HACK THE WORLD & GALAXY WITH OSINT

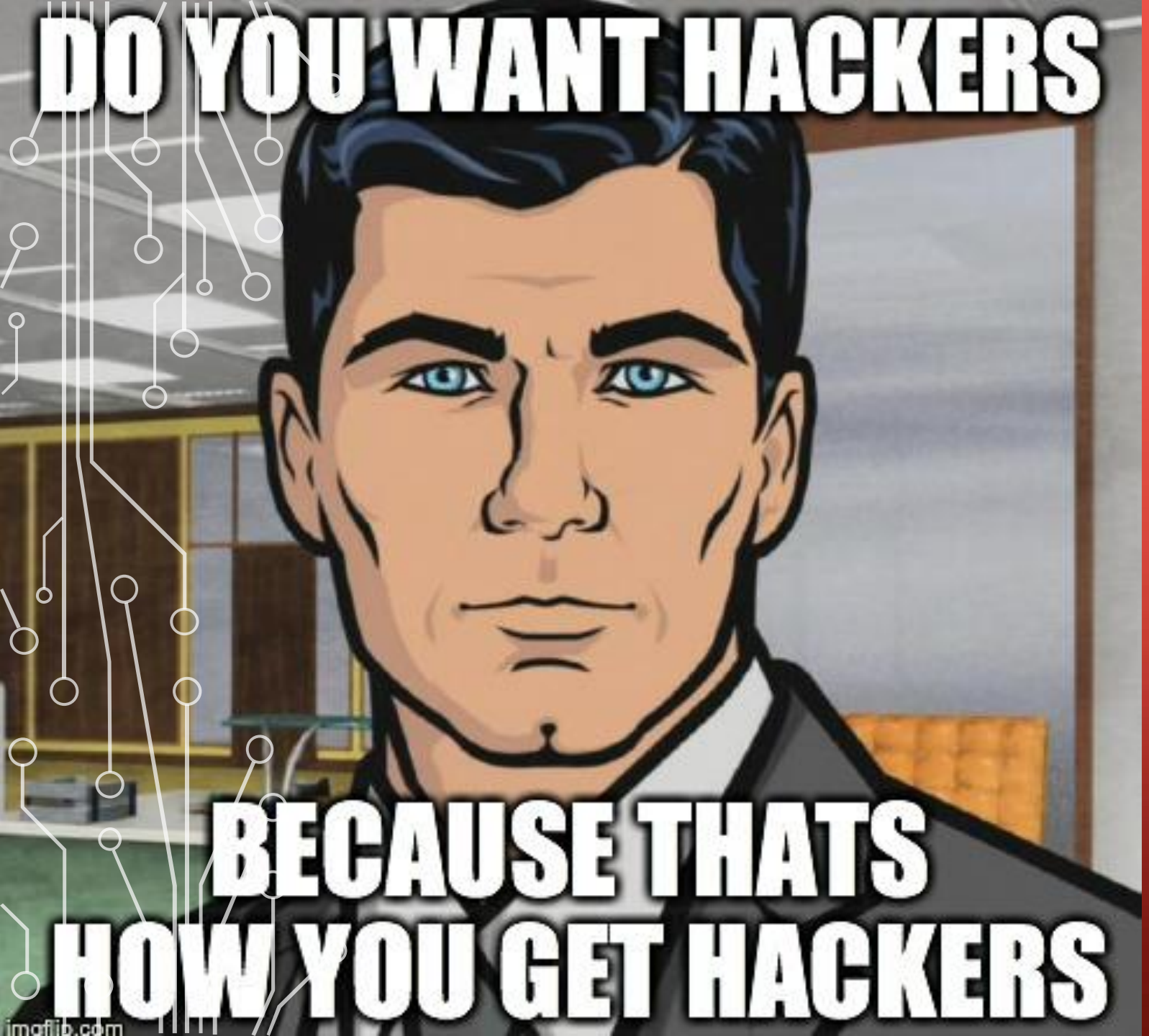
OWASP LONDON

CHRIS KUBECKA, CEO HYPASEC

19 SEPTEMBER 2019

WHO IS THIS CHICA?

- Cyber Warfare
- Headed Aramco Overseas
  Operations, Information Pro
  & Intelligence
- U.S. Air Force Space Comm
  Military Aviator C-5 Loadm

