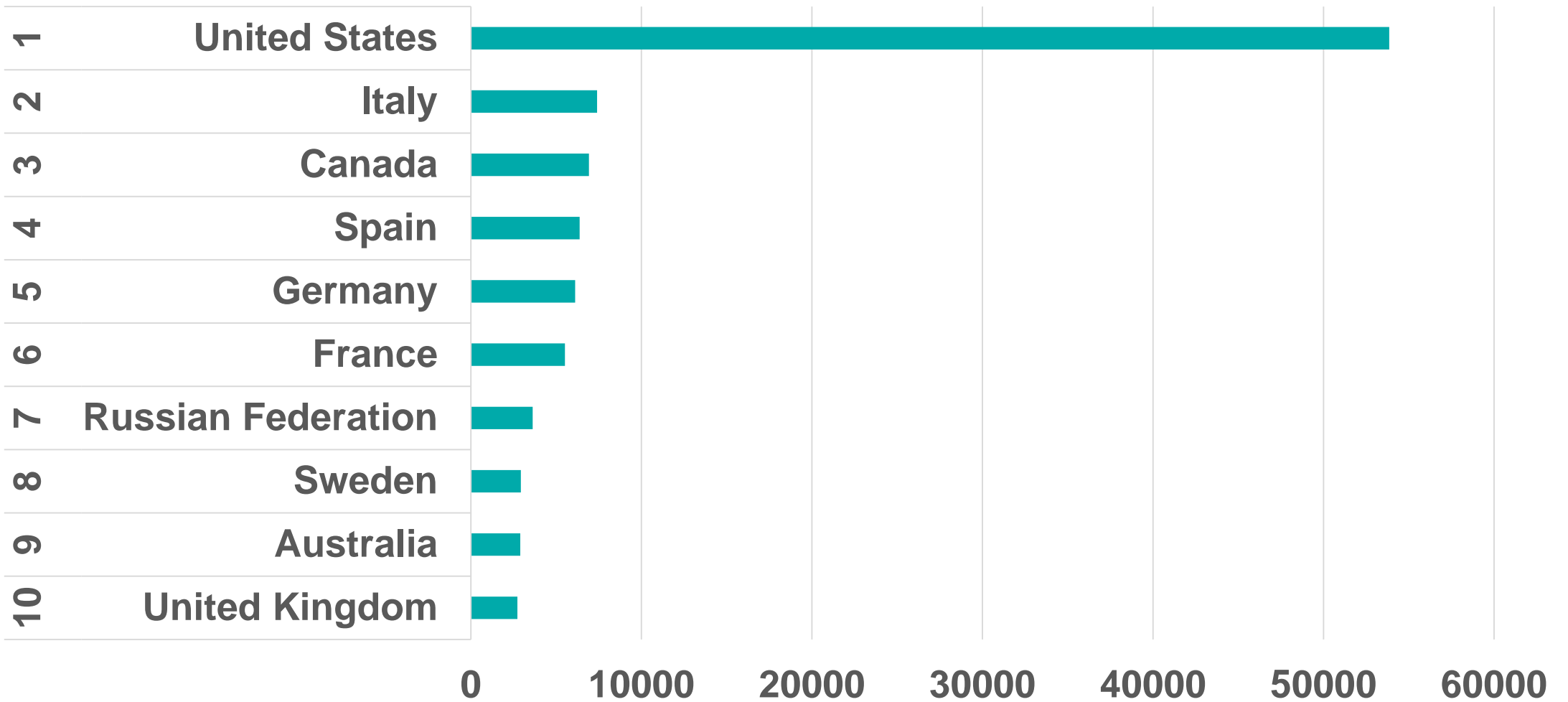
TriOp
Tool for interacting with Shodan.IO to get statistical information/numbers of IPs which satisfy the
queries submitted in bulk

Usage: triop.py [options]

Options:
  -h, --help            show this help message and exit
  -k KEY, --key=KEY     API key for Shodan
  --save_key            save key in a plaintext key file, used in conjunction
                        with option -k   !!!DO NOT USE ON SHARED COMPUTERS!!!
