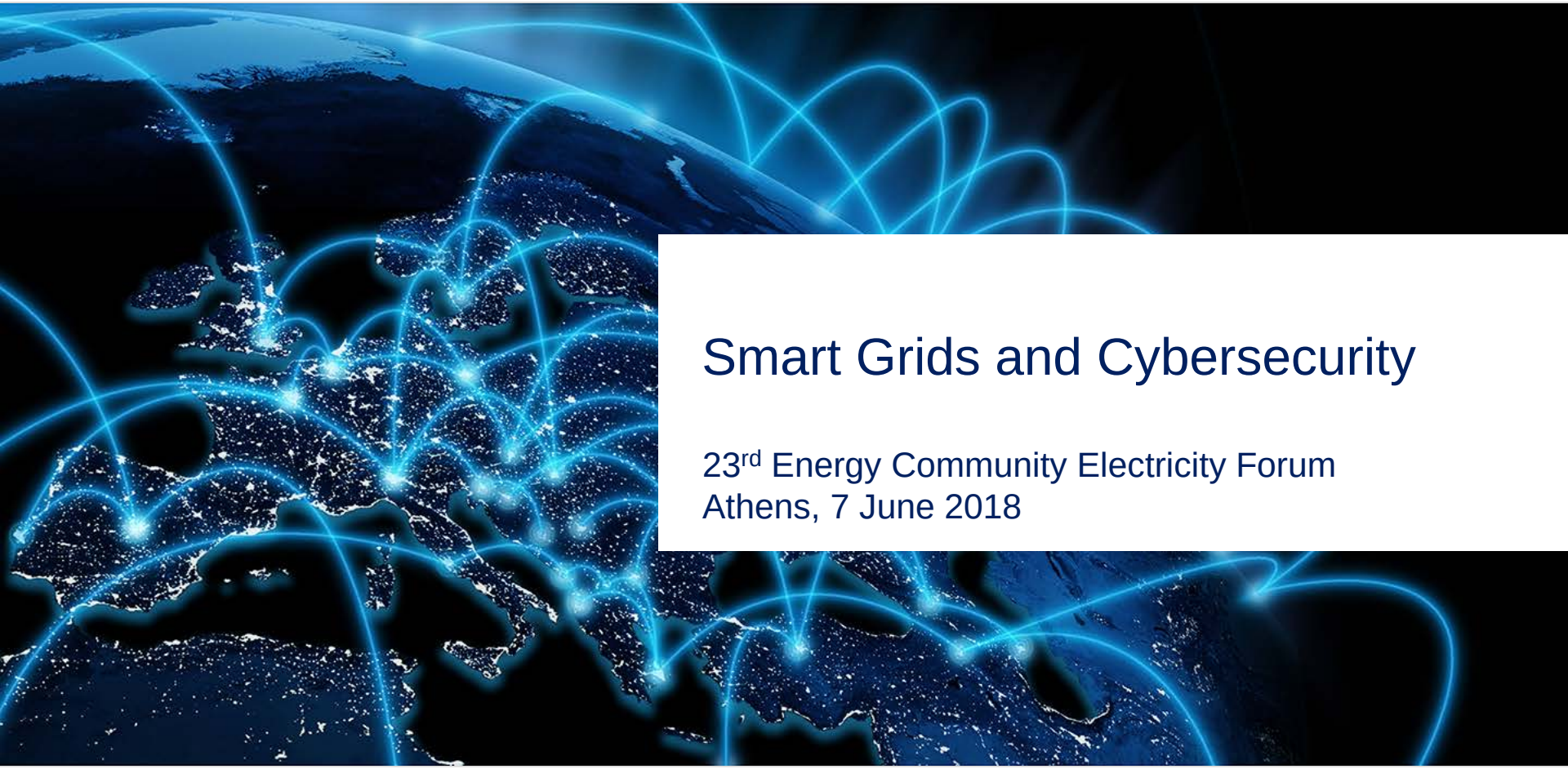


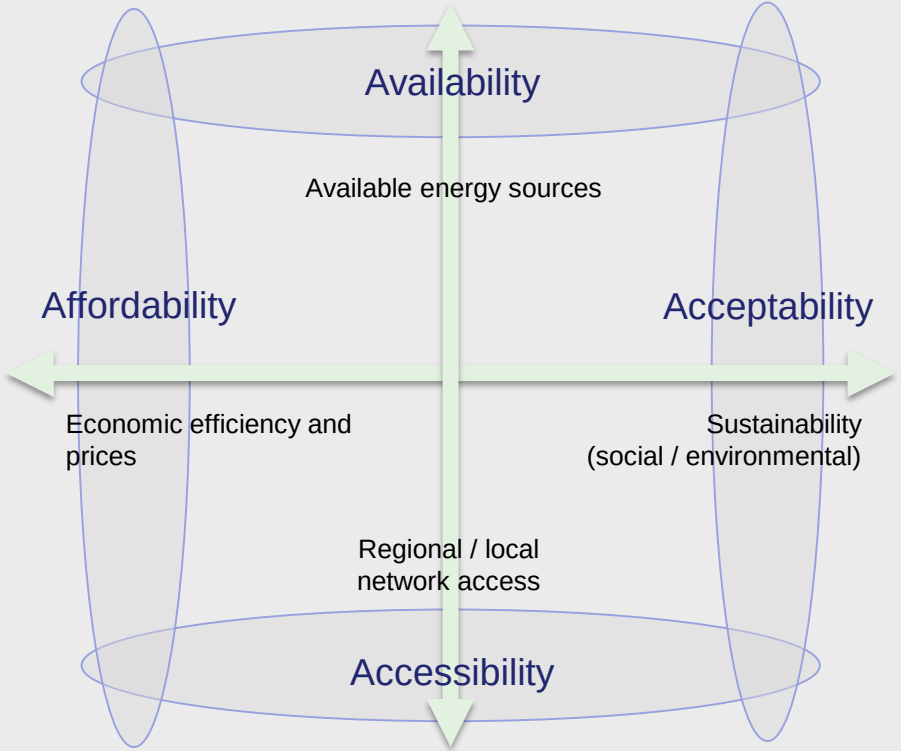
Smart Grids and Cybersecurity

23rd Energy Community Electricity Forum
Athens, 7 June 2018

Energy security and cybersecurity

- **IEA**: Energy Security is the uninterrupted availability of energy sources at an affordable price

- The **"4A"** Energy Security Spectrum[1]
  - Cybersecurity is an integral part of energy security
  - It affects all aspects of energy security (through the network or market infrastructure)
  - Need of cybersecurity response at all stages of the energy cycle
  - Need of trans-sectoral response together with the digital community