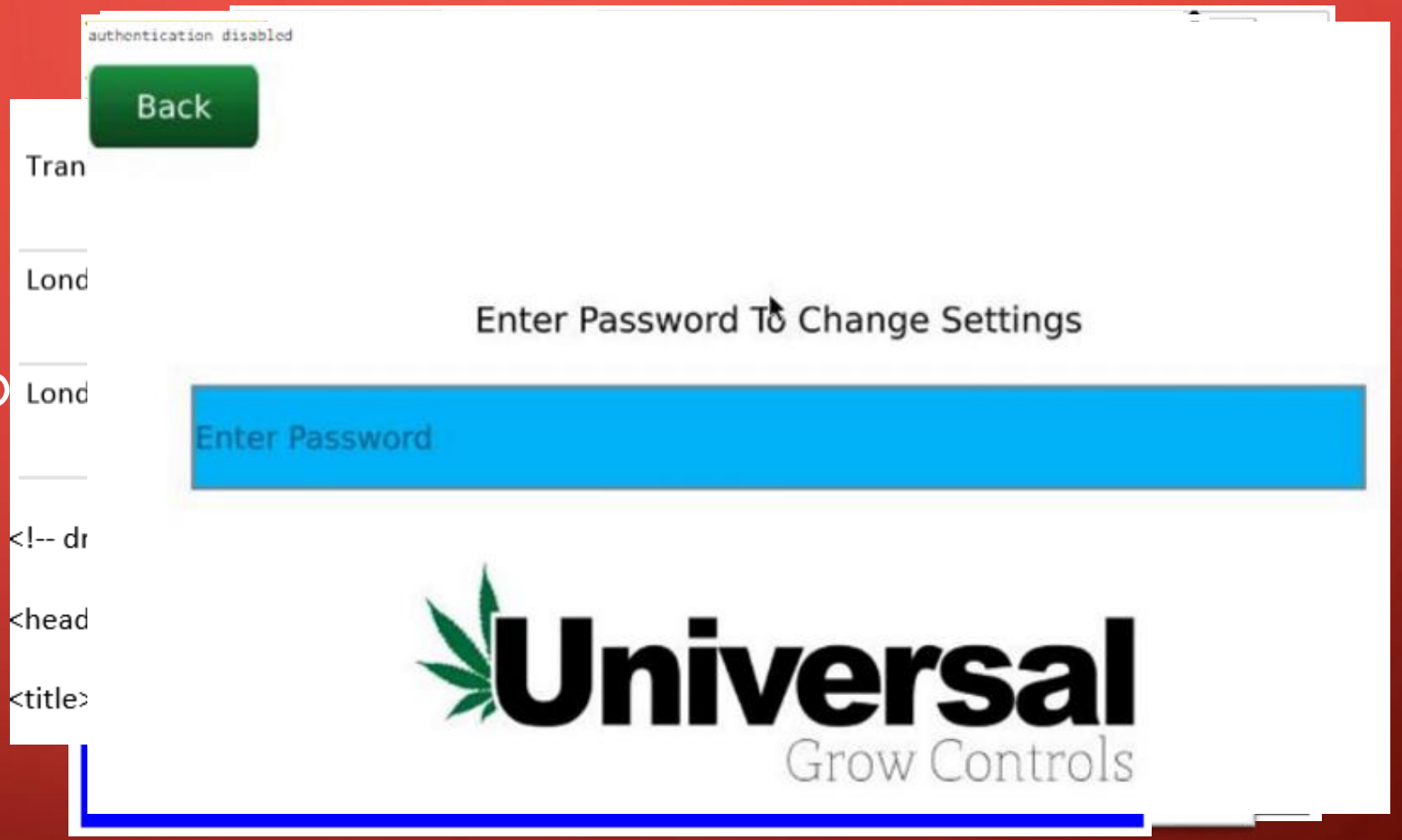


SECURITY & PRIVACY CHALLENGES

- Large number of access points
- Renewable energy systems entry points
- Electricity theft
- Most equipment privately owned
- Lacking standisation
- Security an afterthought

