ACER

European Union Agency for the Cooperation of Energy Regulators

Forum ElCom 2022

18 November 2022

Cyber risks: Overview – from best practices to worst case scenario

by

Stefano BRACCO

(Stefano.BRACCO@acer.europa.eu)

ACER
European Union Agency for the Cooperation of Energy Regulators

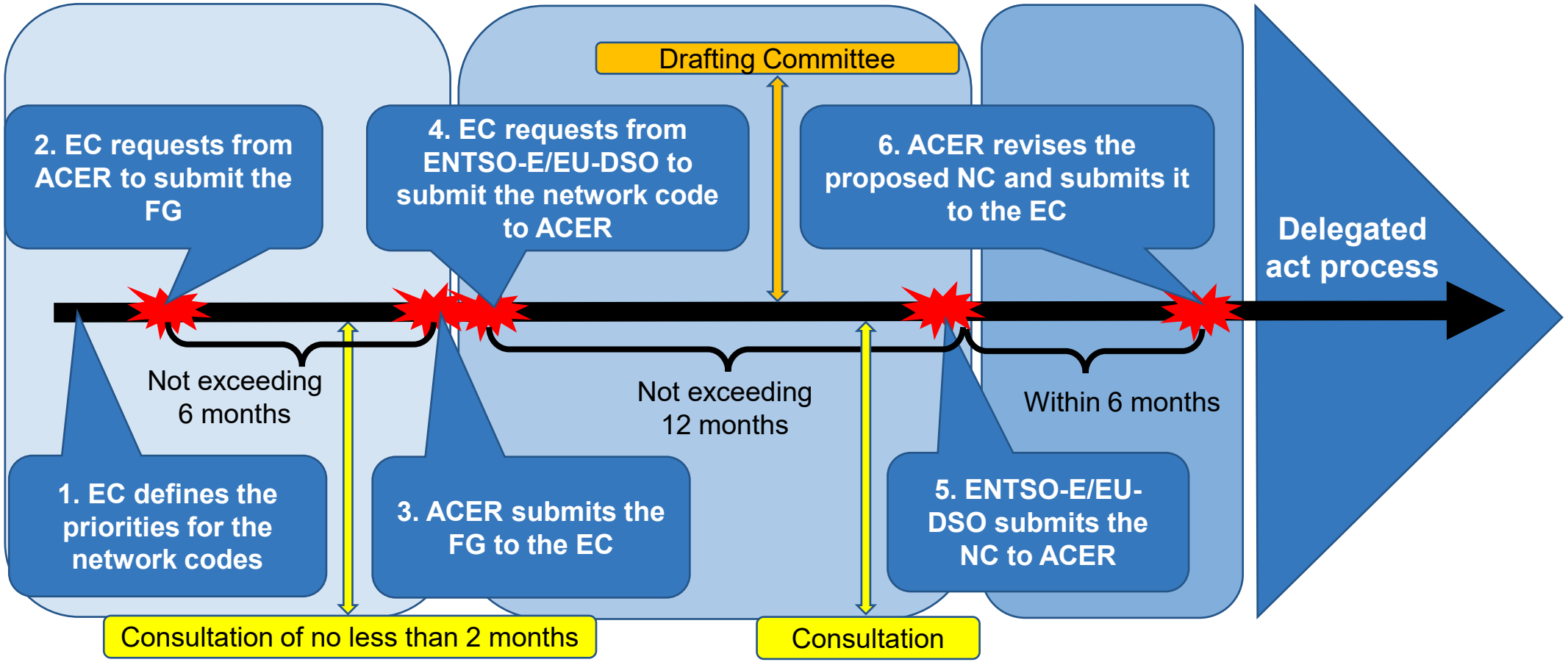
The perfect cyberspace for Electricity…..
That doesn't exist.

ACER
European Union Agency for the Cooperation of Energy Regulators

Regulate or ……..!?!?

Costs of regulation….

