# OMV Group

## Cyber Security

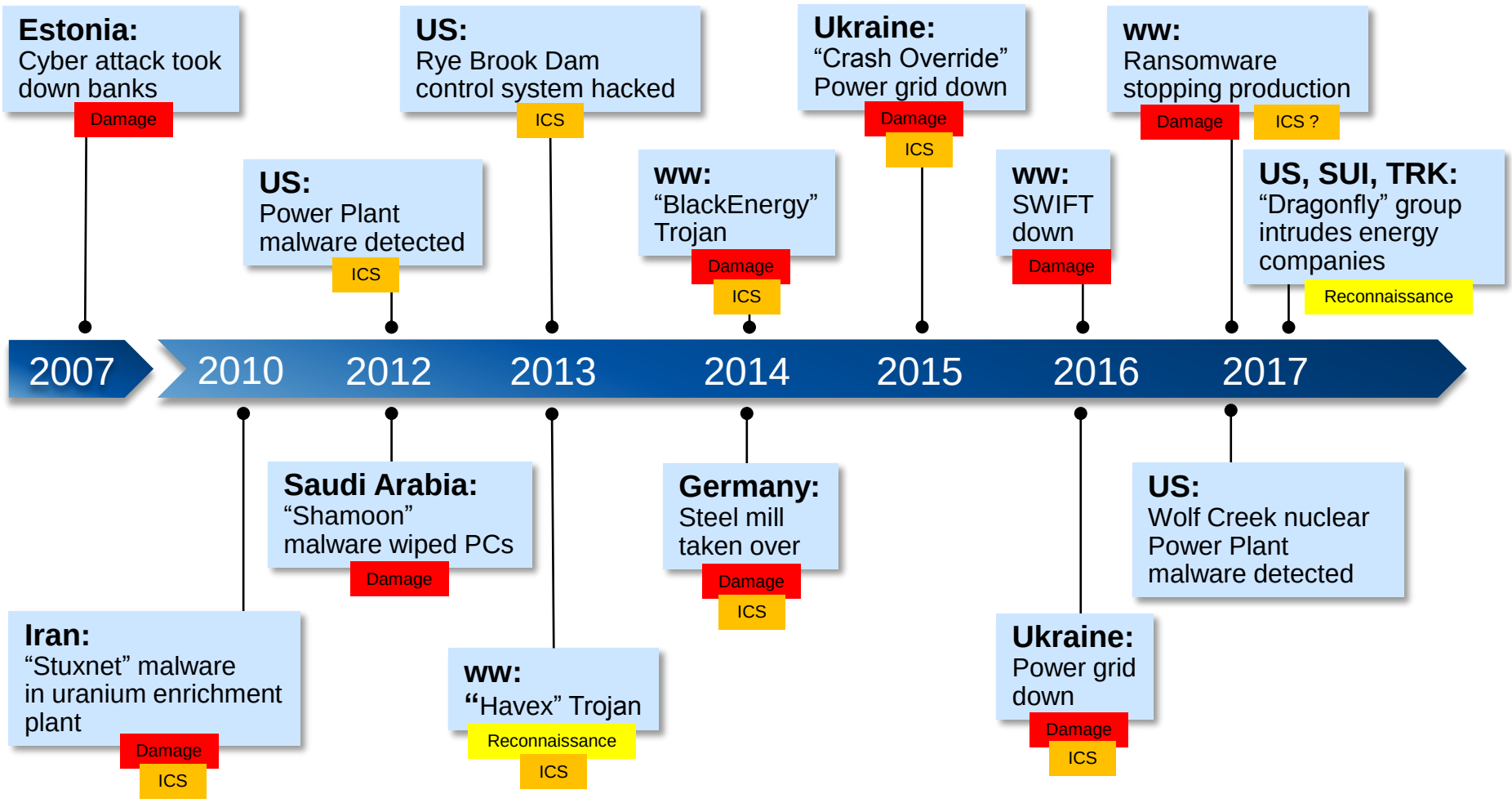
Emerging threats to Industrial Control Systems require intensified countermeasures