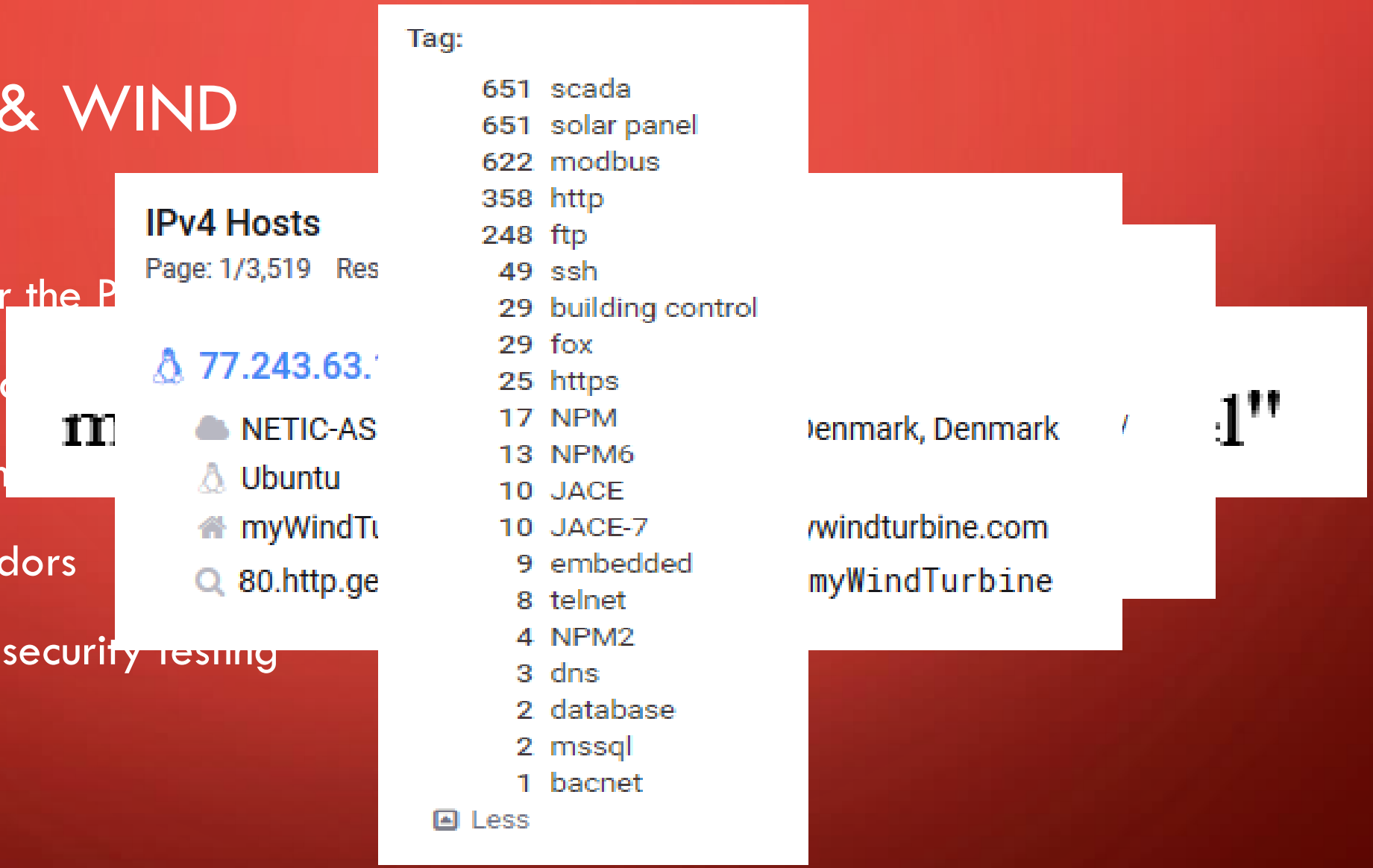
CRITICAL INFRASTRUCTURE

- Power plants
- Water systems
- Agriculture
- Hydroelectric D
- Railway
- Logistics
- Weed



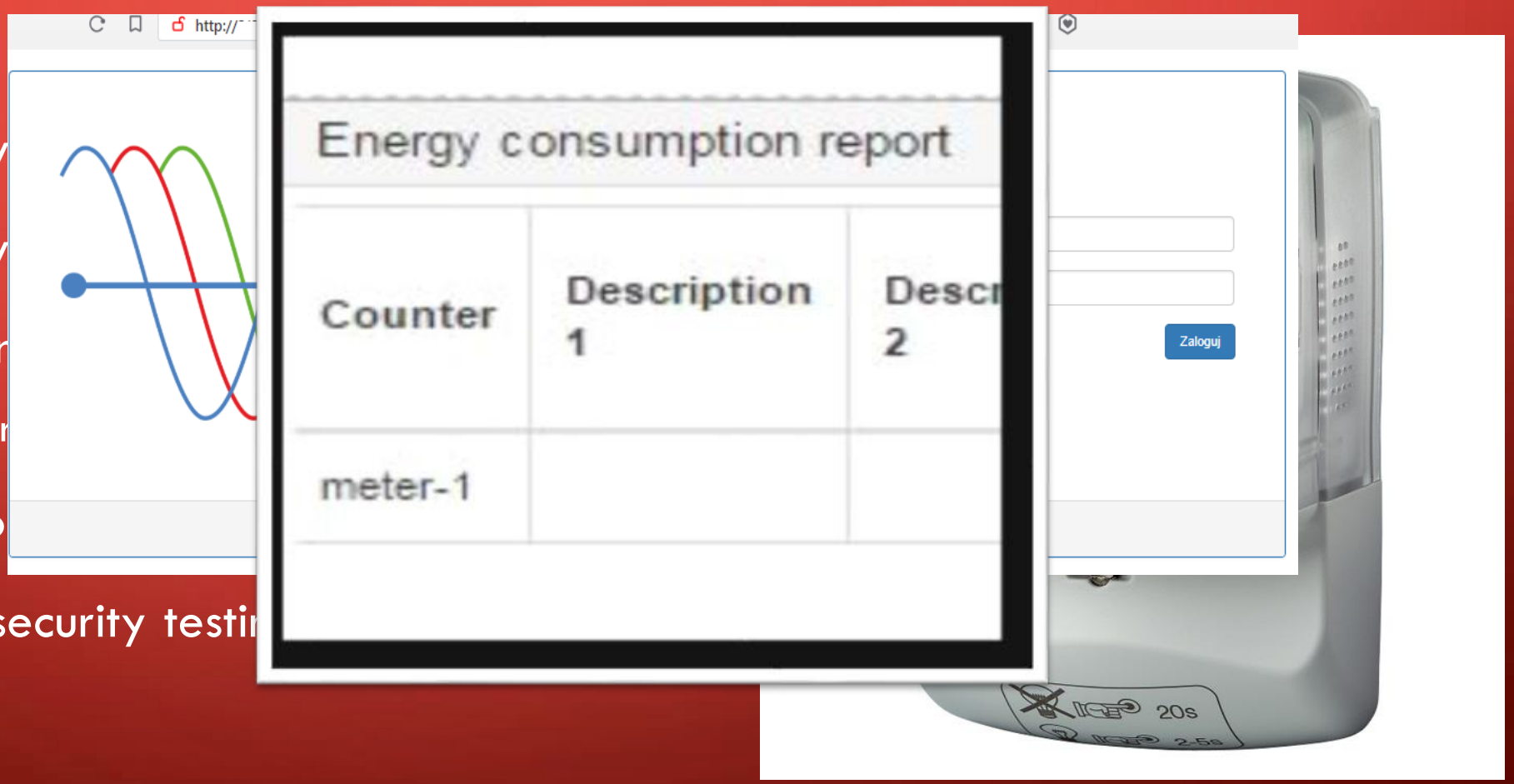
SOLAR & WIND

- Crucial for the P
- Load manc
- Climate ch
- Many vendors
- Not much security testing
- Bonus