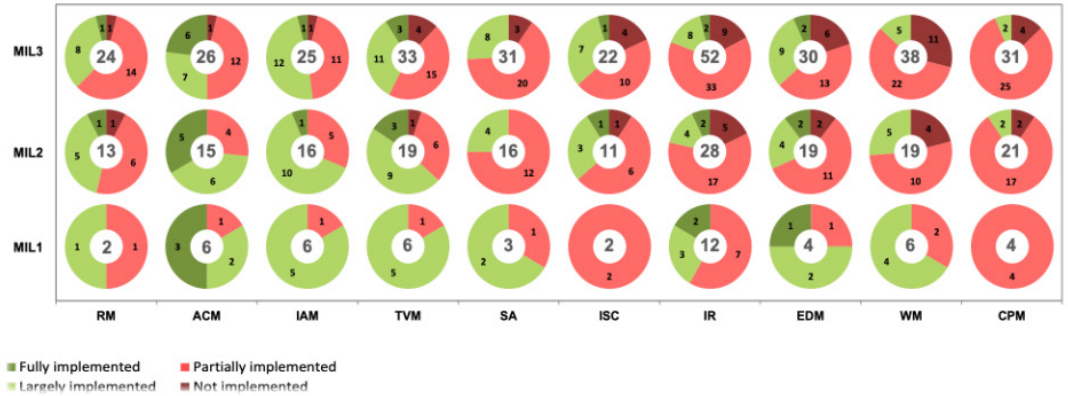
General timeline as set out in Article 59 of REGULATION (EU) 2019/943



ACER
European Union Agency for the Cooperation of Energy Regulators

Other best practices to investigate….

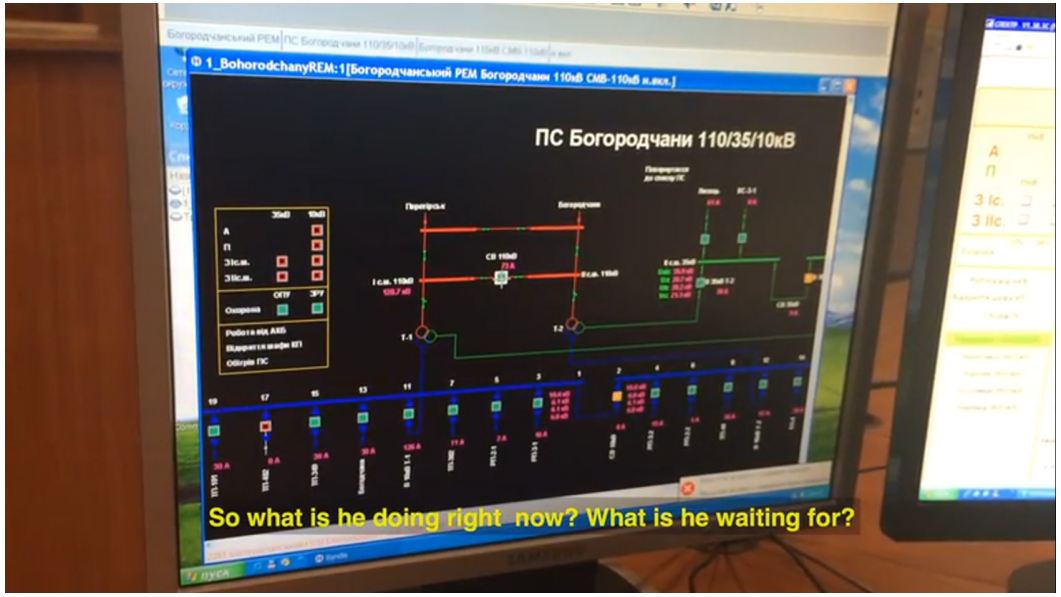
- ✓ Use of existing **STANDARDS** (e.g. ISO and NIST)
- ✓ Use of other tools and guidelines (e.g. C2M2)

