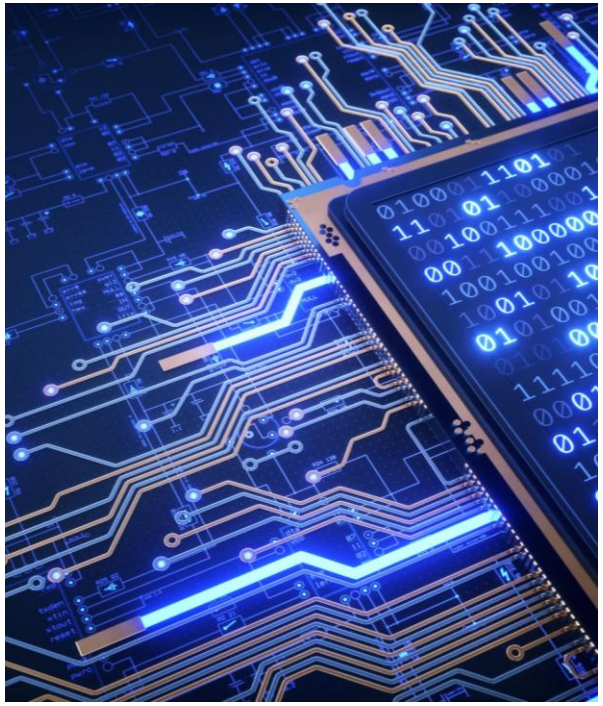


UPPSALA
UNIVERSITET

# Cybersecurity and Threat Landscape of the Electric Grid

STandUP for Energy
30 September 2026
Engla Rencelj Ling, Postdoc, engla.rencelj.ling@angstrom.uu.se

# Motivation



The electric grid is a complex cyber-physical system of many parts



The energy sector is a target in the current threat landscape



Where are we vulnerable and what defences are there?