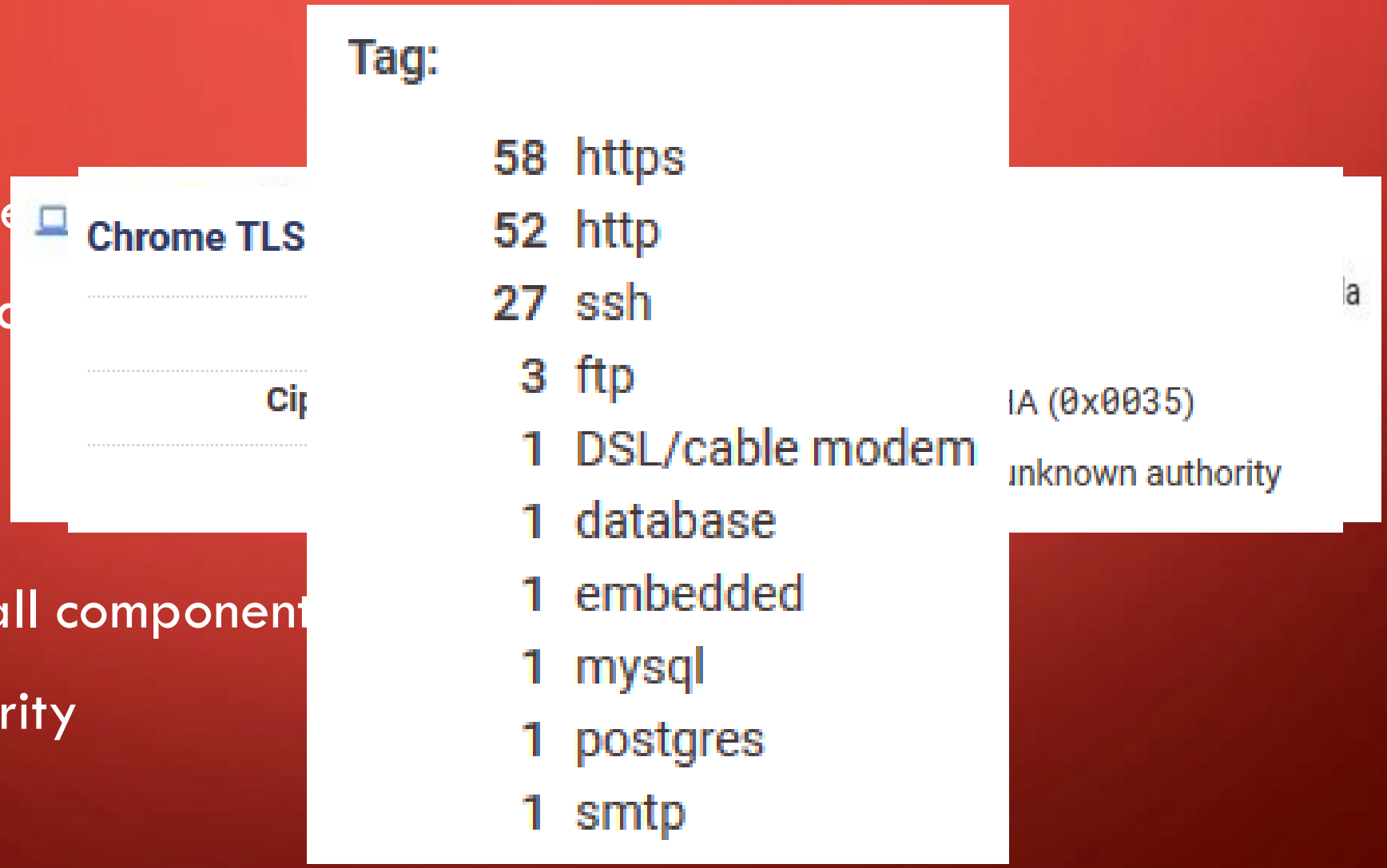
SMART ELECTRIC METERS

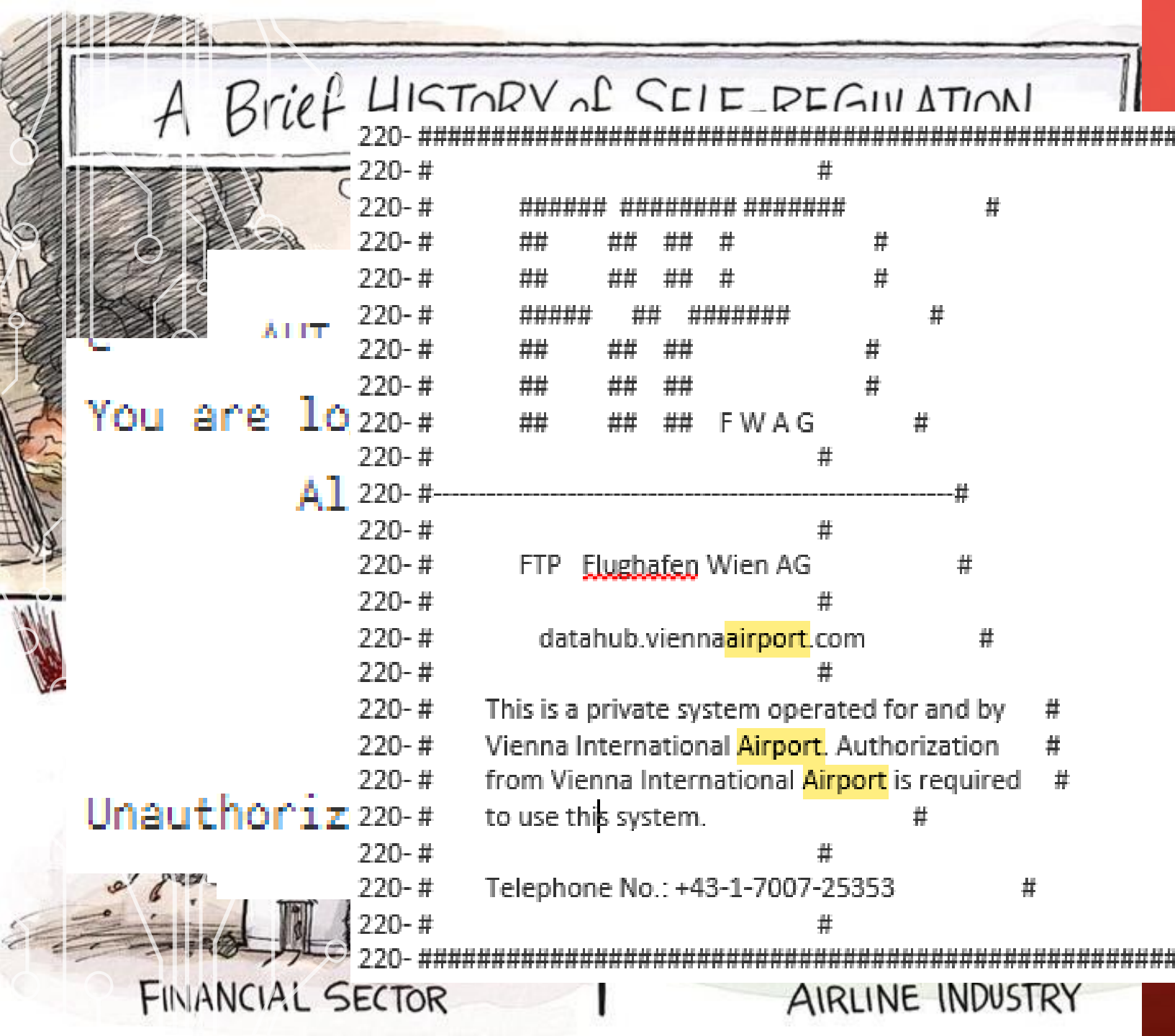
- Mandatory
- Mandatory
- Privacy cor
  - Can be r
- Security co
- No cyber security testi