  -s SEARCH, --search=SEARCH
                        comma-separated list of search criteria
  -S SEARCH_FILE, --search_file=SEARCH_FILE
                        input CSV file(s) with search definitions
  --list_file=LIST_FILE
                        input file containing list of CSV files with search
                        definitions
  --filename_load=FILENAME_LOAD
                        use all files in the same directory which contain the
                        string in their names as search inputs
  -n, --new_file(s)    create new file(s) for results to be saved into
  -c COUNTRY, --country=COUNTRY
```

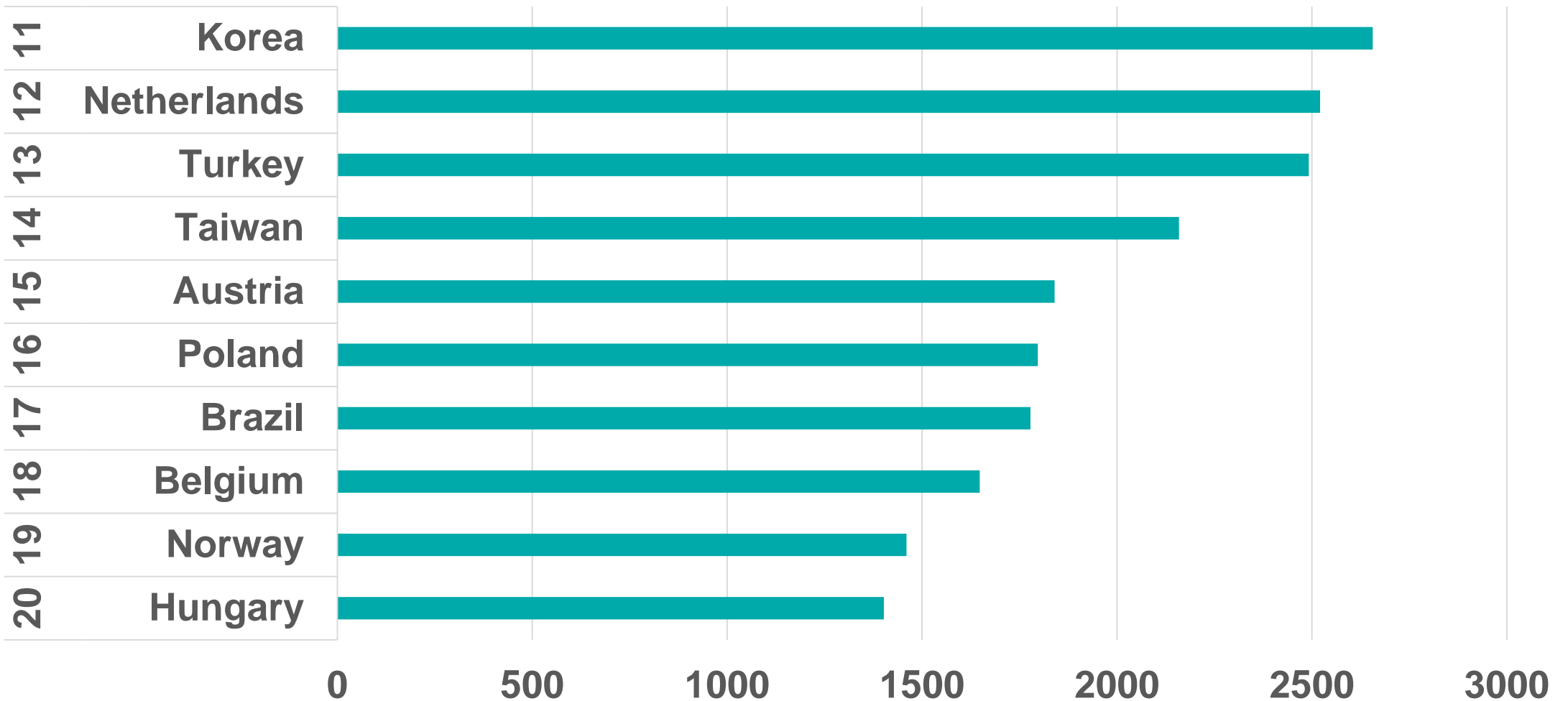


