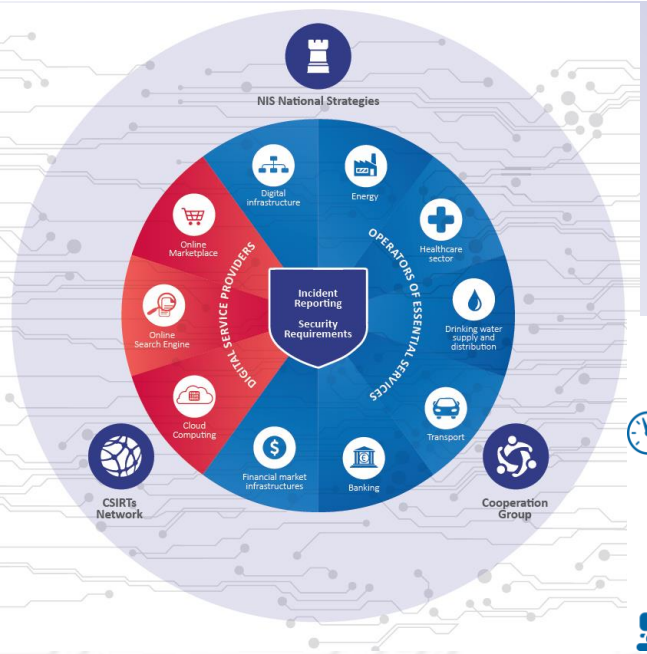
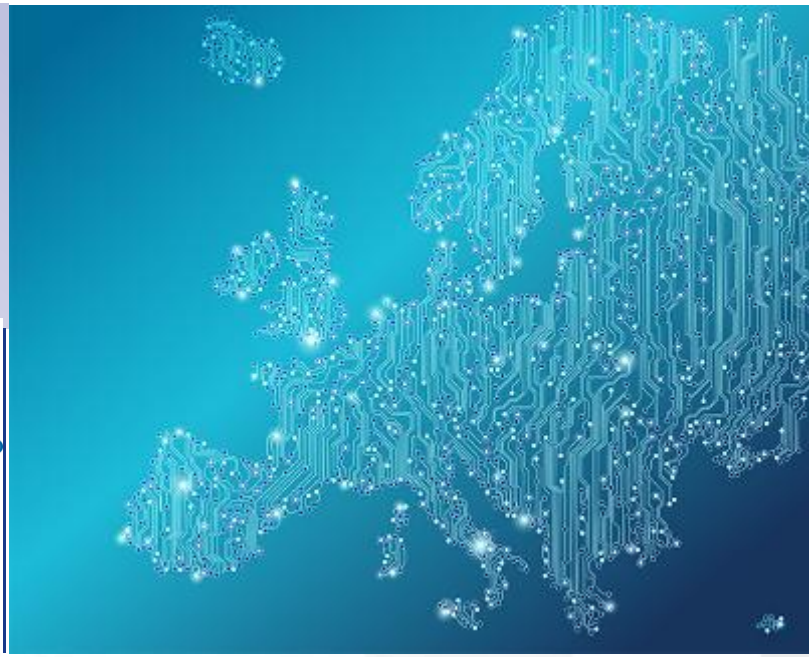