# The Swedish Electricity Transmission Grid

- Ca 16 000 km lines
- 180 substations
- Balancing the 50 Hz



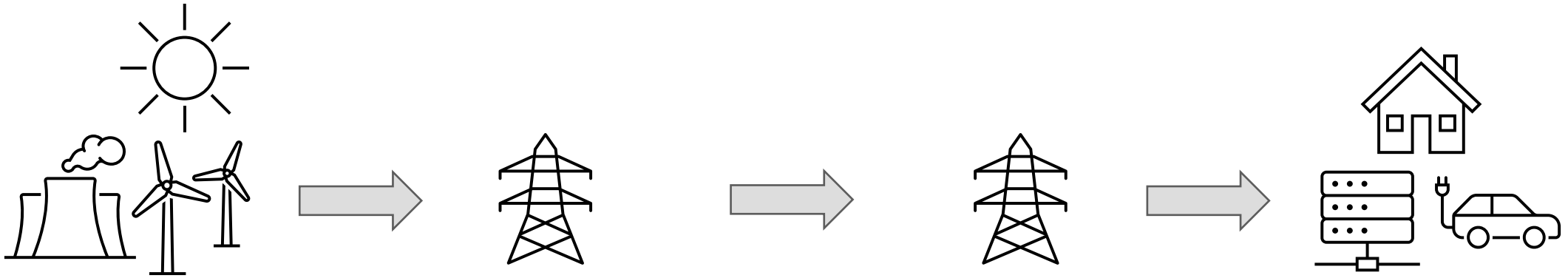

Consumption

Generation

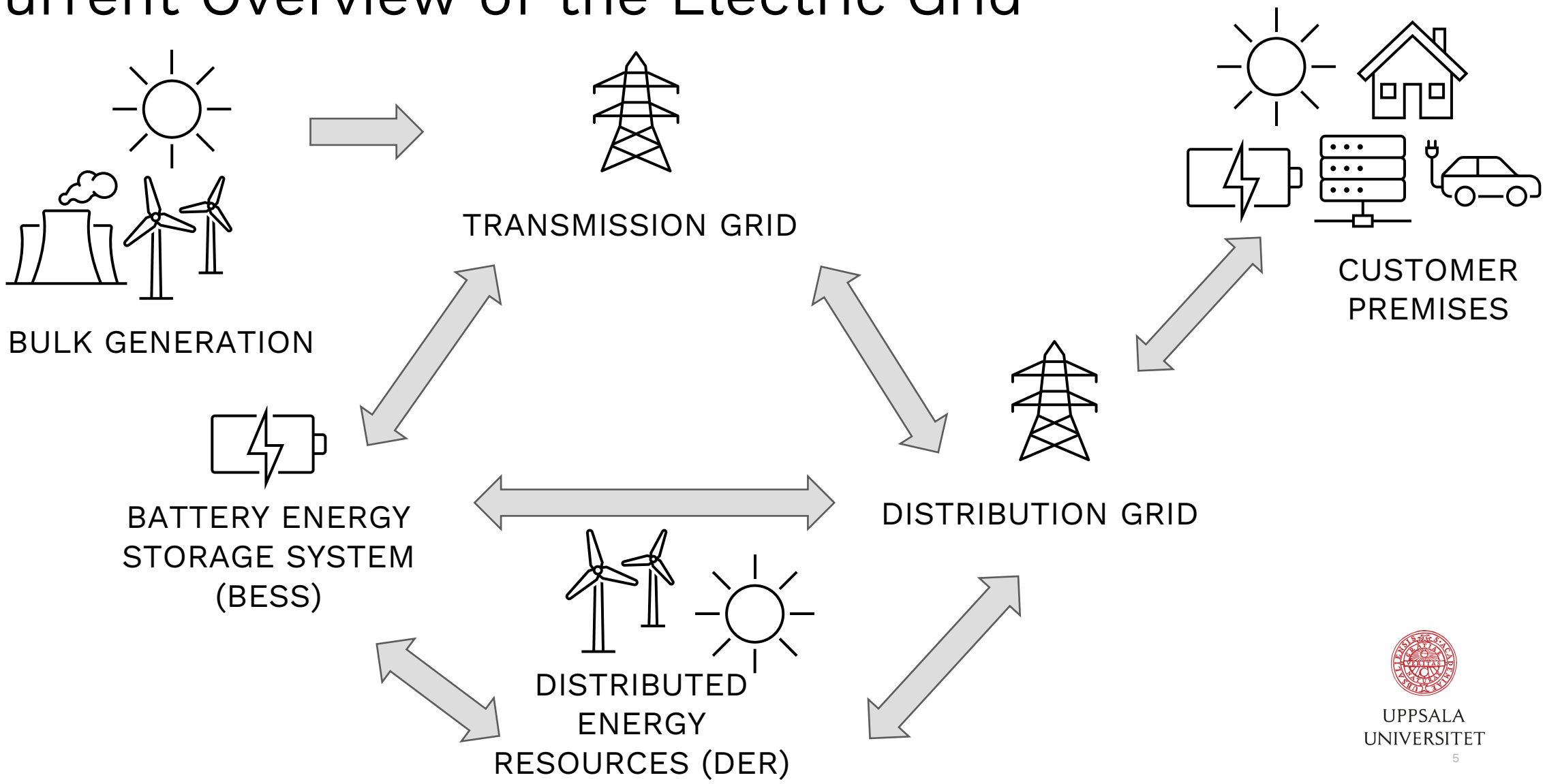
UPPSALA UNIVERSITET

https://www.svk.se/om-kraftsystemet/om-transmissionsnatet/transmissionsnatskarta/