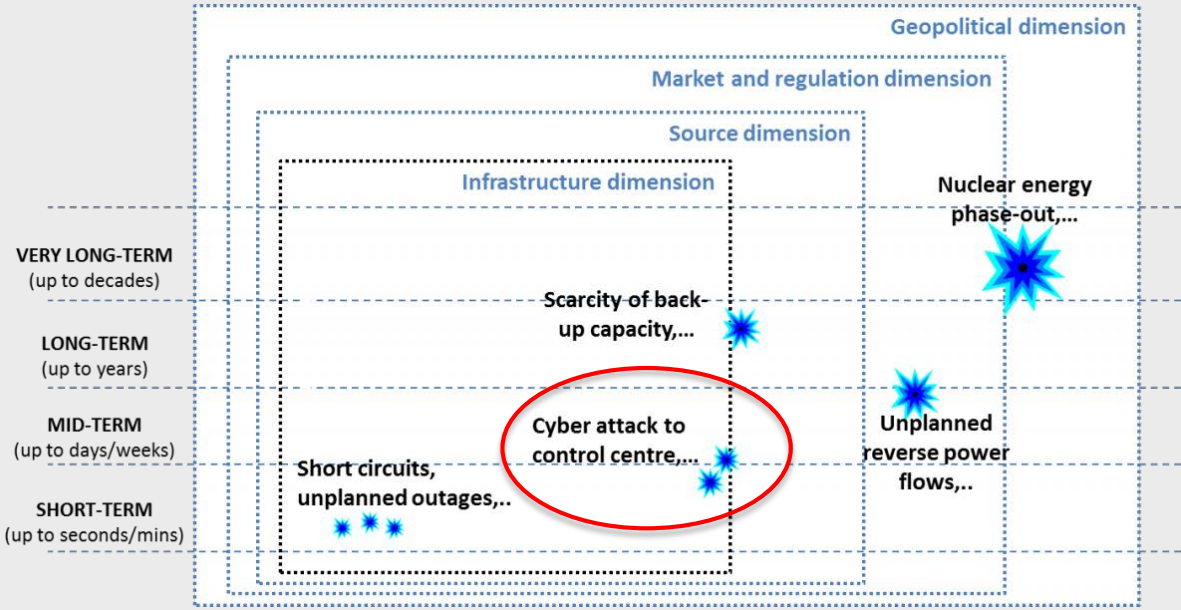


[1] "Indicators for Energy Security" – Kruyt et al, Energy Policy, 37 (6): 2166-2181, 2009

Electricity security

- **JRC**[1]: power system's capability to withstand disturbances (events producing abnormal system conditions), or contingencies (outages of system components) - with minimum acceptable service disruption

  - **Infrastructure** dimension - capability to supply end users with minimum service criteria
  - **Source** dimension - accessibility to primary sources to meet the total demand
  - **Regulation and market** dimension – capability to fulfil delivery with a set of laws, rules, market arrangements and prices
  - **geopolitical** dimension – availability of sources and/or cross-border exchanges in case of economic or geopolitical constraints

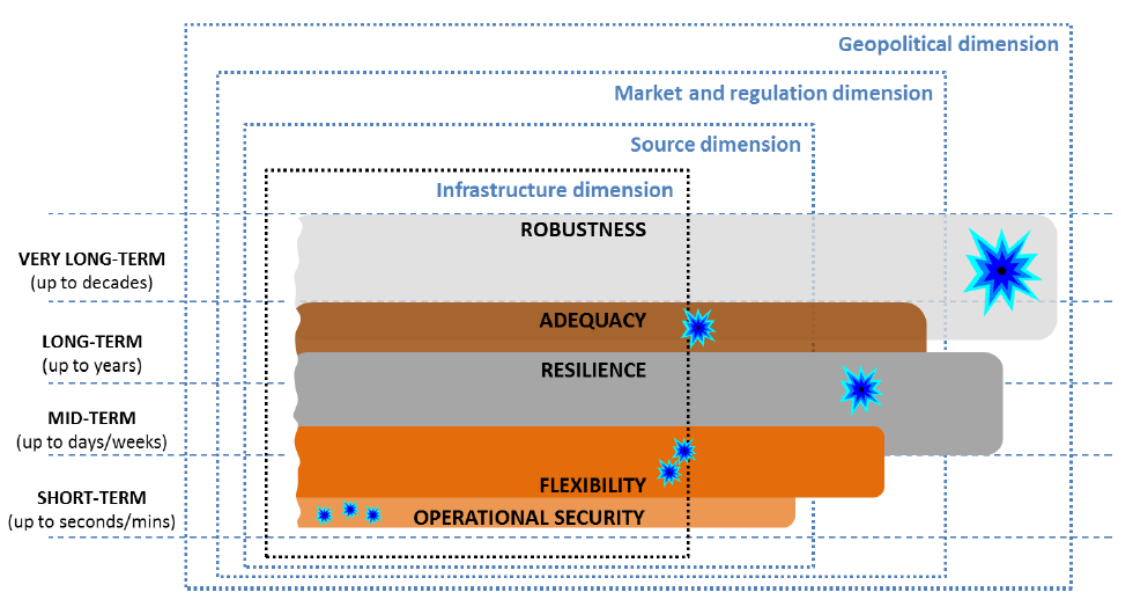


[1] EC – Joint Research Centre – Smart Electricity Systems and Interoperability

Electricity security

❖ Security properties[1]