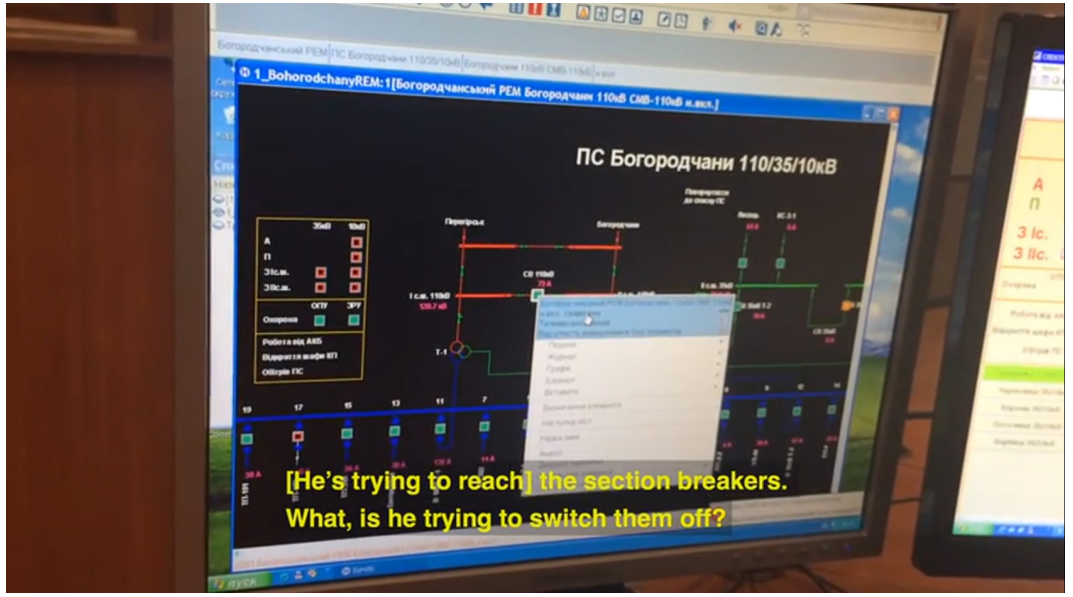


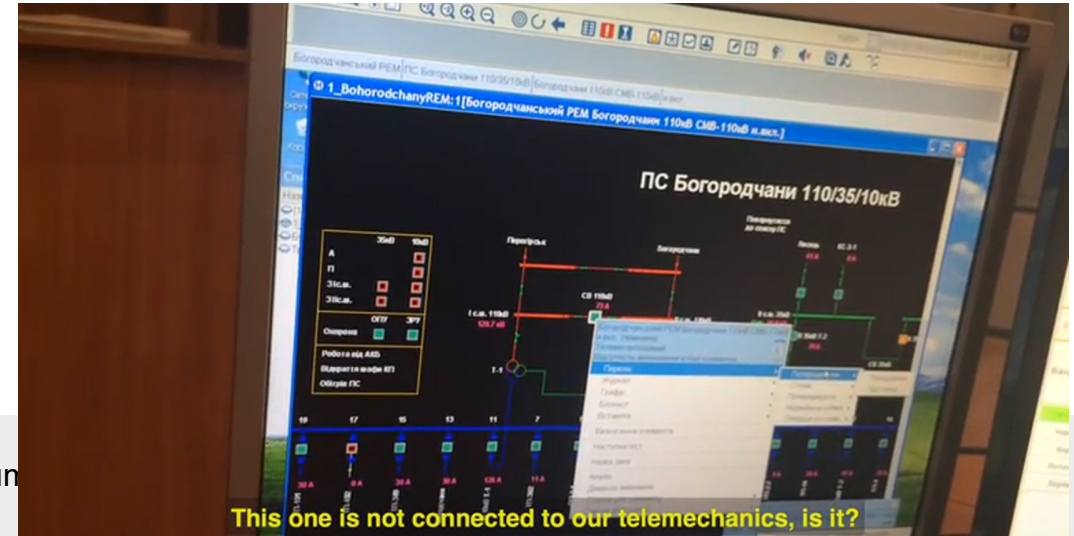
1. Risk Management
2. Asset & Change Management
3. Identity & Access Management
4. Threat & Vulnerability Management
5. Situational Awareness
6. Information Sharing & Collaboration
7. Incident Response
8. Supply Chain Management
9. Workforce Education
10. Cybersecurity Program Management