# How many ICS are out there?



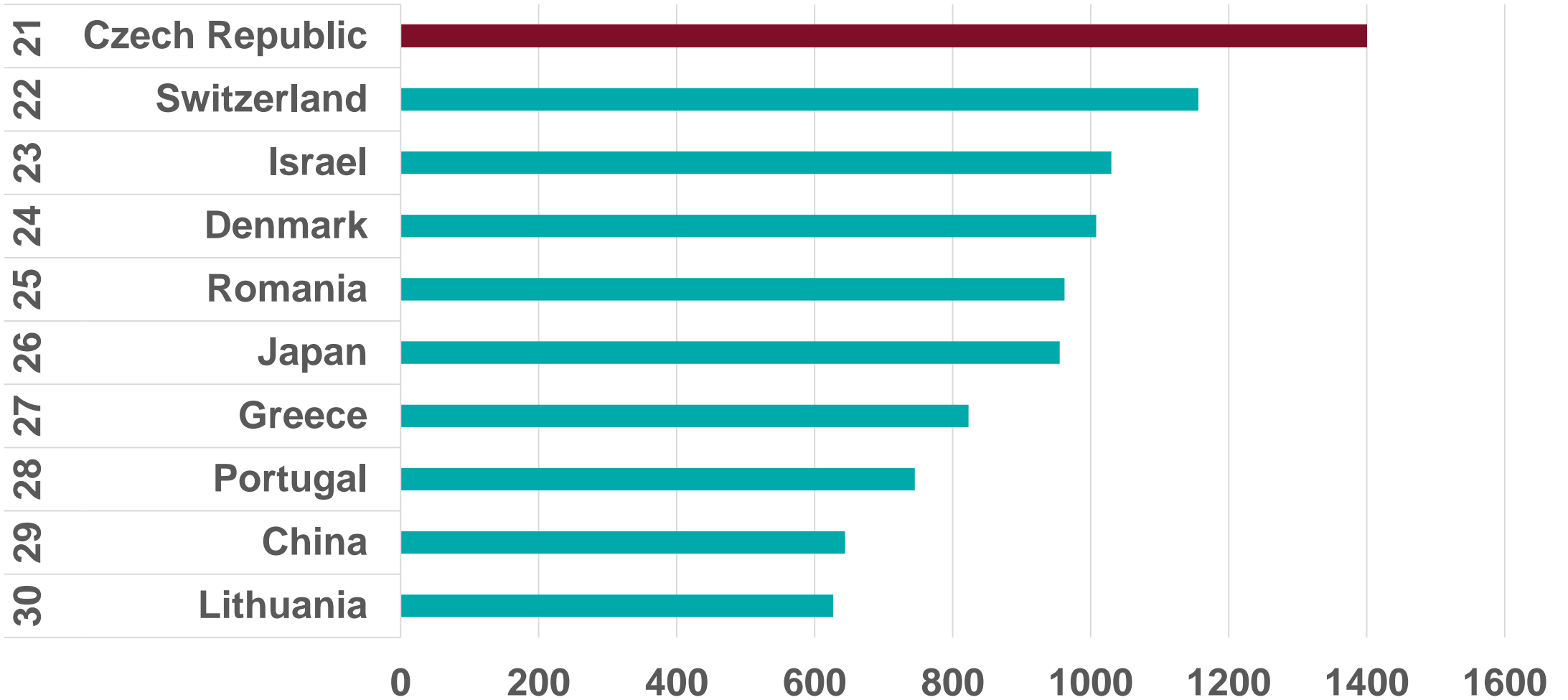


# How many ICS are out there?