- **Operational security** - ability to maintain or to regain operational condition after disturbances
- **Flexibility** - capability to cope with short/mid-term variability of generation and demand (the system is kept in balance)
- **Adequacy** - ability to supply the aggregate demand at all times under normal operating conditions (includes generation/storage, transmission, distribution, end user and market adequacy components)
- **Resilience** - mid-term capability to absorb the effects of a disruption and recover performance level.
- **Robustness** - long-term capability to cope with constraints originating outside the infrastructure dimension.



[1] EC – Joint Research Centre – Smart Electricity Systems and Interoperability

Cyber threats in transmission and MO

- Sources of risk
  - Digitalization
  - Leasing of services
  - Multiple access points
  - Diverse communication channels
  - Interconnection and cross-border threats

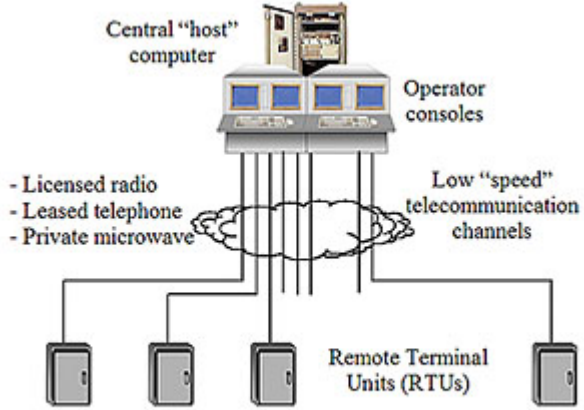


Figure 1.0 – SCADA architecture in the 1970's

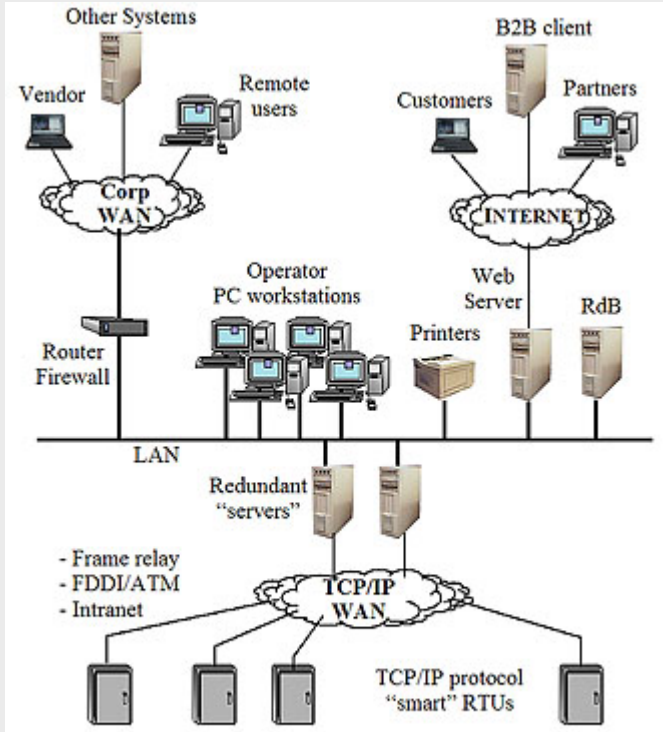
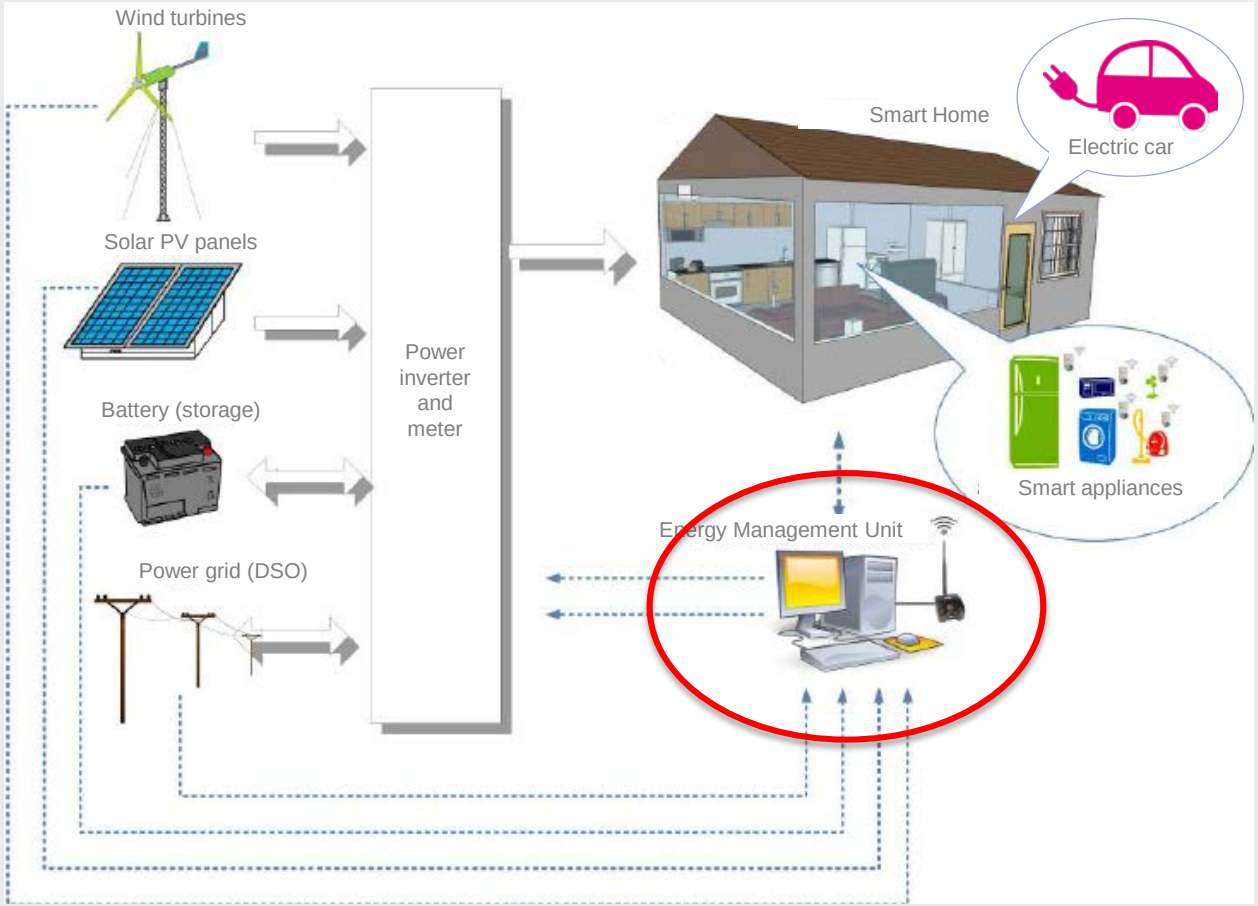