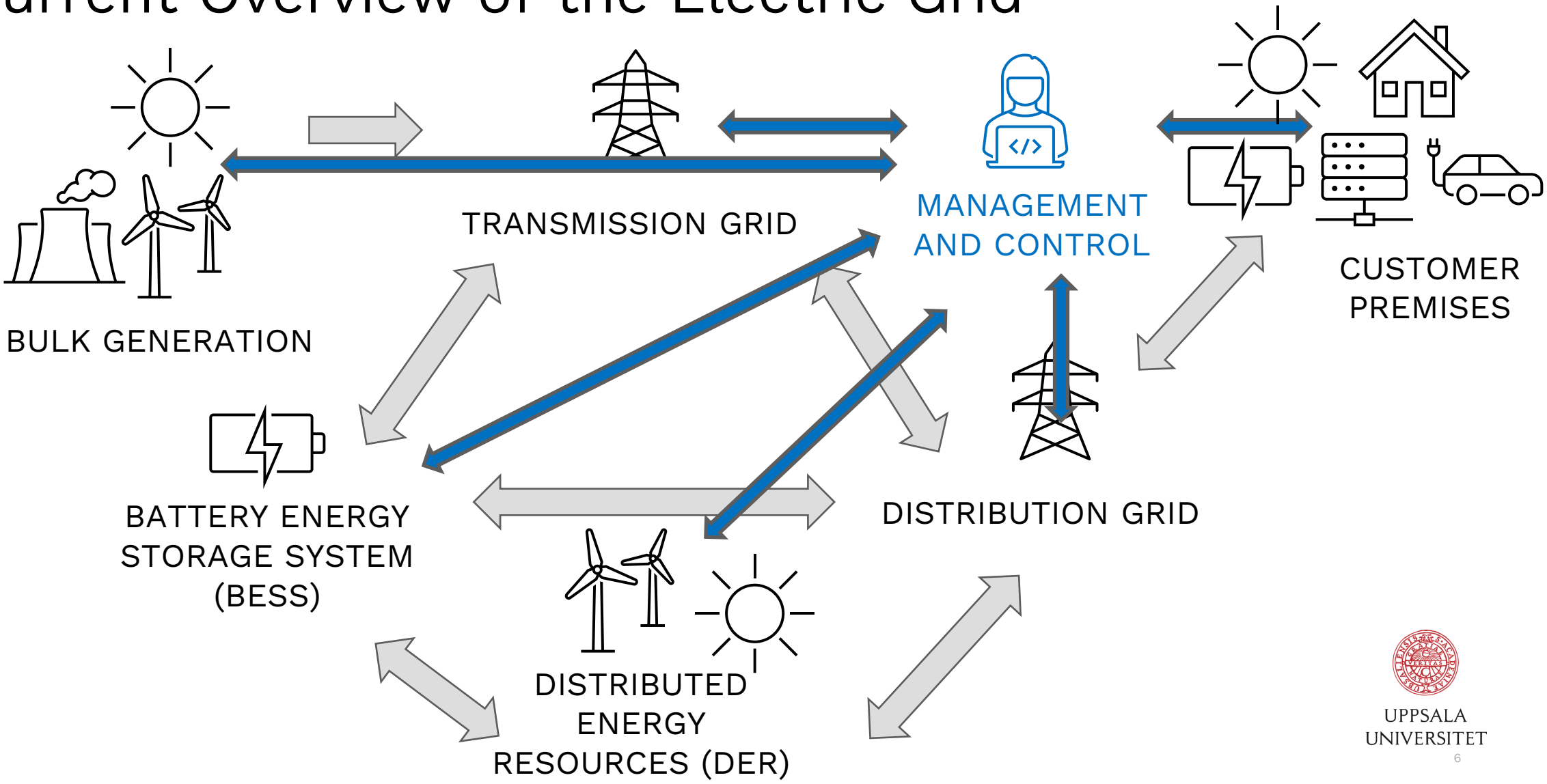
# Traditional Overview of the Electric Grid