# How many ICS are out there?





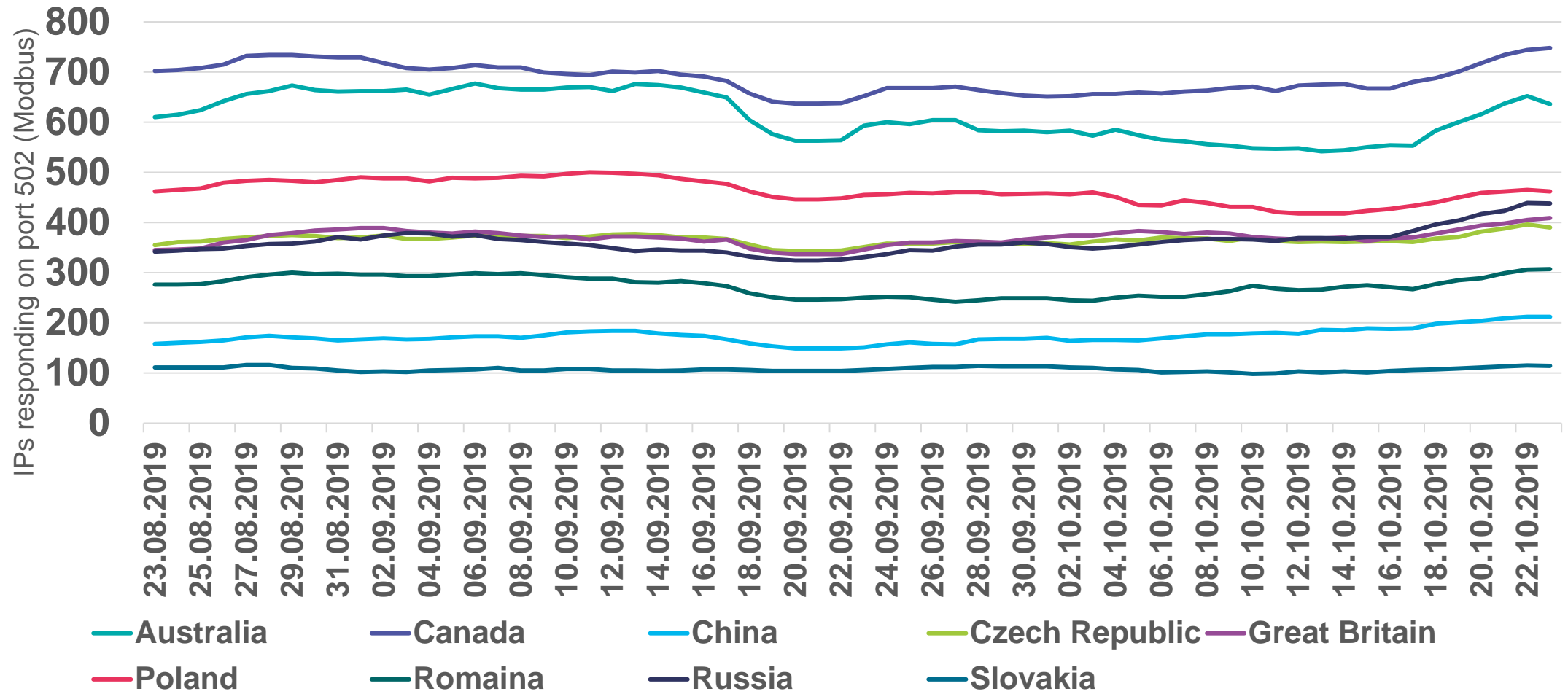