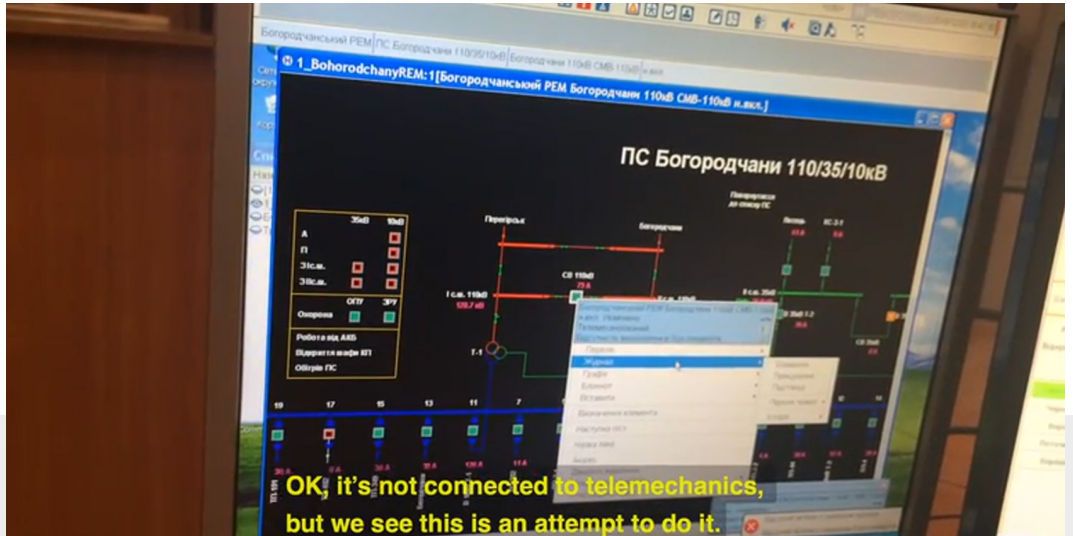
ACER
European Union Agency for the Cooperation of Energy Regulators

Worst case scenario…..

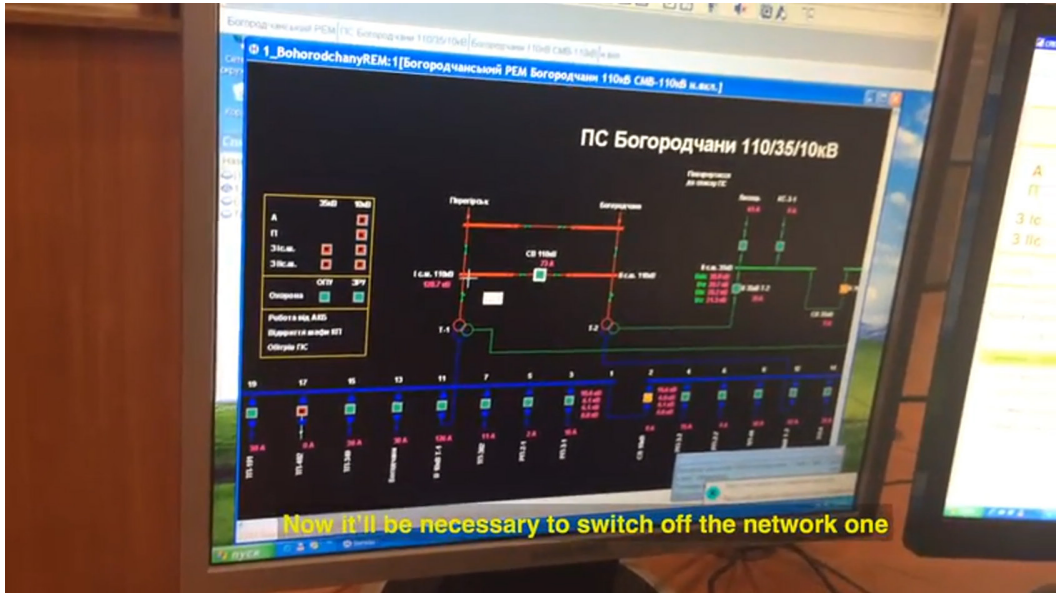


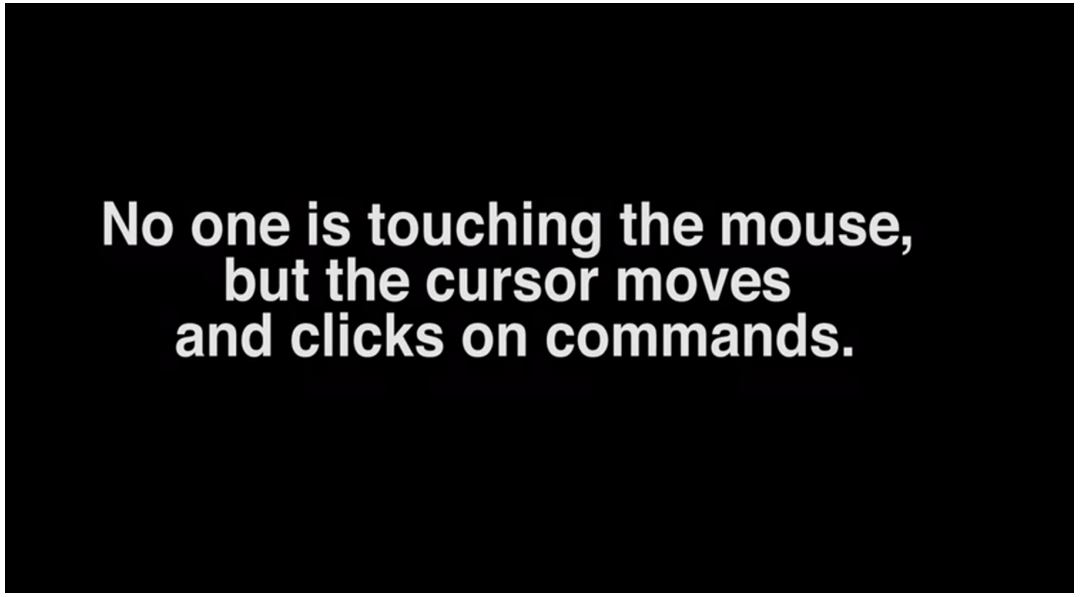


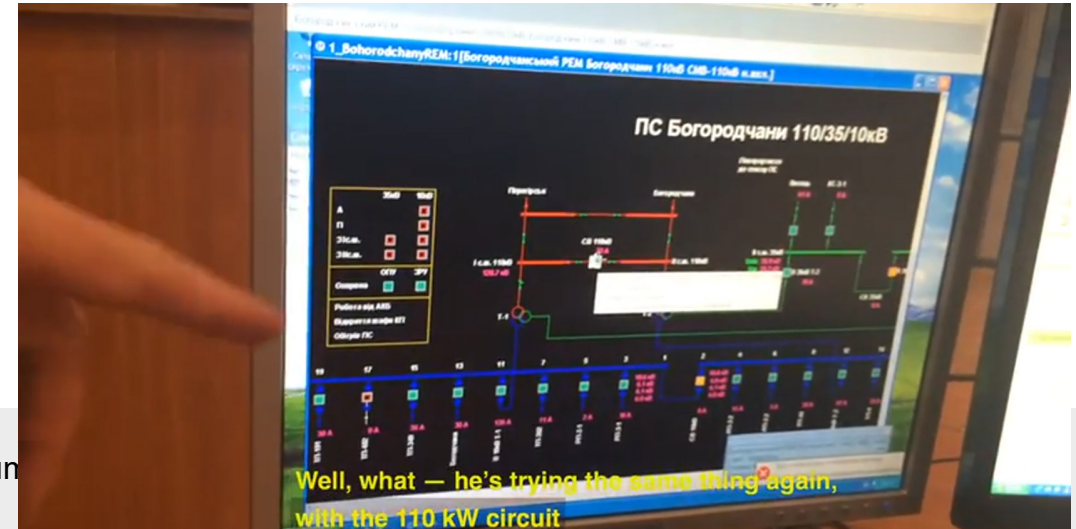


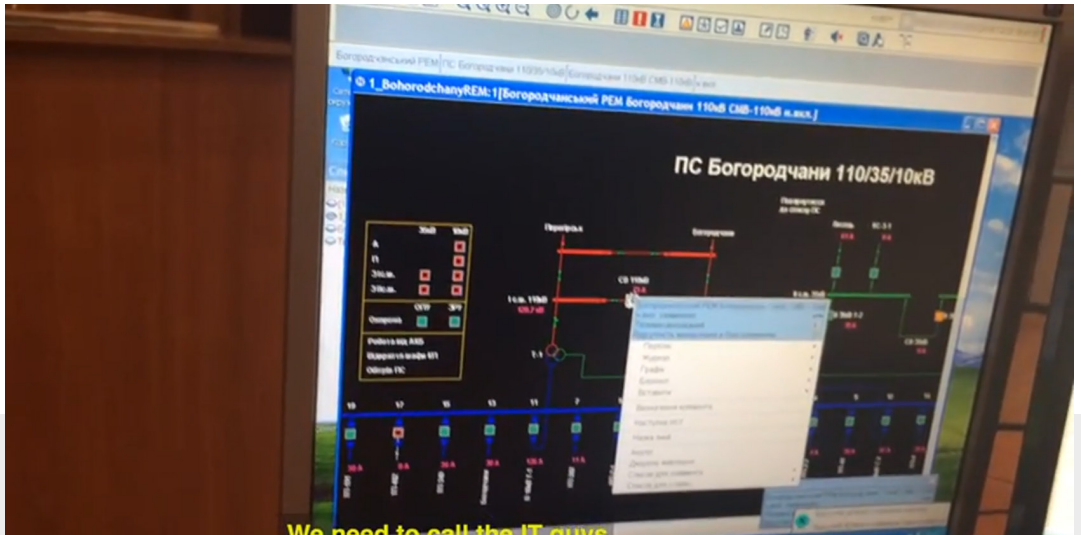


Worst case scenario…..

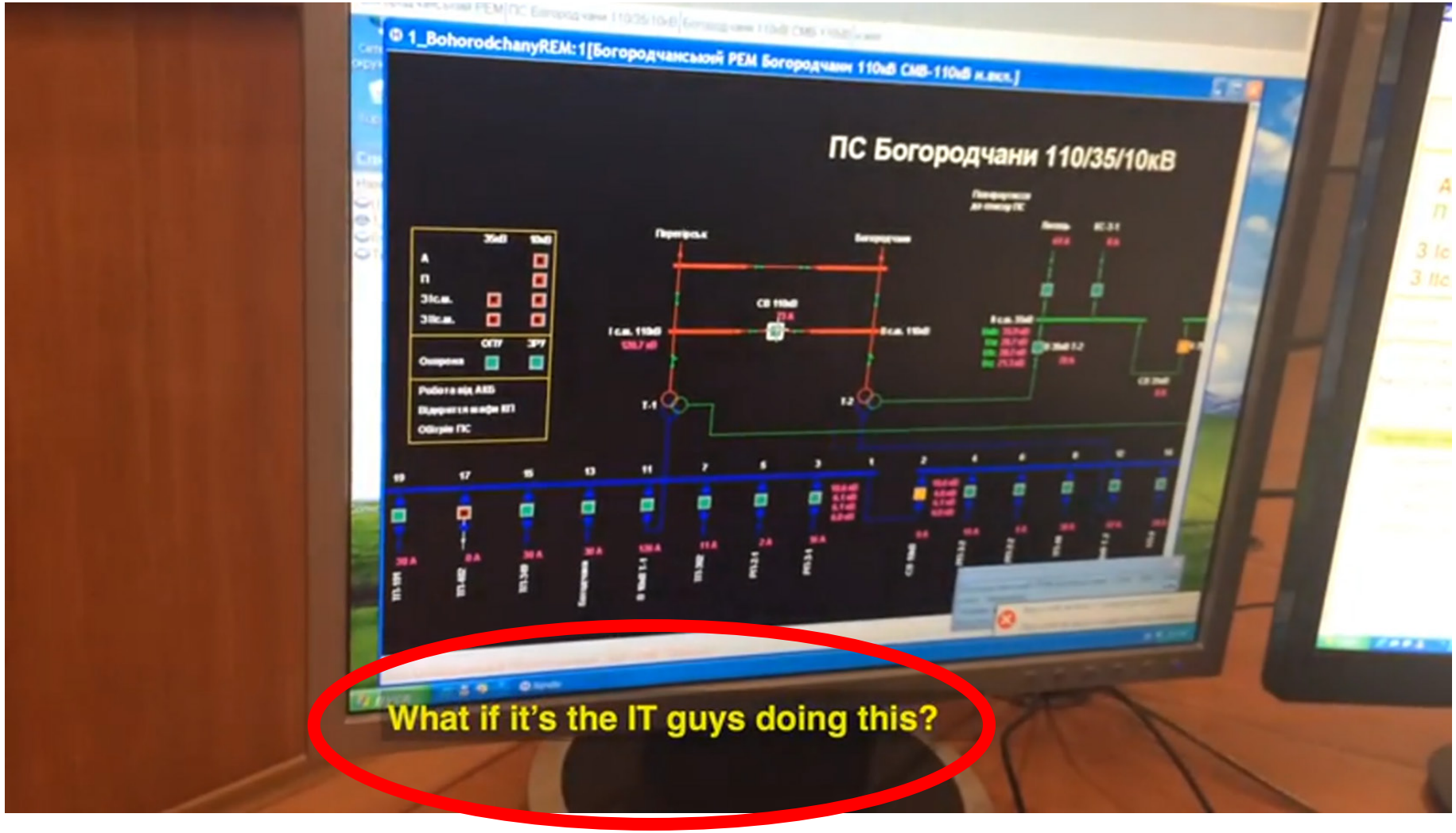








Worst case scenario…..



ACER
European Union Agency for the Cooperation of Energy Regulators

Reality check on a cyber attack to the grid: Ukraine 2015

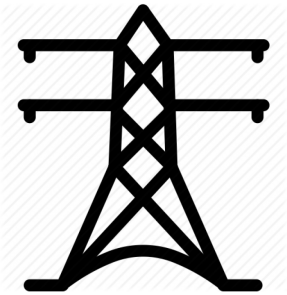
23 Dec 2015 h 15:35

3 DSOs affected

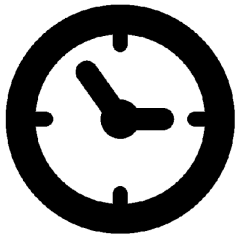
225.000

103 Cities and Towns Affected

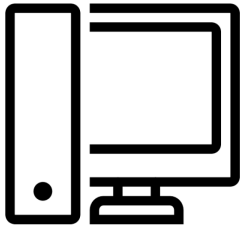
135 MW
Impact



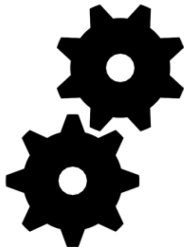
7 x 110 KV SubStations
23 x 35 KV SubStations (up to 50)



3.5 to 7 hours Outage Duration



100s Damaged



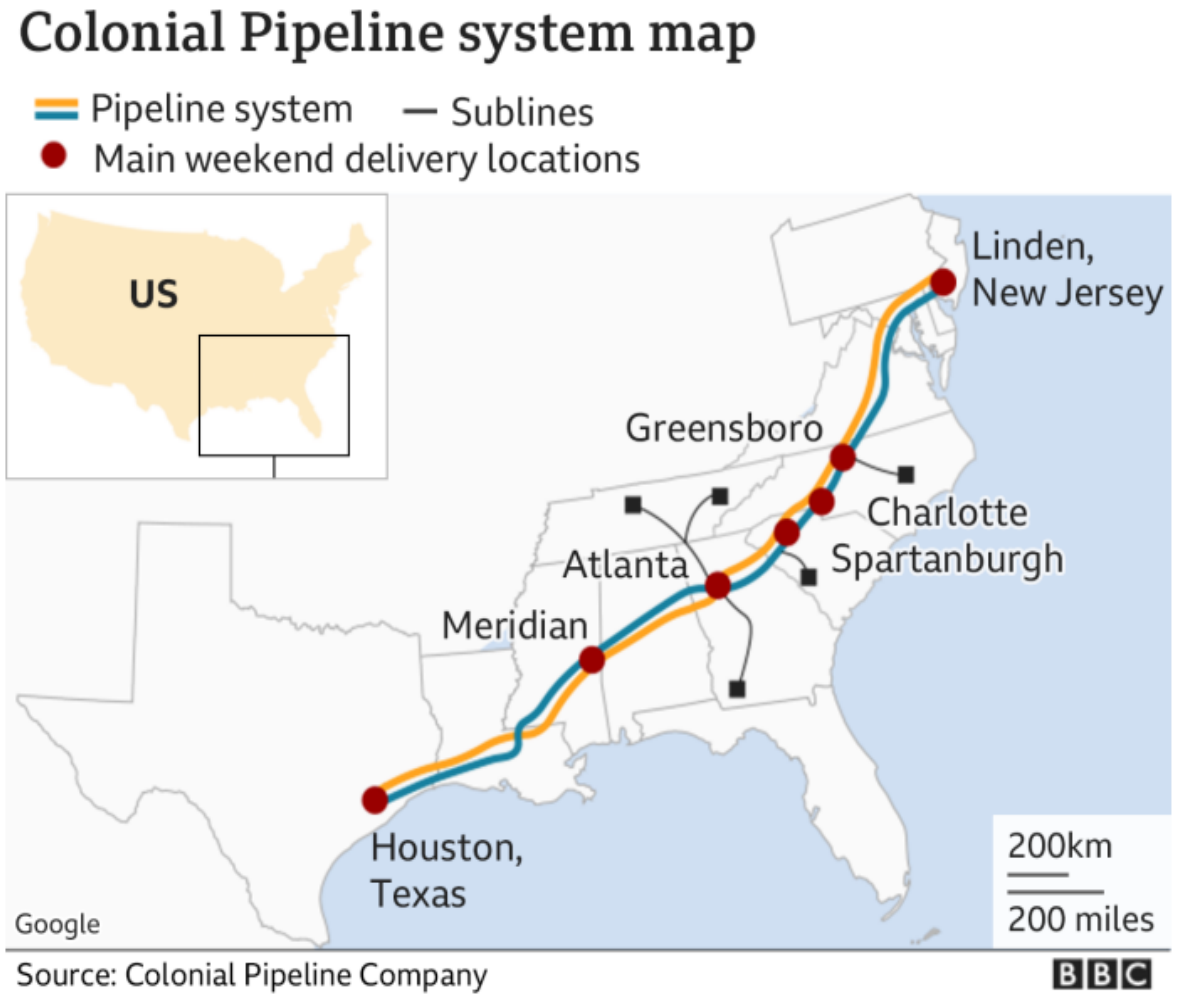
10s Field Device Affectes

Outside Temp. Between 4 and -8° Cent.

(Source: SANS ICS - ICS.SANS.ORG)

ACER
European Union Agency for the Cooperation of Energy Regulators

Reality check on a cyber attack to smart energy infrastructure: Colonial Pipeline 2021



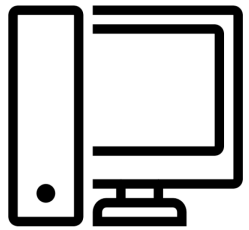
ACER
European Union Agency for the Cooperation of Energy Regulators

Reality check on a cyber attack to a smart and distributed energy infrastructure: Colonial Pipeline 2021

6 May 2021

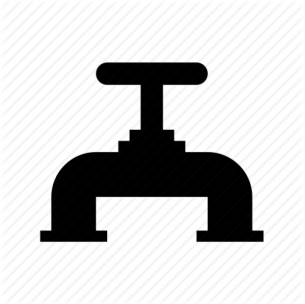
1 single operator affected

2.5 millions barrels per day not delivered

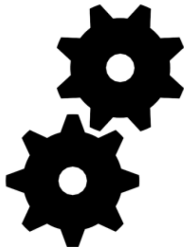


Ramsonware on company's systems in charge of business operations

N millions

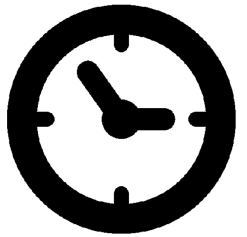


Gasoline, diesel, jet fuel and other refined products through 5,500 miles (8,850 km) of pipelines