OPEN AUTOMATED DEMAND RESPONSE

- North Ame
- Interopera
- Pricing
- Demand
- Controls all component
- Zero security






```
220-###############################################################
220-#                                 #
220-#      ###### ######## #######          #
220-#      ##     ##  ##  #          #
220-#      ##     ##  ##  #          #
220-#      #####    ##  #######          #
220-#      ##     ##  ##             #
220-#      ##     ##  ##             #
220-#      ##     ##  ##  FWAG       #
220-#                                 #
220-#-----------------------------------------#
220-#                                 #
220-#      FTP  Flughafen Wien AG           #
220-#                                 #
220-#        datahub.viennaairport.com          #
220-#                                 #
220-#    This is a private system operated for and by    #
220-#    Vienna International Airport. Authorization    #
220-#    from Vienna International Airport is required   #
220-#    to use this system.                  #
220-#                                 #
220-#    Telephone No.: +43-1-7007-25353          #
220-#                                 #
220-###############################################################
```

AVIATION

. Network Devices

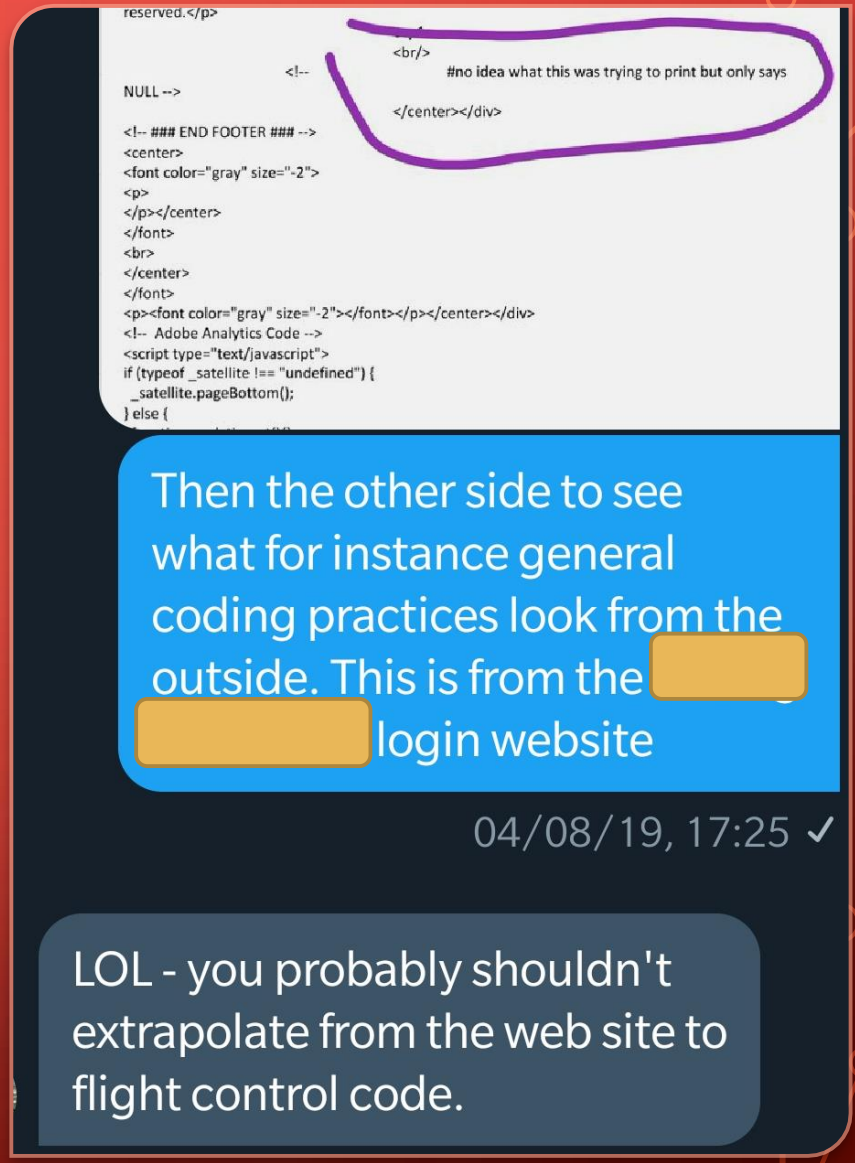
logged

lines.com

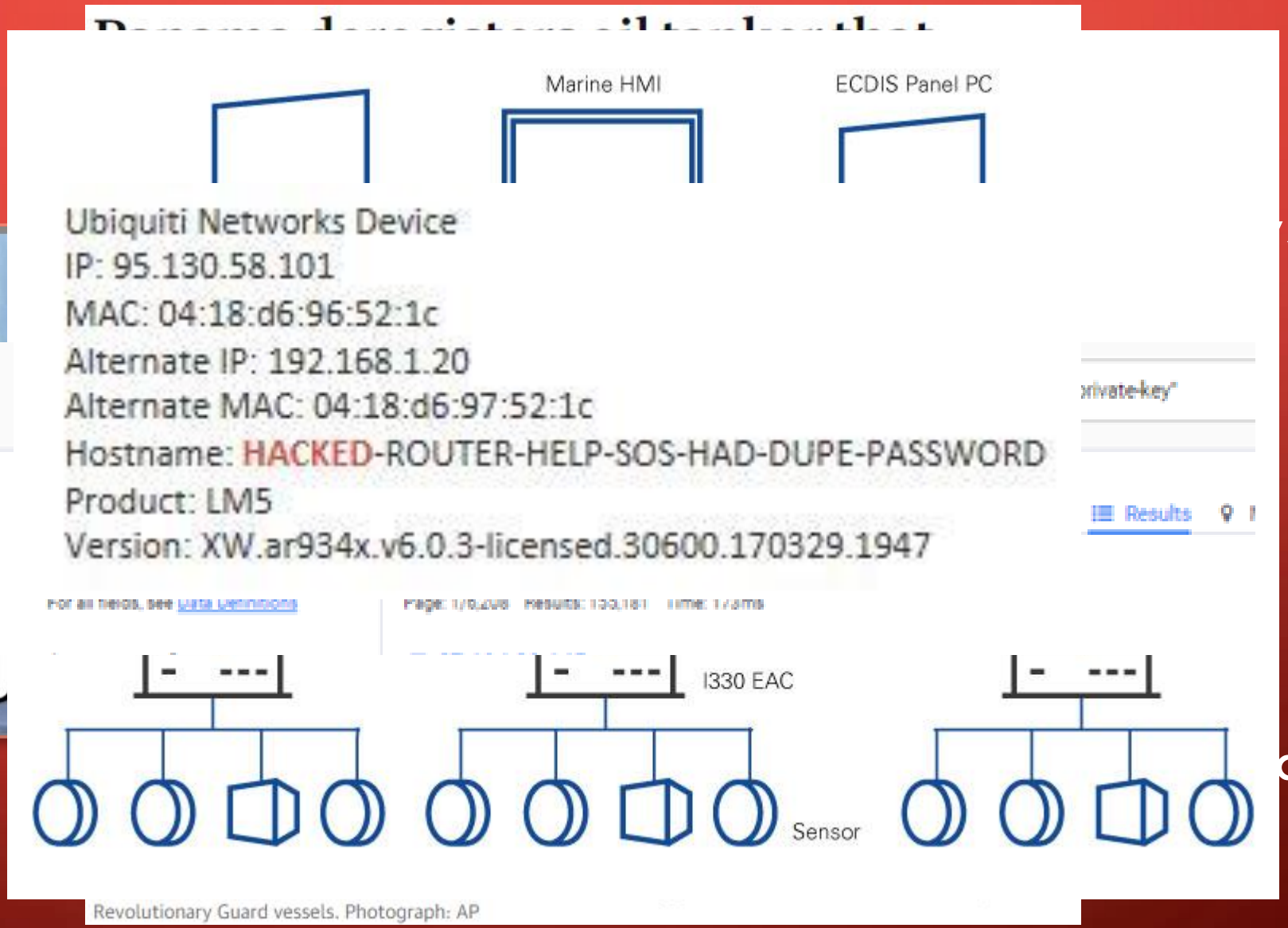
port

US AIRCRAFT MANUFACTURER

- No current coordinated disclosure




I SHOU

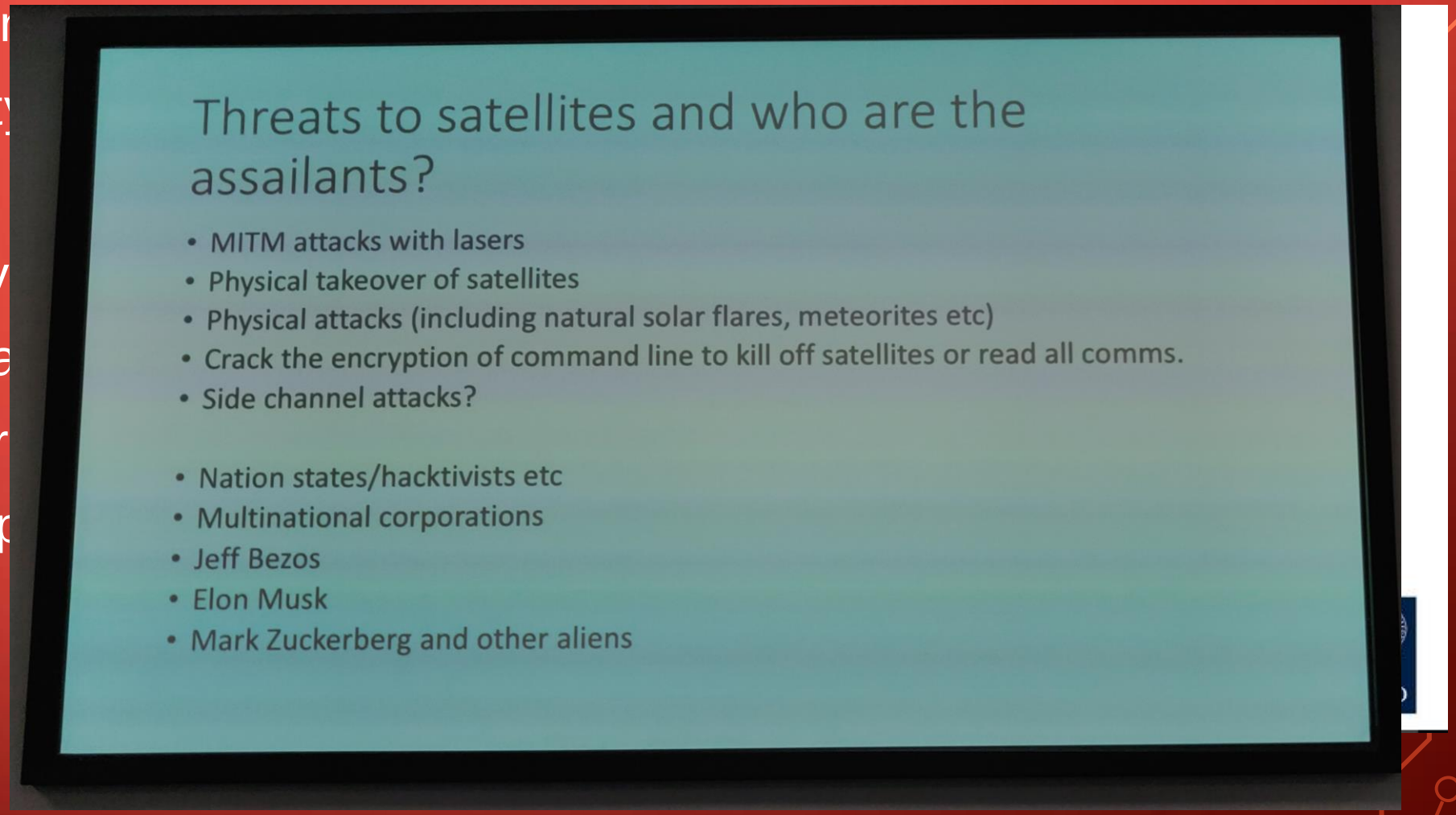

Marine HMI
ECDIS Panel PC
Ubiquiti Networks Device
IP: 95.130.58.101
MAC: 04:18:d6:96:52:1c
Alternate IP: 192.168.1.20
Alternate MAC: 04:18:d6:97:52:1c
Hostname: HACKED-ROUTER-HELP-SOS-HAD-DUPE-PASSWORD
Product: LM5
Version: XW.ar934x.v6.0.3-licensed.30600.170329.1947
I330 EAC
Sensor
Revolutionary Guard vessels. Photograph: AP