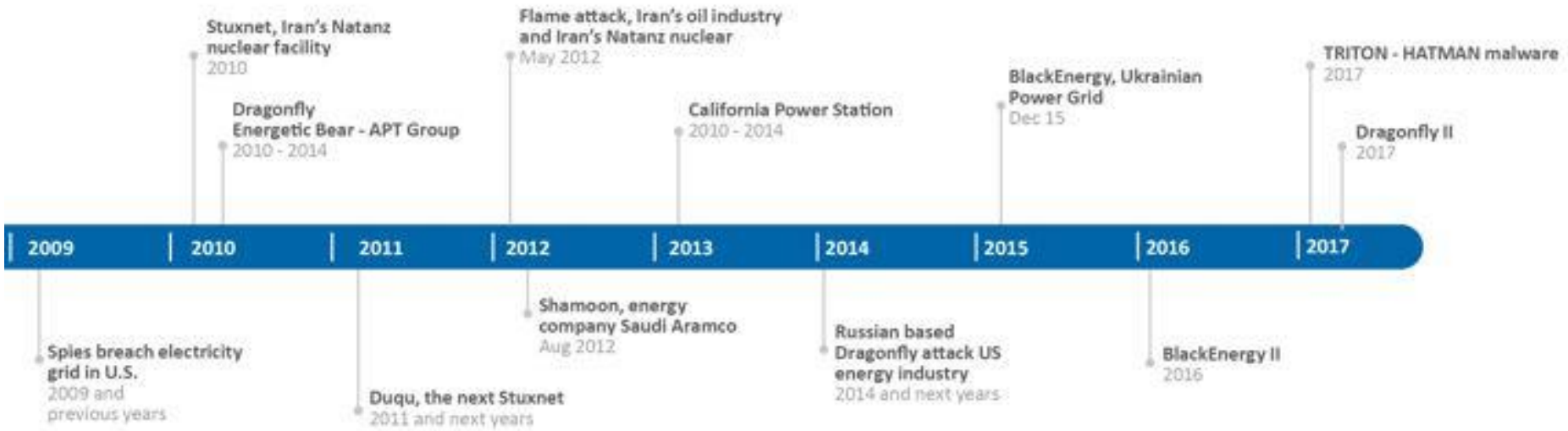
Cyber Security Challenges of EU's Energy Sector

Dr. Evangelos Ouzounis, HoU - Secure Infrastructures and Services

Brussels, 11.10.2018

Energy and ICT – a great future

.. with interesting past

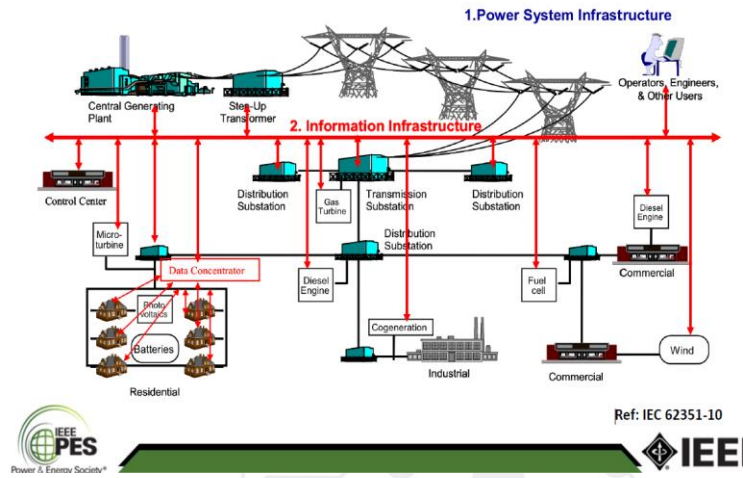


- **The number and frequency of attacks is increasing**
- **Sophistication level is increasing**
- **Expertise required to launch an attack is decreasing, ie more people can effectively do that**

Threat Landscape (1)

- Complex networks and services
- Significant physical disasters
- Low quality of software and hardware
- Interdependencies on ICT and other sectors
- New emerging technologies
  - Smart grid and Renewables
  - (I)IoT
  - Smart Cars,
  - 5G