# That's not great...

- 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

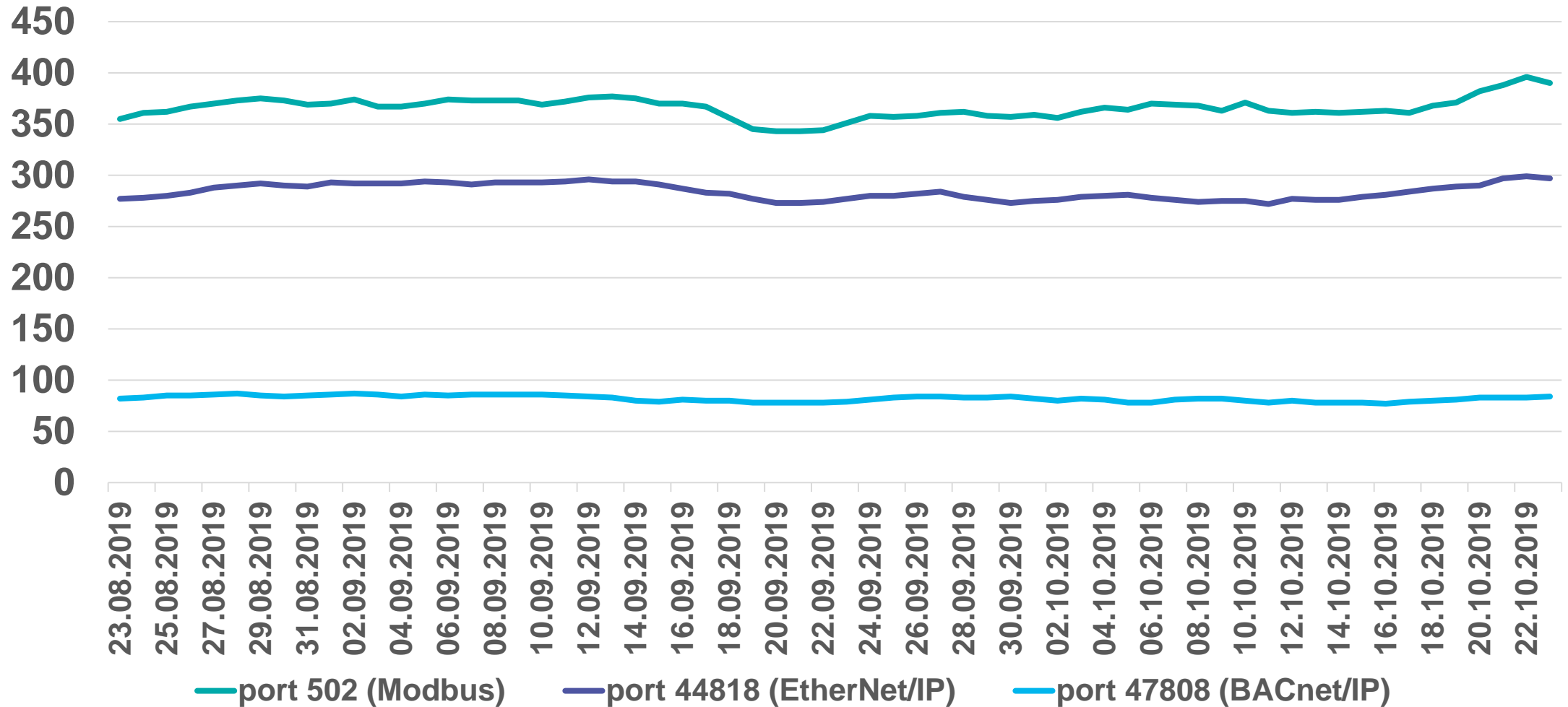


# ...but is this normal?



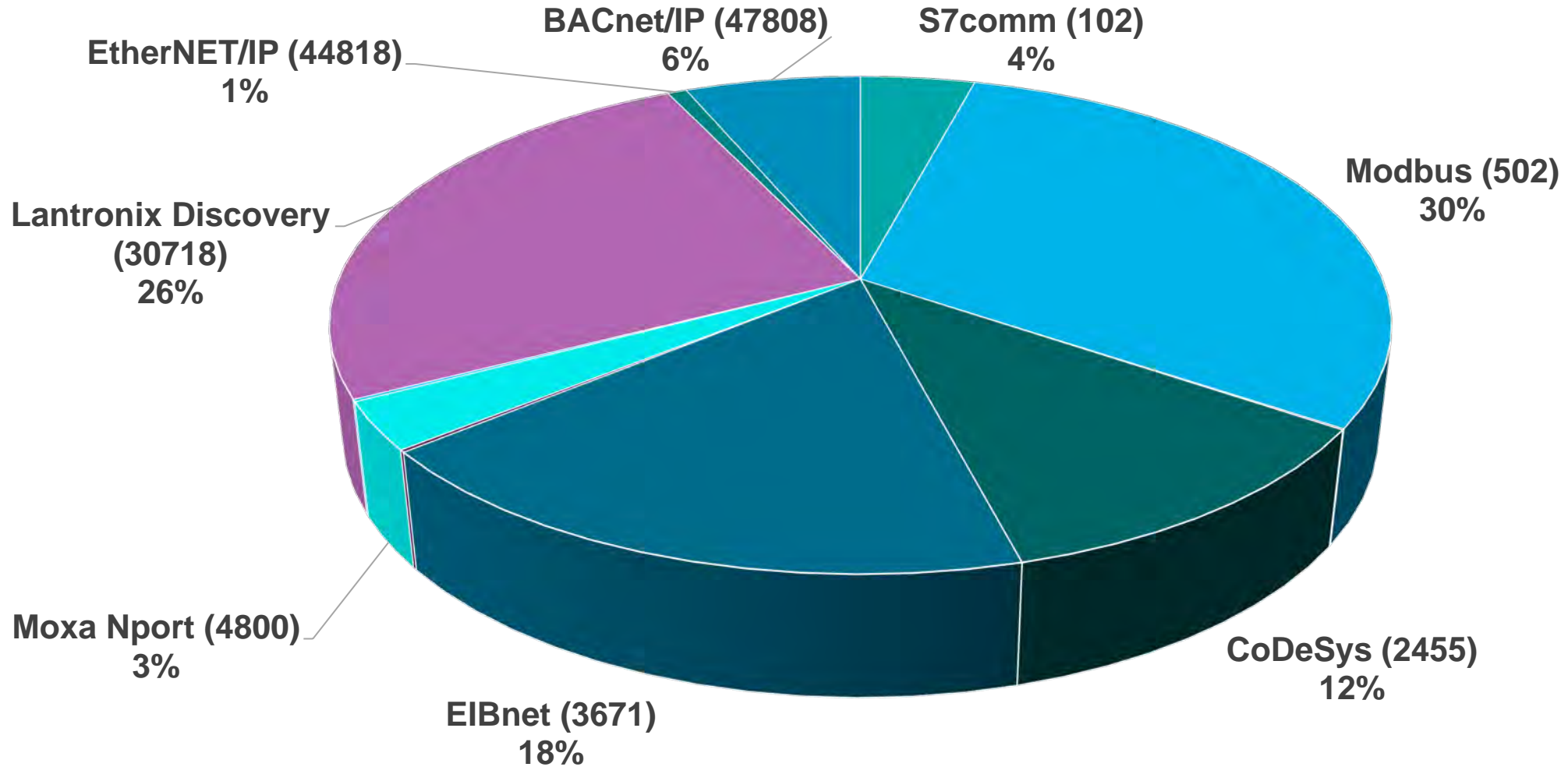


# Let's take a look at the Czech Republic...





# 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

# SIEMENS SIMATIC HMI Miniweb on HMI\_Panel

Name   
Password  [Login](#)

- ▶ Start page
- ▶ Remote Control
- ▶ Control Functions
- ▶ System Diagnostics
- ▶ File Browser

## Control Functions

### Control of HMI\_Panel

Runtime operations

#### Start/Stop

The runtime is **running** (updated at 14:59.00 22.10.2019)

[Start runtime](#)  
[Stop runtime](#)

#### Export recipes

←

#### Import recipes

Delete all existing records before loading the new records  
 Import new records. Replace duplicates with imported records  
 Import new records. Replace duplicates with existing records

→ [Browse...](#) No file selected.

#### Export user administration data

←

#### Import user administration data

→ [Browse...](#) No file selected.