Figure 1.1 – SCADA architecture in the 2000's

Cyber threats in distribution



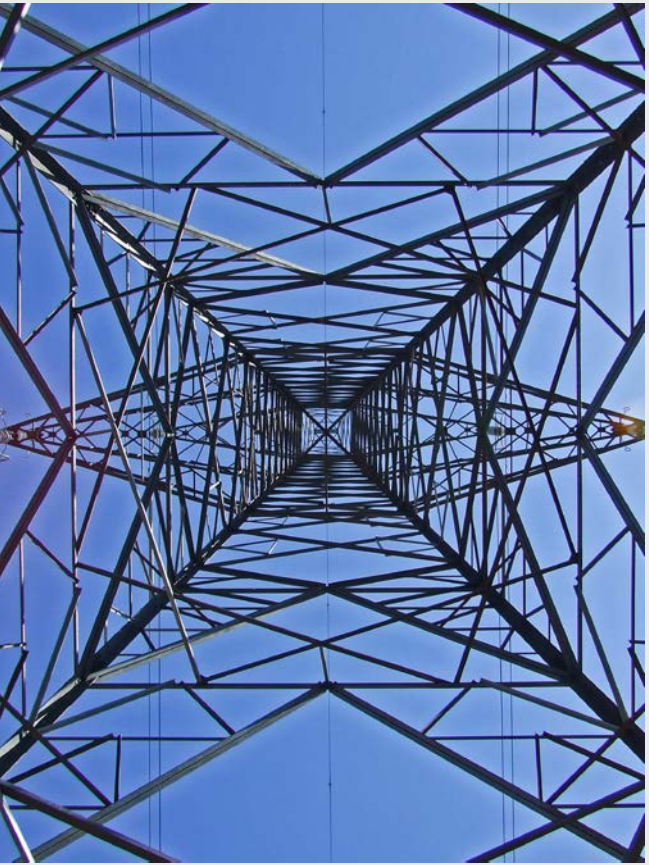
❖ "Smart home" threats

- Complex processing and forecasts
- Rollout of smart meters – access and use of data
- De-centralized devices behind the meter
- Expanding market for end-user products
- Diverse unreliable technologies and applications
- Internet access, remote controls
- Insufficient or missing safety standards
- Data ownership and protection not defined and implemented
- Threat from "simple mistakes"

Cybersecurity policies

- Cybersecurity is here to stay
- It is a direct consequence of the present evolution of the power systems and demands corresponding attention
- 100% security does not exist – it is a combination of preventive (resilience) and corrective measures (flexibility), balanced through proper assessment of the risk
- It introduces a new industry of digital products and services, new scope of cross-regional cooperation, new rules in human behaviour and new category of costs
- It requires development of special methodologies, training and education, and represents a source of employment
- It penetrates all layers of the telecommunication technology, and requires concerted and immediate action based on own or reliable resources and standards

Cybersecurity best practices



- Apply REDUNDANCY and meshed architecture in critical network infrastructure
- Establish generic SECURITY OPERATIONAL CENTRES in major energy companies and on national level
- Security MONITORING of assets, data management systems and available cyber defence technologies
- Application of RULES on cyber defence – guidelines, protocols, methodologies, protection mechanisms and defence strategies
- Training and SYMULATIONS of possible cyber threats, apply policies to increase AWARENESS
- Develop RECOVERY strategies, mechanisms and backup systems for critical services and information
- Establish COOPERATION MECHANISMS with neighbouring operators and practice for exchange of information and logistics

Cybersecurity in the Energy Community

❖ Cyber attacks in **Ukraine** electricity networks

- **December 2015** – three Oblenergo (DSO) systems compromised: **Prykarpattya** – switched off 30 SS (230.000 citizens) for a period of 6 hours; **Chernivtsi** and **Kiyv** to lower extent - imposed vast damage on systems and data
- **December 2016** – 330 kV Transmission SS **Kiyv North** SCADA system compromised causing blackout for 1/5 of Kiyv demand for one hour – advanced, automated malware, swappable, adaptable and universal, simultaneous threat to multiple systems