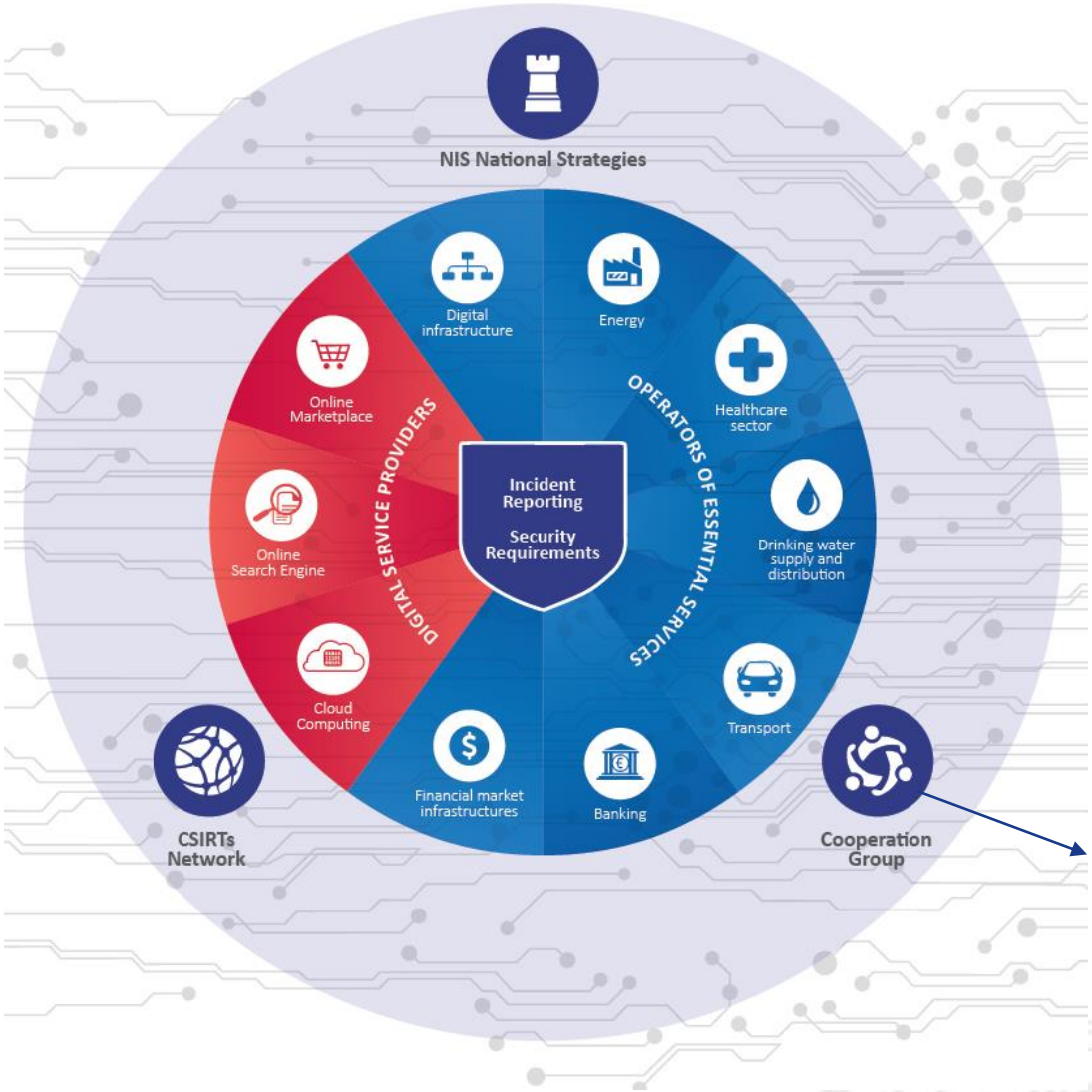
Complexity of Power Systems



Threat Landscape (2)