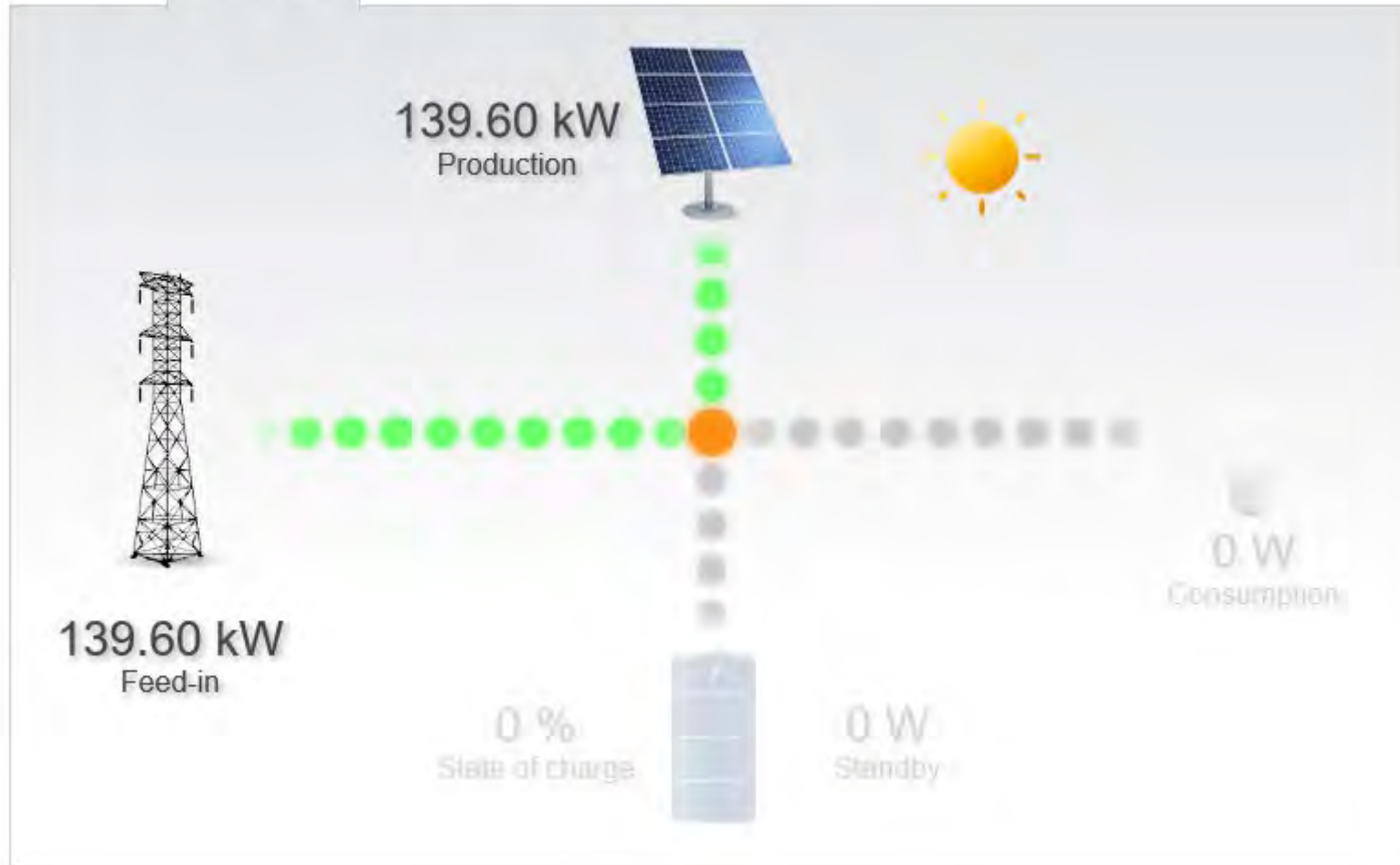
**BENDER** CP700 COMTRAXX

Bus overview

Subsystem [1] !