❖ NIS Directive - (EU) 2016/1148

- ECS proposed adaptation and adoption of the NIS Directive (energy) in the Energy Community
- PHLG (March 2018) Conclusions:
  - Acknowledged the necessity to build cybersecurity capabilities and risk management and incident reporting culture in the Energy Community
  - ECS to explore the incorporation of NIS Directive, take steps and discussions for identification of suitable provisions, and prepare a proposal with adaptations and appropriate timing
  - Recommended to eliminate regulatory gaps and develop cooperation structures, certification framework and research and education programs

NIS Directive

- Build sufficient capacities at national level
  - Adopt a national NIS strategy
  - Designate national competent authorities, single contact points and Computer Security Incident Response Teams (CSIRTs)
- Identify critical infrastructure, operators of essential services (**OES**), and relevant digital service providers
- Build structures for **cross-border** cooperation and exchange of information
  - At strategic level - creating a Cooperation Group of national authorities
  - At operational level - creating a network of national CSIRTs

NIS Directive

❖ Cumulative conditions for identification of OES

- provision of a service essential for critical societal / economic activities
- provision of that service depends on network and information systems
- an incident would have significant disruptive effects on the provision of that service

❖ Security and Notification Requirements imposed on OES

- take technical and organizational measures
  - to secure networks and systems
  - to prevent and manage risks
  - to handle incidents and minimize their effects
- notify incidents

❖ Monitoring and enforcement powers

Cybersecurity in the Energy Community

❖ Recommendations (based on NIS Directive):

- Create a Cooperation Group between CPs and MSs
- Put in place common certification conditions across the Energy Community
- Eliminate regulatory gaps
- Initiate cooperation on the establishment of research and education programmes
- Develop a common crisis management and rapid emergence response mechanism, *inter alia* through Title III or Title IV measures
- Step-up public-private cooperation in cybersecurity

❖ Study on Cybersecurity in the energy sector of the Energy Community

- Objectives
  - Identify weaknesses, risks and exposure to cyber threats in the energy systems
  - Identify the existing regulatory framework and regulatory gaps for cybersecurity governance
  - Identify the relevant provisions of NIS Directive and provide impact assessment of their implementation
  - Propose the necessary measures for cybersecurity on local level
  - Propose a model for regional cooperation in managing cybersecurity risks and reporting incidents
- Task 1
  - Identify potential cyber threats, critical infrastructure and operators exposed, responsible policy authorities, institutional framework and service providers in cybersecurity – both in the energy and in related IT environment
  - Identify the standard technologies and practices, training, international cooperation, standards, technologies and certification schemes, enforcement authorities
  - Identify a set of relevant risk scenarios and develop a methodology for assessment
  - Identify the applicable legal and policy framework relevant for cybersecurity in the domain of energy
  - Make assessment on the level of compliance with the NIS Directive and related acquis and applied EU policies, data protection and confidentiality, cybercrime conventions and OSCE Confidence Building Measures

❖ Study on Cybersecurity in the energy sector of the Energy Community

- Task 2
  - Based on the analysis of Task 1, identify the legal and regulatory gaps, inconsistencies and potential obstacles for implementation of the relevant provisions of the acquis (NIS Directive)
  - Based on the defined methodology provide analysis of the behaviours, effects and impact of cyber threat scenarios (simulations) defined in Task 1
- Task 3
  - Propose amendments, policies, measures, procedures and recommendations to bridge the identified legal and regulatory gaps, including proposals to overcome threats and weaknesses observed through the simulations
  - Make impact assessment for the application and implementation of the proposed measures and estimate the required resources to be invested
- Task 4
  - Propose a model of regional cooperation on cybersecurity addressing preventing and managing potential cyberattacks, covering all relevant aspects covered in the analysis
  - Propose a blueprint for common mechanisms for cyber crisis management, exchange of information, certification, education and training – along with a roadmap including expected timing for implementation

Simon.Uzunov@energy-community.org
www.energy-community.org