VCSW 2018

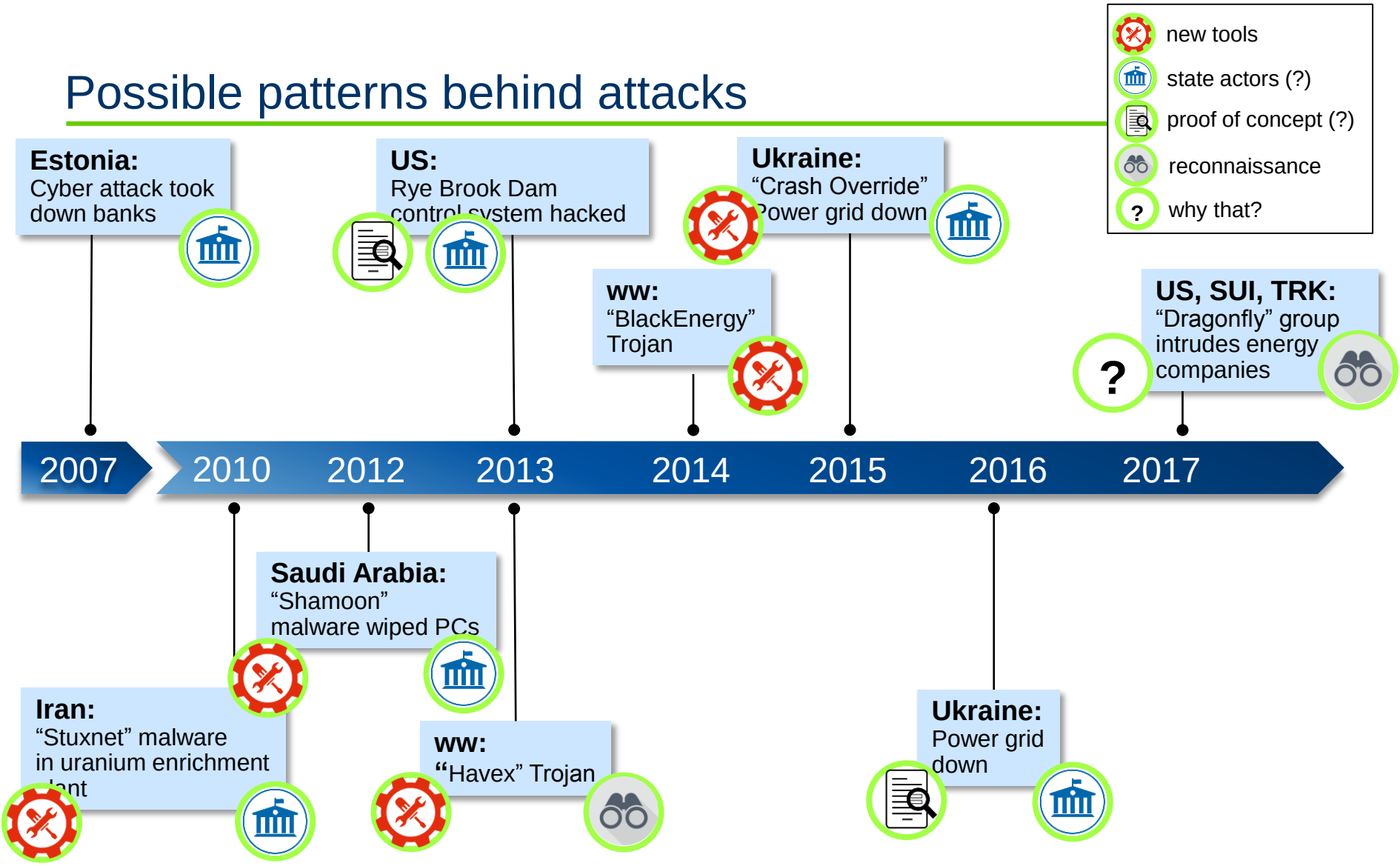


The energy for a better life.

# History of attacks affecting critical infrastructure



# Possible patterns behind attacks



# ICS/SCADA Systems provide exploitable vulnerabilities

- **ICS/SCADA equipment specifics**:
  - designed primarily for operational safety and reliability
  - security not top priority
  - long lifecycle
  - patching possibility not always built in
  - downtime (for patching) not desired

Vulnerabilites

+

Lack of Patches

+

delayed Patching

=

exploitable Vulnerabilities

# Exposure of ICS/SCADA Systems is growing

- **Increased exposure of ICS/SCADA systems**:
  - Digitalization requires more data exchange
  - Remote service instead of physical access
  - Increasing amount of involved devices
  - New connection technologies (e.g. wireless)
  - Trend to standardization
  - More Windows-based solutions in ICS environments (e.g. HMI)

growing Attack Surface

+

Loss of Obscurity

=

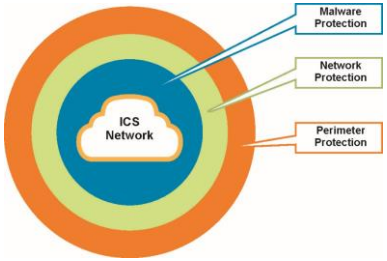
increased Exposure

# Defense against Cyber Security Threats
## Components to be considered

### ARCHITECTURE

Planning and running systems considering security aspects

- "Security by Obscurity" does not protect anymore
- Multiple layer defense:
  - Perimeter protection
  - Network protection
  - Malware protection




### PASSIVE DEFENSE

Systems without human interaction

- Perimeter Protection:
  - Firewalls to outside and within ICS
  - Unidirectional gateways: outbound only
- Network segmentation & protection
  - VPN between ICS components
  - Access Control Lists
  - 802.1.x
- Malware Protection for SCADA systems
- Systems on latest patch level

### ACTIVE DEFENSE

Analysts monitoring, responding and learning from intrusions

- Log file monitoring of firewalls within the SCADA/ICS environment + to the "outside world"
- Fast reaction / having resources available quickly
- Using trained, aware people for operations and defense

### INTELLIGENCE

Collecting data, condensing it into information and producing intelligence

- Lessons learned from previous experiences
- Exchange with peers / CERT/ national organizations
- Vulnerability feeds / external warnings + reaction on them
- Good cooperation with "classical IT"

Source of drawing :
E-ISAC "The Sliding Scale of Cyber Security"

# Further readings

- IEC 62443-2-1
  Industrial communication networks – Network and system security –
  Part 2-1: Establishing an industrial automation and control system security program
- National Institute of Standards and Technology (NIST), Guide to Industrial Control Systems (ICS) Security, NIST SP 800-82 Rev. 2
  https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
- ENISA, Can we learn from SCADA security incidents?
  https://www.enisa.europa.eu/publications/can-we-learn-from-scada-security-incidents/at_download/fullReport
- ENISA, Communication network dependencies for ICS/SCADA Systems
  https://www.enisa.europa.eu/publications/ics-scada-dependencies/at_download/fullReport
- ISACA SCADA Cybersecurity Framework
  https://www.isaca.org/Journal/archives/2014/Volume-1/Pages/SCADA-Cybersecurity-Framework.aspx
- RISI Industrial Security Incidents Database (ISID) – discontinued since 2015
  http://www.risidata.com/Database
- 21 Steps to Improve Cyber Security of SCADA Networks
  https://energy.gov/oe/downloads/21-steps-improve-cyber-security-scada-networks

# Thank you for your attention!