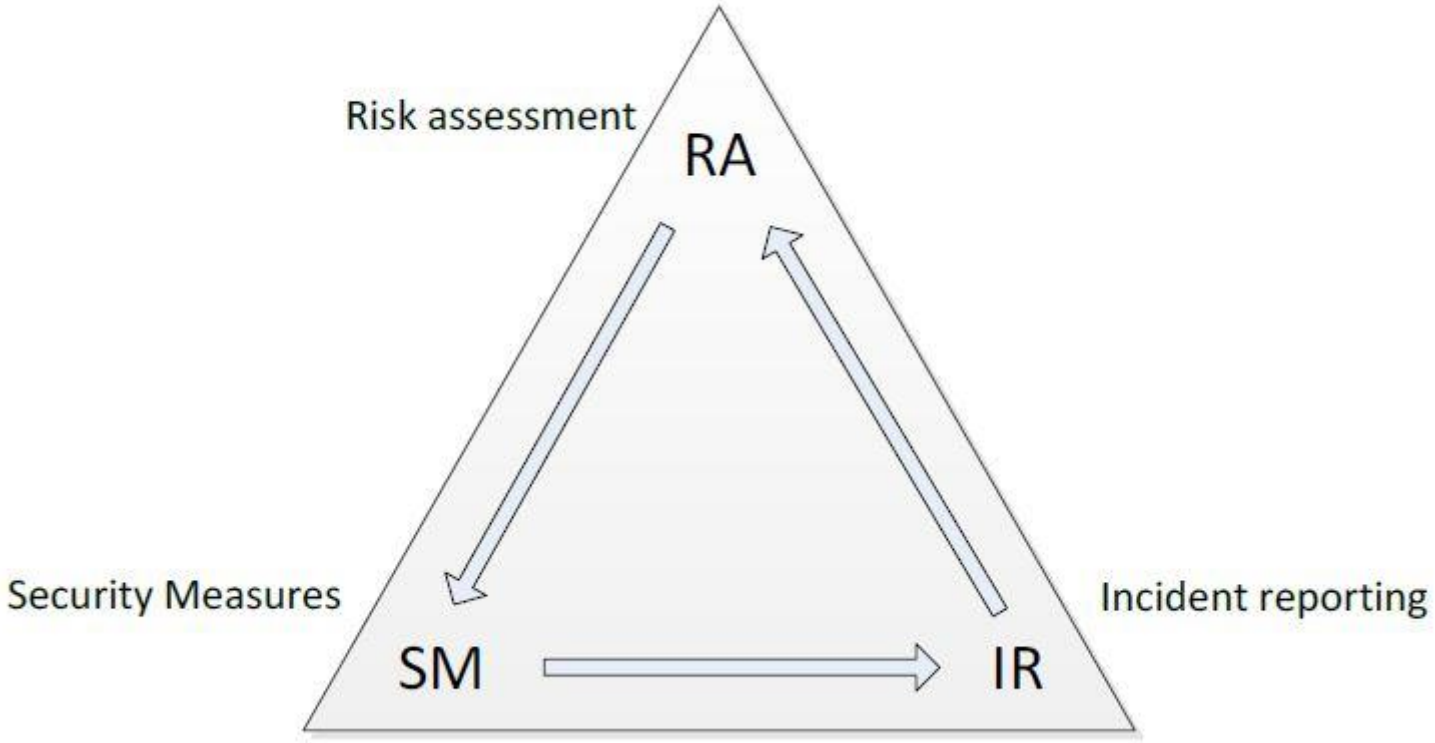
- Asymmetric threats allowing remote attacks to CII
- Increasing organized cybercrime and industrial espionage
- Regulatory Inconsistencies
- Cyber Security Maturity and skills sets
- Lack of international agreements and standards
- Lack of well functioning, international incident handling/crisis management mechanism