Yield data / Current values / Energy flow

COCKPIT ENERGY FLOW TABLE



A  
N  
W  
T  
f  
B  
a  
I  
D  
D  
L  
d



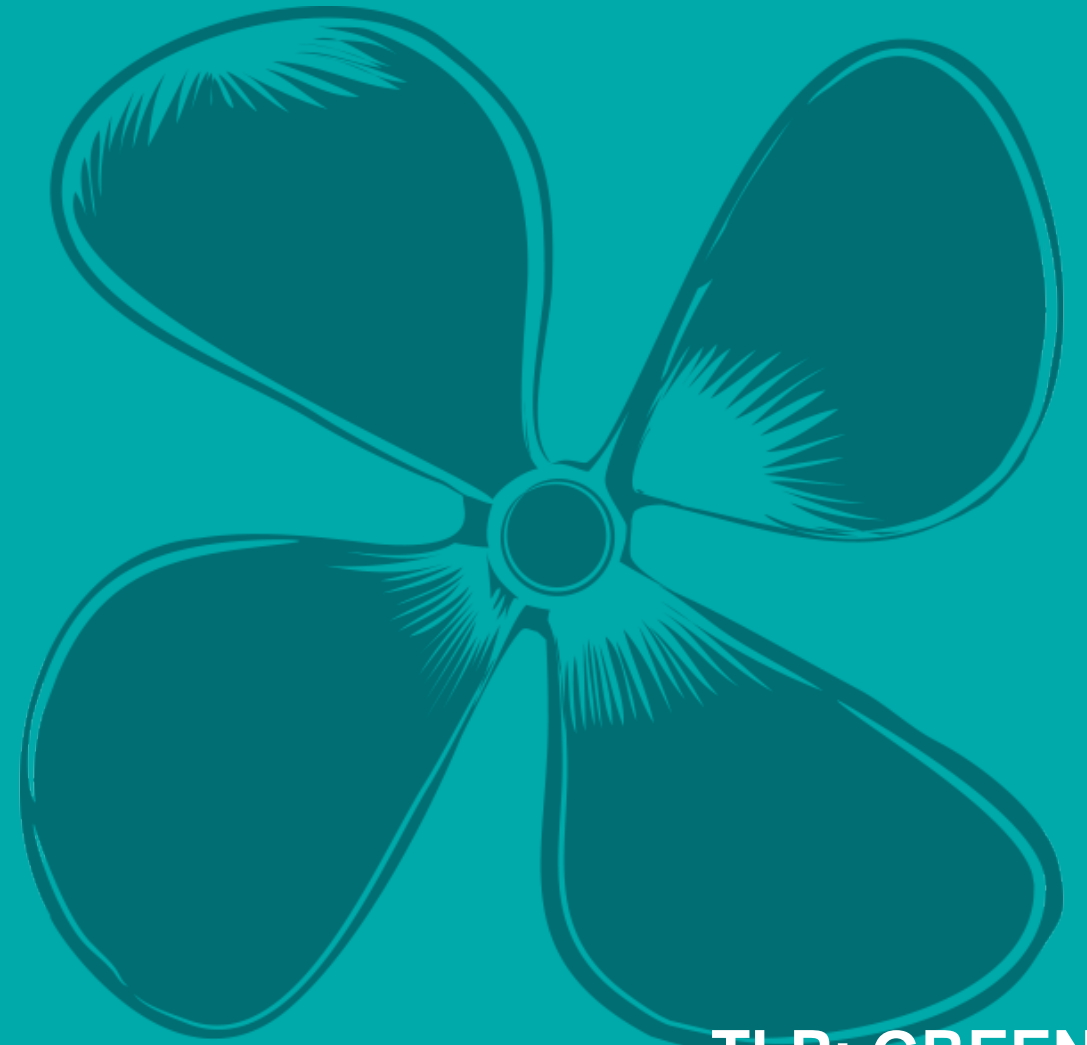


# Informing interested parties

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

**X ALEF**

**Thank you for  
your attention**



**TLP: GREEN**