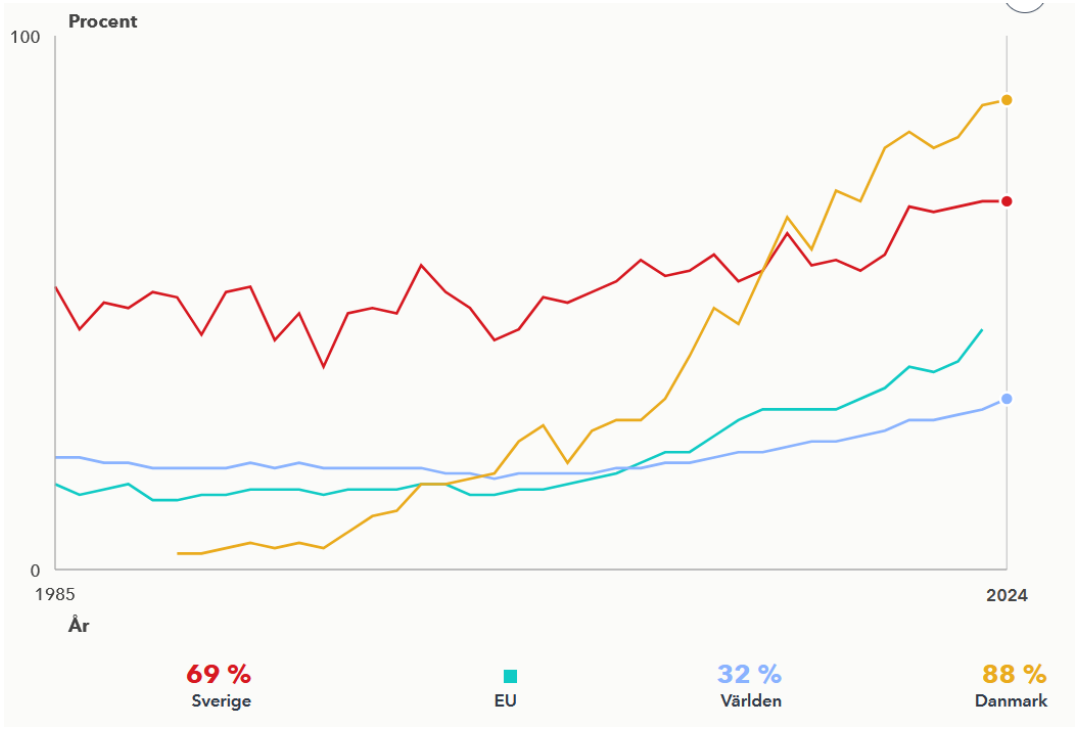
# Current Overview of the Electric Grid

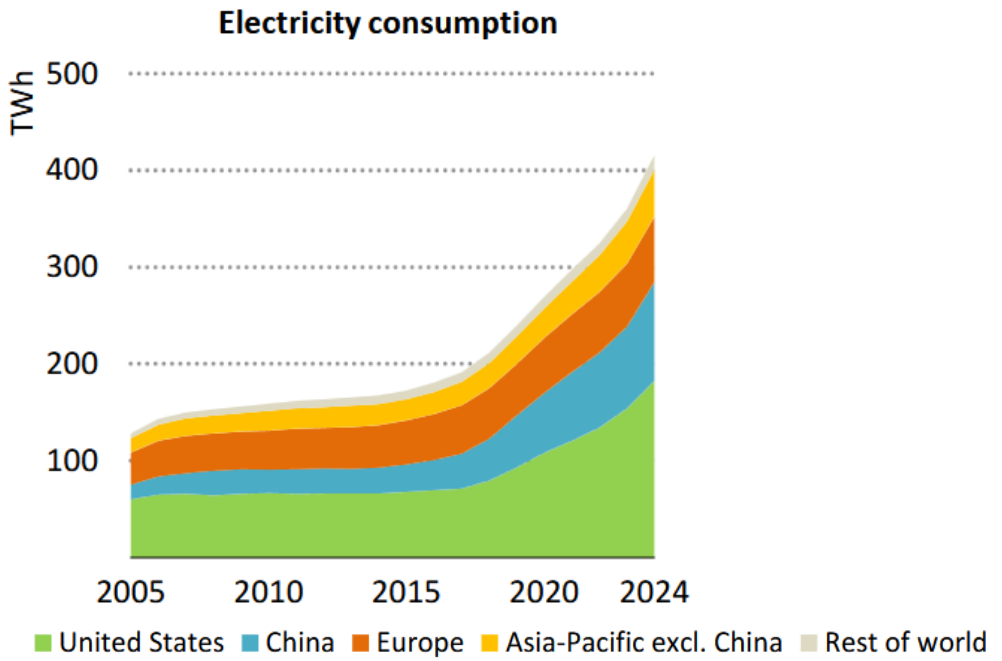


# Current Overview of the Electric Grid



# The energy sector is gaining more attention




Increase in Renewable Energy Resources

Increase in datacentre electricity consumption

https://www.ekonomifakta.se/sakomraden/energi/energiproduktion/elproduktion-med-fornybara-energikallor-internationellt_1208635.html

https://iea.blob.core.windows.net/assets/de9dea13-b07d-42c5-a398-d1b3ae17d866/EnergyandAI.pdf