stem

d IIOT

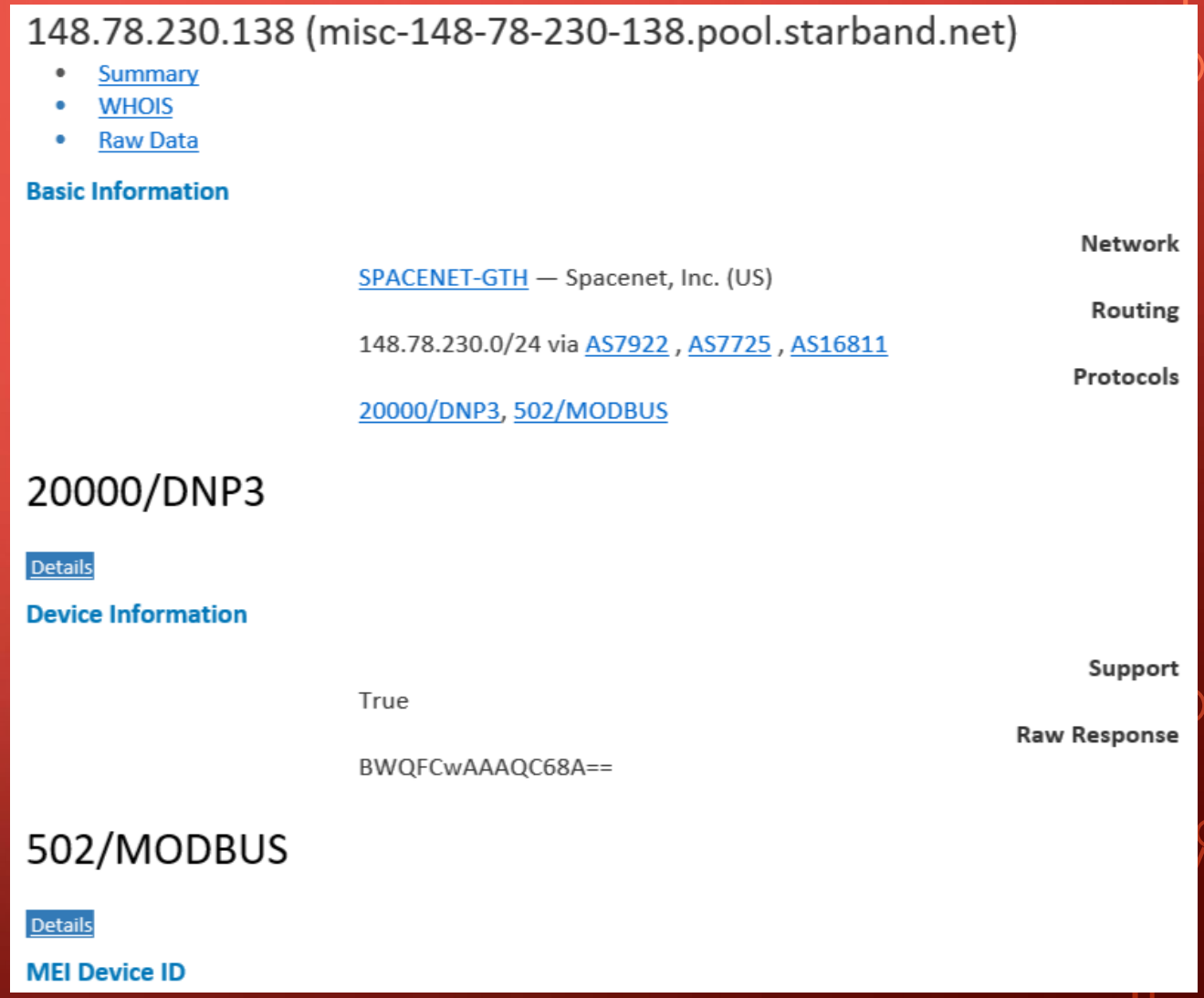
SPACE ASSET CHALLENGES

- Legacy equipr
- Interoperabilit
- IOT
- Lack of Encry
- Nation-state a
- Solar weather
- Radiation flipp
- Surveillance
- Manipulation
- Debris
- Loss of visibility
- Low cost uncontrolled launches



DISCOVERING IOT SPACE ASSETS

- Tool used Censys.io
- Free
- Vulnerabilities
  - DNP3 Protocol
  - Modbus Protocol
- Working to expand Censys


148.78.230.138 (misc-148-78-230-138.pool.starband.net)

- Summary
- WHOIS
- Raw Data

Basic Information

Network

SPACENET-GTH — Spacenet, Inc. (US)

Routing

148.78.230.0/24 via AS7922 , AS7725 , AS16811

Protocols

20000/DNP3, 502/MODBUS

20000/DNP3

Details

Device Information

Support

True

Raw Response

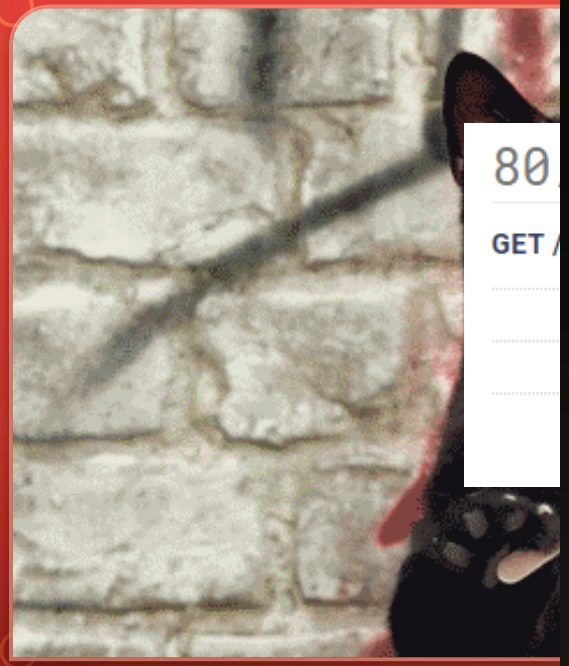
BWQFCwAAAQC68A==

502/MODBUS

Details

MEI Device ID

SE?



http://[redacted].adsl.highway.telekom[redacted]

NO GIMMICKS.
REAL SMART HOMES.

Loxone Web Interface

Username

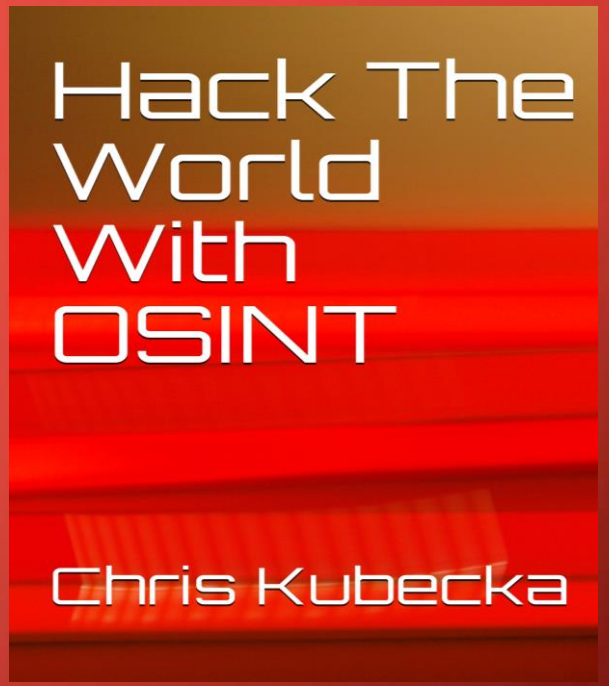
Password

Connect

iele
R BESSER

iele & Cie. KG

QUESTIONS & THANK YOU



- Thanks to @Beauwoods @Orbit_RRI & @UnivOxford, FAIR Space Hub, Royal Holloway, EU Commission

- Darknet Diaries Shamoon episode 30
- https://en.m.wikipedia.org/wiki/Chris_Kubecka
- *When the internet gives you remotely exploitable systems, take them. They're like free candy, right?*

- Chris Kubecka