NISD and the Energy Sector

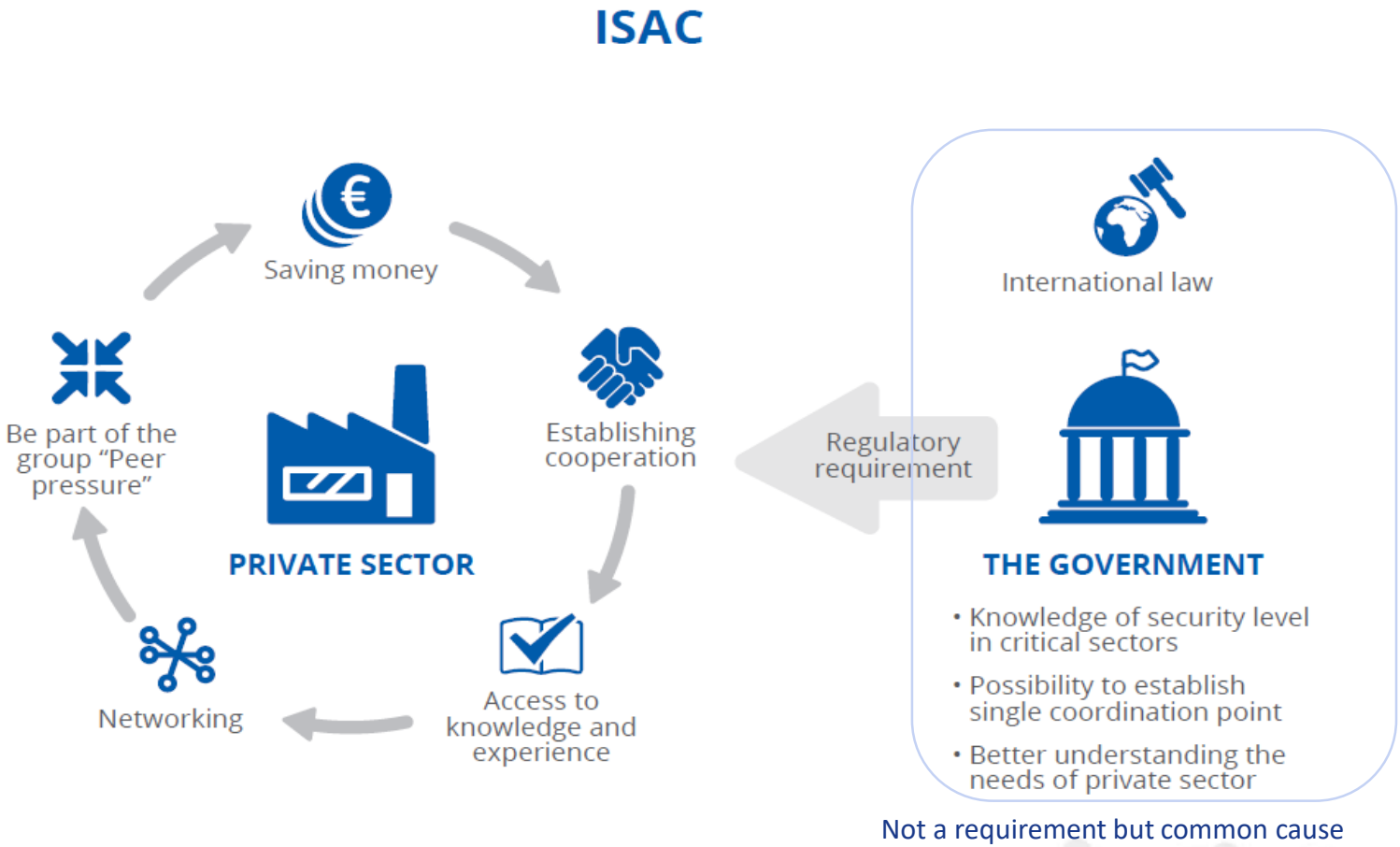


WS8 on cyber security for the energy sector – AT is the leader

Key Security Requirements



Public Private Co-operation



Not a requirement but common cause

Food for thought

- Harmonization of security requirements across the EU based on NISD requirements
- Foster public private co-operation at national, regional and EU level
- Mandatory reporting of all significant incidents following a holistic approach
- Study interdependencies and supply chain integrity
- Risk assess the emerging technologies for the energy value chain (e.g. IoT, AI, Blockchain,)
- Develop and promote certification schemes for the energy sector
- Regulatory simplicity and consistency

Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu