EUROPEAN UNION AGENCY
FOR CYBERSECURITY

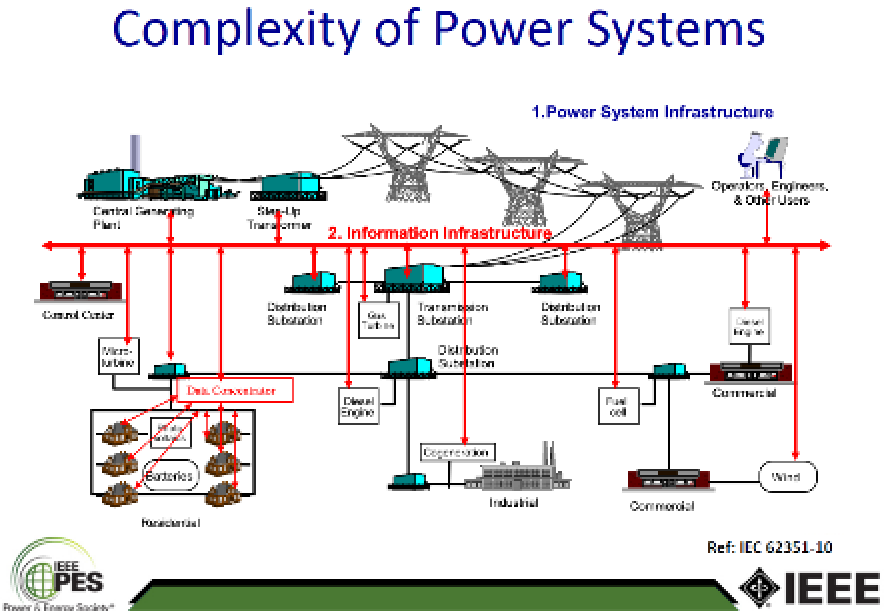
ENERGY SECTOR CYBERSECURITY - ENISA ACTIVITIES

Christina Skouloudi
Information Systems and Network Security Expert

17 | 7 | 2020

1. The need for a sectorial approach to energy cyber security
2. Policy context - The NIS Directive
3. ENISA activities
4. Open issues
5. Conclusions

WHY IS IT MORE COMPLICATED?



Complexity of Power Systems

Ref: IEC 62351-10

- Roles and responsibilities at the state level
- Real time requirements
- Complex networks and services
- Interdependencies on other sectors
- New technologies: new potential avenues of attack
- The IT/OT problem

ENERGY SECTOR: AN ATTRACTIVE TARGET

Cultural reasons:

- Physical protection, safety, availability

Historical reasons:

- ICS initially used proprietary software.
- For specific activities, without security specifications.
- COTS in business and industrial entities of energy companies.
- Complex networks and services

Organizational reasons:

- Different company units can be used as a backdoor to ICS. (eg the Ukrainian case).
- Dependence on third party providers.

Operational reasons:

- Industrial operations continuity makes updating/patching difficult.

POLICY CONTEXT: THE NEED FOR A SECTORIAL APPROACH

- Directive on European Critical Infrastructures (EU) 2008/146

- Cyber Security Strategy (2013)

- Network and Information Security Directive (EU) 2016/1148

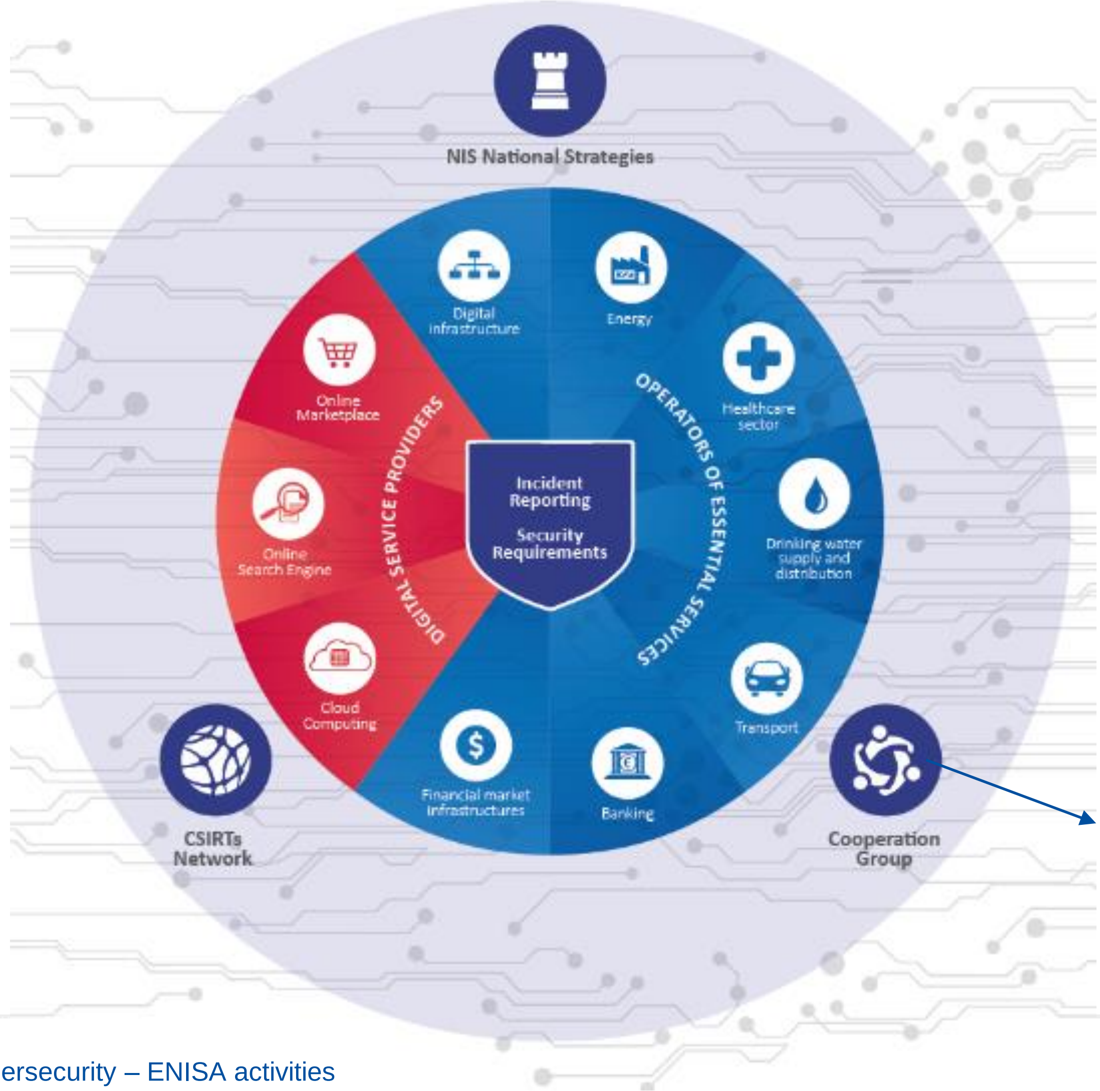
- Data Protection: Regulation (EU) 2016/679 – GDPR

- Cyber security Act (2017)

- The Cyber security Act: Regulation (EU) 2019/881

- COM Recommendation on cyber security in the energy sector (2019)

THE ENERGY SECTOR IN THE NIS DIRECTIVE



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

NISD: SECTORIAL IMPLEMENTATION

- WS 8 on energy sector security

- ENISA has a key role
  - Drafting the Reference document
  - Knowledge transfer
  - Knowledge building sessions
- ENISA, with the administrative support of COM, organized the first joint sectorial workshop with EE ISAC and WS8 Energy Sector

- COM RECOMMENDATION C(2019) 2400 on cybersecurity in the energy sector

- ENISA intends to contribute with knowledge transfer on minimum security measures for the energy sector