0 Field Device Affected

45% of fuel used along the Eastern Seaboard



- May 6, 2021 (data stolen)
- May 7, 2021 (malware attack)
- May 12, 2021 (pipeline restarted after payment of 4.4 Mln Ramson/75 Bitcoins)

ACER
European Union Agency for the Cooperation of Energy Regulators

The worst is right in front of you…. And it is unconventional!

ACER
European Union Agency for the Cooperation of Energy Regulators

Conclusions

- The worst case scenario will never be defined. Don't neglect risks, anticipate them.
- Regulation is important but don't wait, plan efforts already today, if possible, in cooperation with others and on your level.
- Start looking in unconventional ways to tackle the problem (as a community): understand the economy of cybersecurity, invest in digital diplomacy and how you can contribute, and many other collateral topics. This is an efficient and mature way to look at the problem and to find a solution in the medium-long term.

WARNING: rules for wars and conflicts do not apply one to one to DIGITAL CONFLICTS, so aggressiveness of cyber-adversaries is unpredictable.

Thank you!
Any questions?

ACER
European Union Agency for the Cooperation
of Energy Regulators

info@acer.europa.eu
acer.europa.eu
@eu_acer
linkedin.com/in/EU-ACER/

ACER
European Union Agency for the Cooperation of Energy Regulators

Many thanks for your attention!

My E-Mail: stefano.bracco@acer.europa.eu