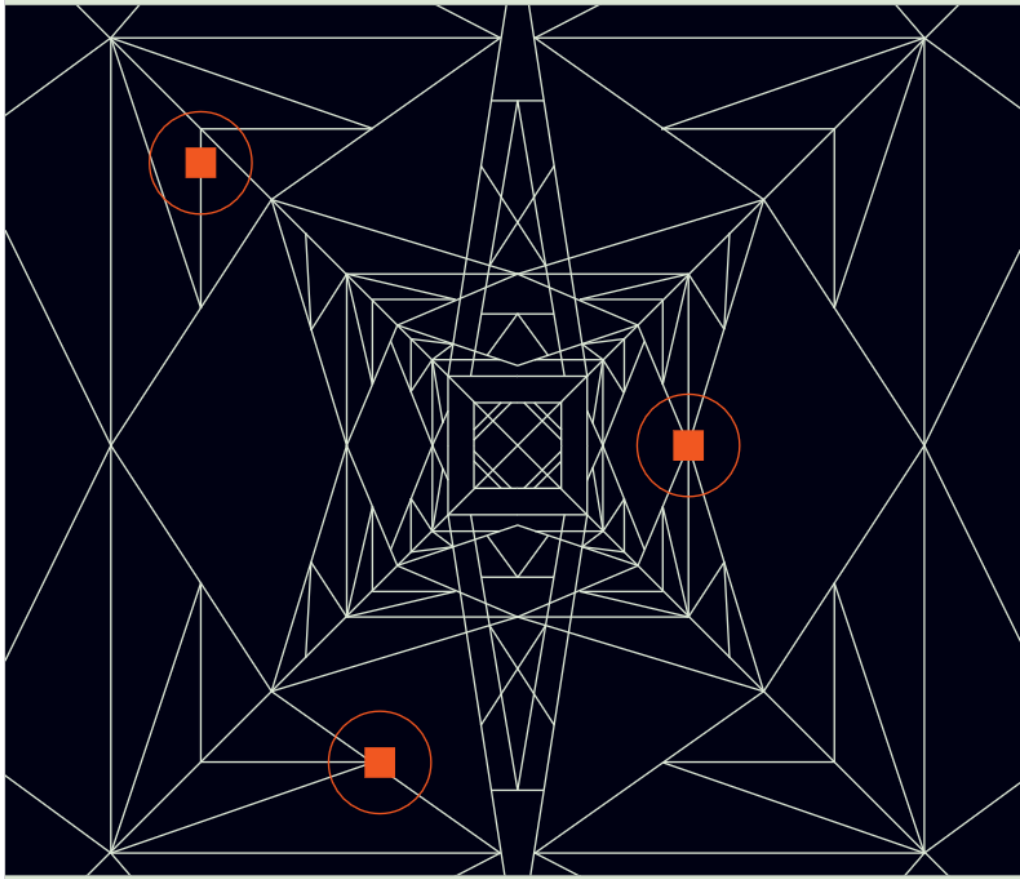
UPPSALA UNIVERSITET



# Threat Landscape

- Protecting critical infrastructure is essential
- It’s not a question of **if**, but **when**
- NIS2, Cybersecurity law
- “Fight AI with AI”

UPPSALA UNIVERSITET



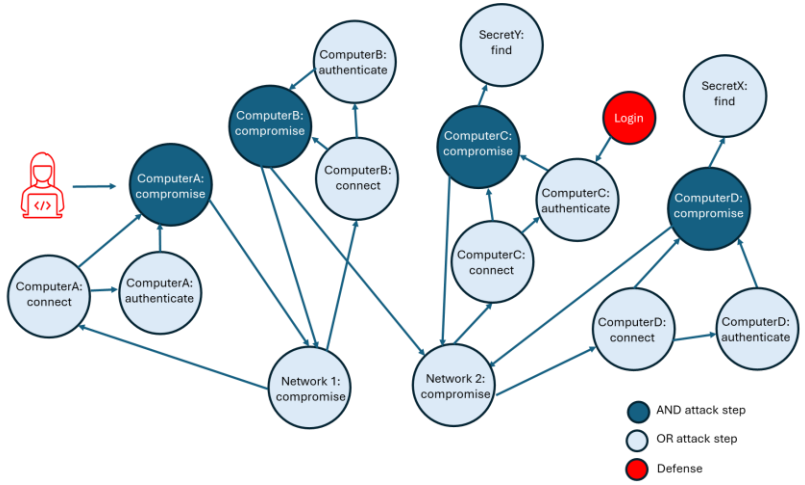

# DER attack

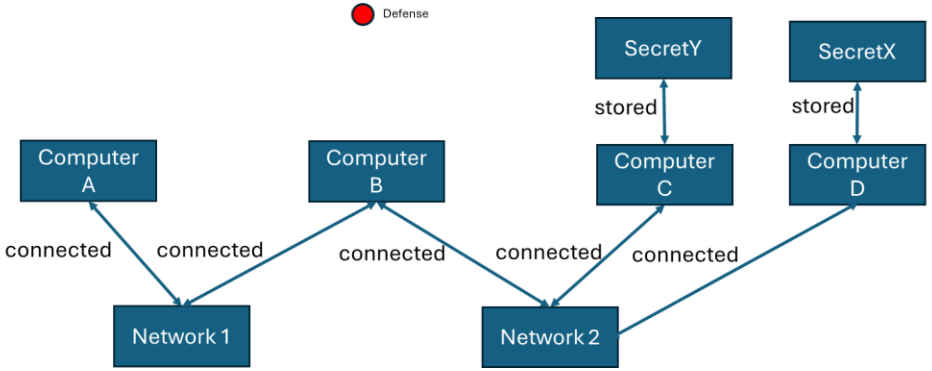
- 29 December 2025
- Coordinated attack against Poland
  - At least 30 wind power and solar panel plants
  - One manufacturer
  - One electric heating plant
- Affected both IT and OT
- The attackers were fully aware and target oriented

UPPSALA UNIVERSITET



https://cert.pl/uploads/docs/CERT_Polska_Energy_Sector_Incident_Report_2025.pdf



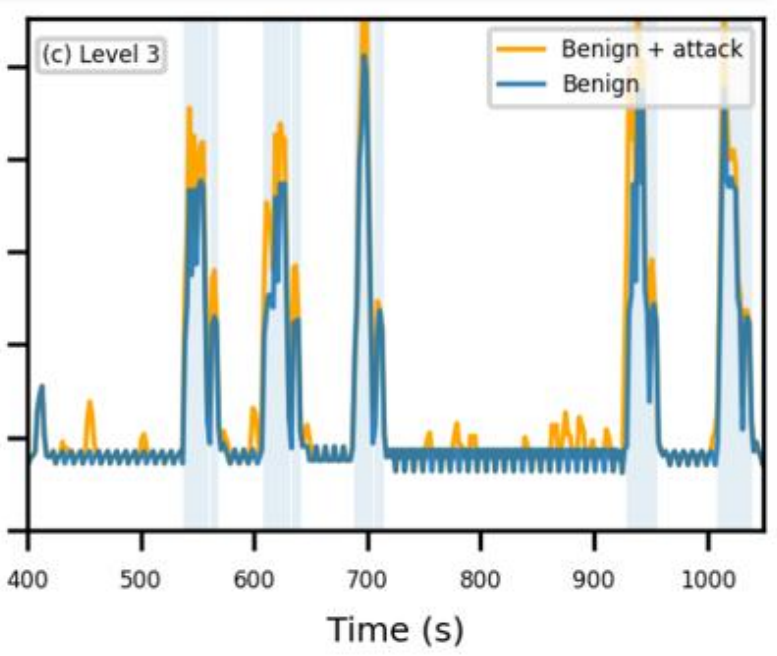



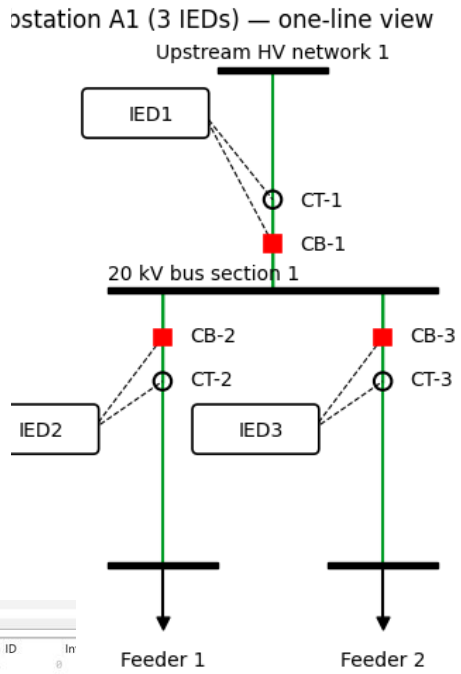

```
asset Secret {
    | find
}
asset Computer {
    | connect
        -> authenticate,
           compromise
    | authenticate
        -> compromise
    # login
        -> authenticate
    & compromise
        -> computerNetwork.compromise,
           storedSecret.find
}
asset Network {
    | compromise
        -> participant.connect
}
associations {
    Secret [storedSecret] * <-- stored --> * [computerStorage] Computer
    Network [computerNetwork] * <-- connected --> * [participant] Computer
}
```

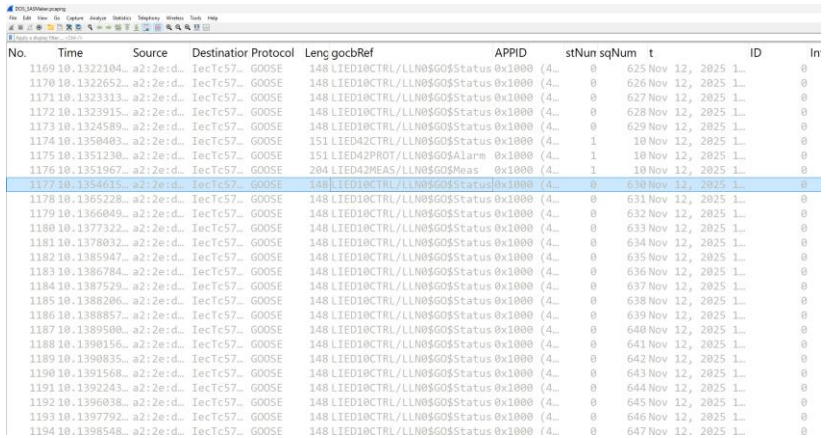
# Threat Modelling

- Proactive approach
- Formal methods, graphical methods[1]
- Known vulnerabilities, Time-To-Compromise[2]

1. Engla Rencelj Ling and Mathias Ekstedt, A threat modeling language for generating attack graphs of substation automation systems, International Journal of Critical Infrastructure Protection, vol. 41, no. 100601, 2023, doi: 10.1016/j.ijcip.2023.100601
2. Engla Rencelj Ling and Göran Ericsson, “Cybersecurity Entry Points to the Energy Sector and their Time-To-Compromise”, in Proceedings of the 25th European Conference on Cyber Warfare & Security (ECCWS 2026), 2026, Vol. 25, p. 636-644, Nottingham, England, 2026, doi: 10.34190/eccws.25.1.467



# ML-based Anomaly Detection[1]

- Low cybersecurity due to high-performance requirements
- Using ML to learn what the expected traffic pattern is
- Creating datasets

1. Filip Natvig, Engla Rencelj Ling and Göran Ericsson, “SASMaker: A Framework for Generating Synthetic IEC 61850 Traffic from Diverse Substation Setups”, CIGRE Session 2026, Session Paper D2-11435, Paris, France.

UPPSALA UNIVERSITET



UPPSALA
UNIVERSITET

Engla Rencelj Ling, PostDoc
engla.rencelj.ling@angstrom.uu.se