ESTABLISHED RELATIONS WITH EU INSTITUTIONS AND OTHER KEY STAKEHOLDERS

DG-ENER

- Advisory board
  - European Energy Cybersecurity Strategy
  - SGTF Expert Group 2 on Recommendations for the implementation of specific measures
- Steering
  - SGTF Expert Group 2, Proposal for a list of security measures for smart grids

ACER and CEER

- Workshops and knowledge exchange

ENTSO-E

- Consultations on technical reports
- Contribution to ENTSO-E CEF Sub Team 1 - ISMS / SSDLC

MOBILISING COMMUNITIES

- Studies on smart grid security/certification and ICS-SCADA security

- Organising events and workshops

- Report on energy sector dependency on time sensitive services

- ES-C2M2 for Europe
  - Stock taking with stakeholders from the private as well as the public sector
  - Objectives
    - Map the ES-C2M2 with well known standards and frameworks
    - Identify challenges for an EU ES-C2M2

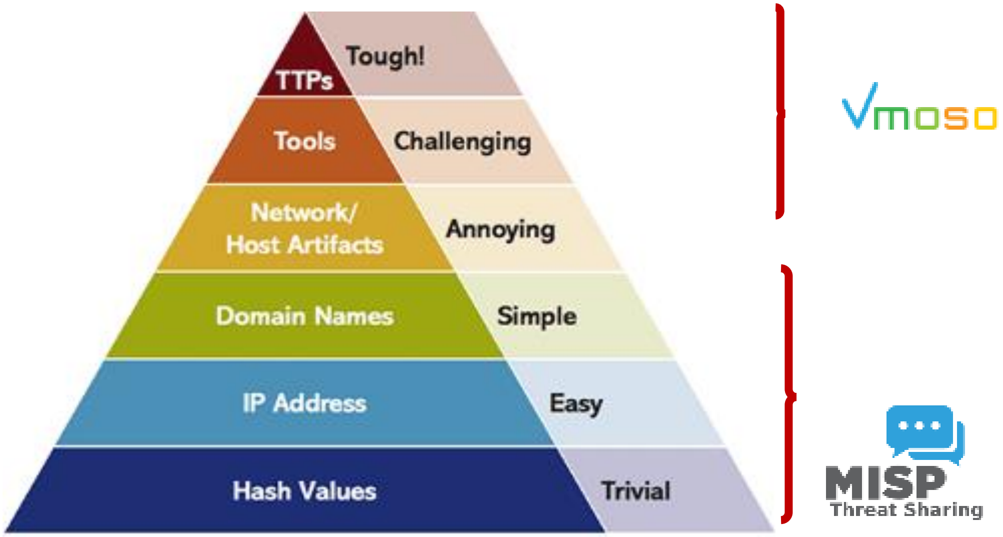
POWER SECTOR DEPENDENCY ON TIME SERVICE

Communication network interdependencies in smart grids

INFORMATION SHARING

EU Energy ISAC

- ENISA is a founding member
- Webinars
- Threat- landscape process
- Trainings
- Facilitation of plenary meetings
  - EE ISAC meeting in Athens, September 2017
  - Next EE ISAC meeting in Athens, November 2019



OPEN ISSUES

- Collaboration with the private sector is missing from the NISD
- Small operators are not in scope of the NISD
- Responsible disclosure of vulnerabilities
- Gaps in coordination during crisis
- Insufficient overview of the big picture as per the threat landscape and early warning capability
- Dependencies on other sectors are not take into account

CONCLUSIONS

1 Cyber attacks on CIIs is now the norm than a future trend.

2 Enable higher level of security for Europe's Infrastructures.
NISD first piece of work at EU level
Updated Cyber security strategy

3 MS and private sector, with the assistance of ENISA, should co-operate to protect CIIs

- sharing experiences and information
- developing and deploying good practices
- co-operate with NRAs to achieve EU wide harmonization of EU regulations

4 "Collaboration is Everything".

Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu