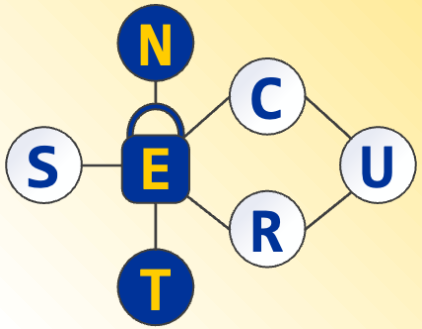


Enhancing Cross-Sectoral Collaboration in Cybersecurity in Estonia, Czechia, Lithuania, Ukraine, and the Netherlands

Funded by the European Union

Context and Problem: Cybersecurity of Substations in Wartime

16-06-2026

9:00-12:00 CET (Czechian / Dutch time)

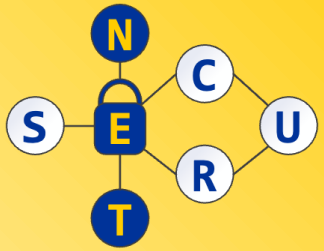
10:00-13:00 EET (Estonian/ Lithuanian/ Ukrainian time)

Speaker: Veronika Latyshevska

Engineer of project management group, strategic planning department, JSC "Prykarpattyaoblenergo"

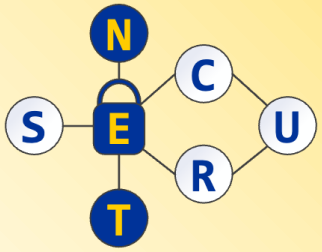
Funded by the European Union Horizon Europe programme under Grant Agreement No. 101217315. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Agenda



1	Why substations matter in wartime
2	Wartime pressure on the energy operator
3	Physical and cyber resilience are connected
4	Physical threats affect operational capability
5	Cyber attacks against energy infrastructure are not theoretical
6	Limitations of traditional SCADA and OT interfaces
7	Human factor and fragmented information
8	Why a new visual layer is needed

Why substations matter in wartime



0.4–110 kV
Distribution System Operator

24,500 km
Overhead lines

6,600
Transformer substations

JSC “Prykarpattyaoblenergo” - Distribution System Operator

Power distribution infrastructure in western Ukraine

555,000
Consumers

1,700 km
Cable lines

130
High-voltage substations

Critical infrastructure supporting households, hospitals, businesses, transport, and public services.

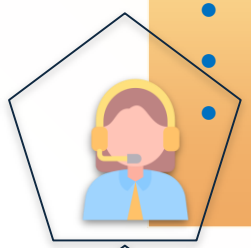
Wartime pressure on the energy operator

Personnel pressure

- mobilisation of employees
- limited staffing
- workload increase

Emergency communication

- fast internal updates
- unstable communication channels
- messaging channels (WhatsApp, Telegram etc.)



Remote coordination

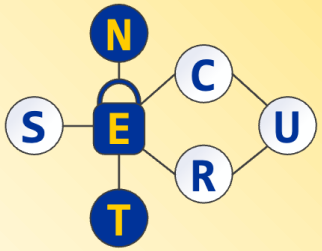
- coordination between field teams
- dispatch centres and management
- remote training and support

Safety Procedures

- work during air alerts
- emergency operating conditions
- rapid decision-making under pressure

Cybersecurity in wartime is also about helping operators understand the situation quickly and act correctly under pressure.

Physical and cyber resilience are connected



Physical infrastructure

- substations
- power supply
- field equipment

Communication

- reserve Internet
- backup channels
- Starlink terminals

OT Systems

- SCADA
- RTUs
- automation devices

Operators

- situational awareness
- remote coordination
- restoration activities

Customers

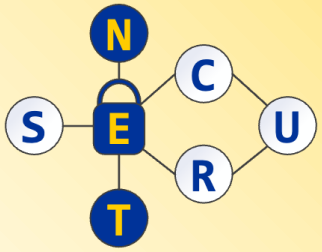
- households
- hospitals
- businesses

Backup power | Reserve communication | Generators | Shelters | Starlink

Physical threats affect operational capability

Physical damage can affect maintenance, testing and restoration capability.

Cyber attacks against energy infrastructure are not theoretical



2015

Ukrainian power grid cyber attack

- operational disruption
- SCADA/security lessons learned

Small source:
E-ISAC / SANS

2016

Industroyer / CrashOverride

- malware targeting grid operations

Small source:
Dragos

2022

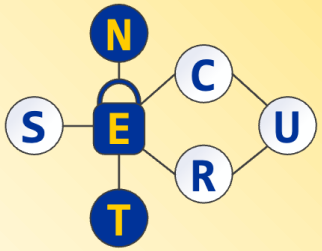
Industroyer2 attempt

- attack against Ukrainian energy sector prevented

Small source:
CERT-UA

Cyber threats can affect real operational processes, communication, and situational awareness in the grid.

Limitations of traditional SCADA and OT interfaces



Alarms

- events
- notifications

SCADA

- electrical parameters
- topology
- switching

Maintenance Database

- maintenance history
- inspections

OPERATOR

Documentation

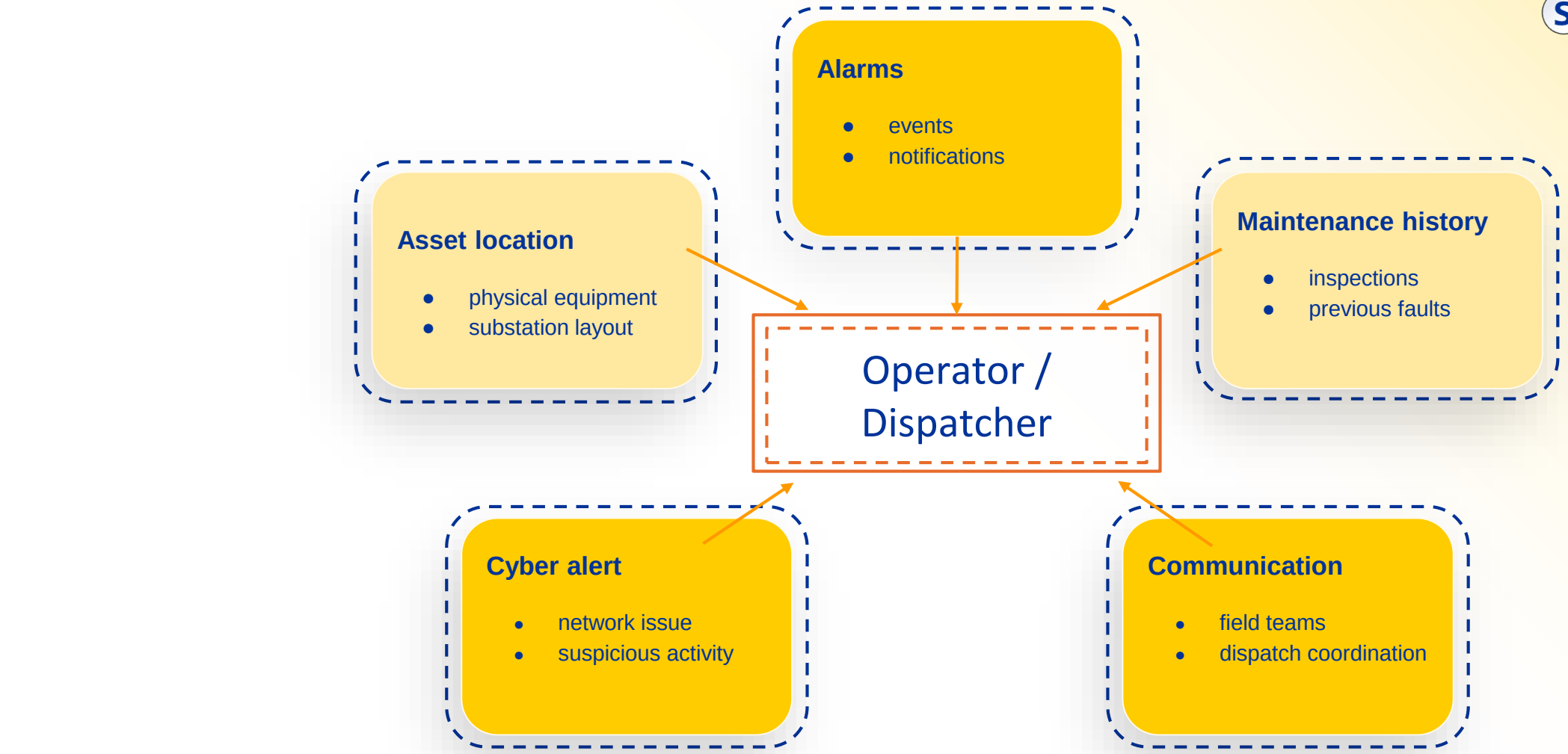
- technical documentation
- asset information

Cyber Monitoring

- security alerts
- network monitoring

Information exists, but it is distributed across multiple systems and interfaces.

Human factor and fragmented information



Clarity | Speed | Context | Reduced workload

Human-system interaction directly affects operational resilience and cybersecurity.

Why a new visual layer is needed

Real Substation

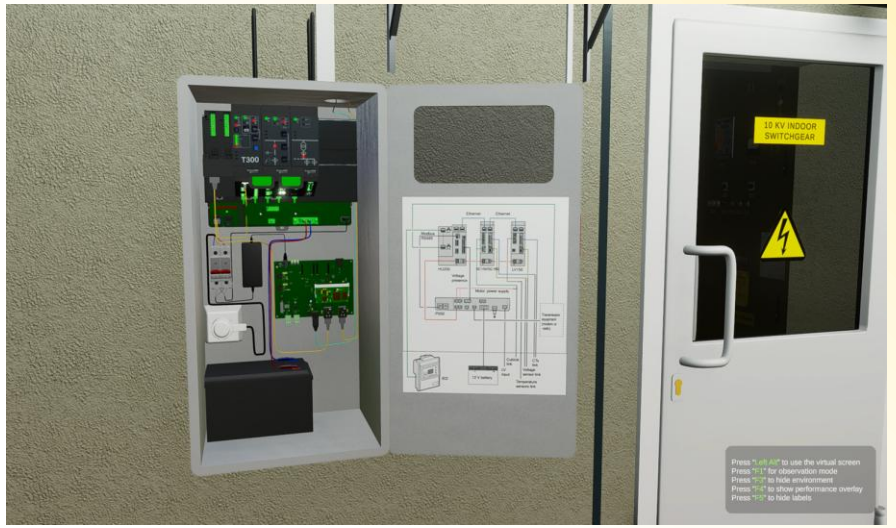
- physical infrastructure
- equipment
- operational environment

Digital Representation

- BIM model
- laser scanning
- Unity environment

Contextual Information Layer

- maintenance information
- cyber awareness
- asset context
- training support



THANK YOU FOR YOUR ATTENTION!

ПРИКАРПАТТЯ ОБЛЕНЕРГО

Funded by
the European Union

eFORT