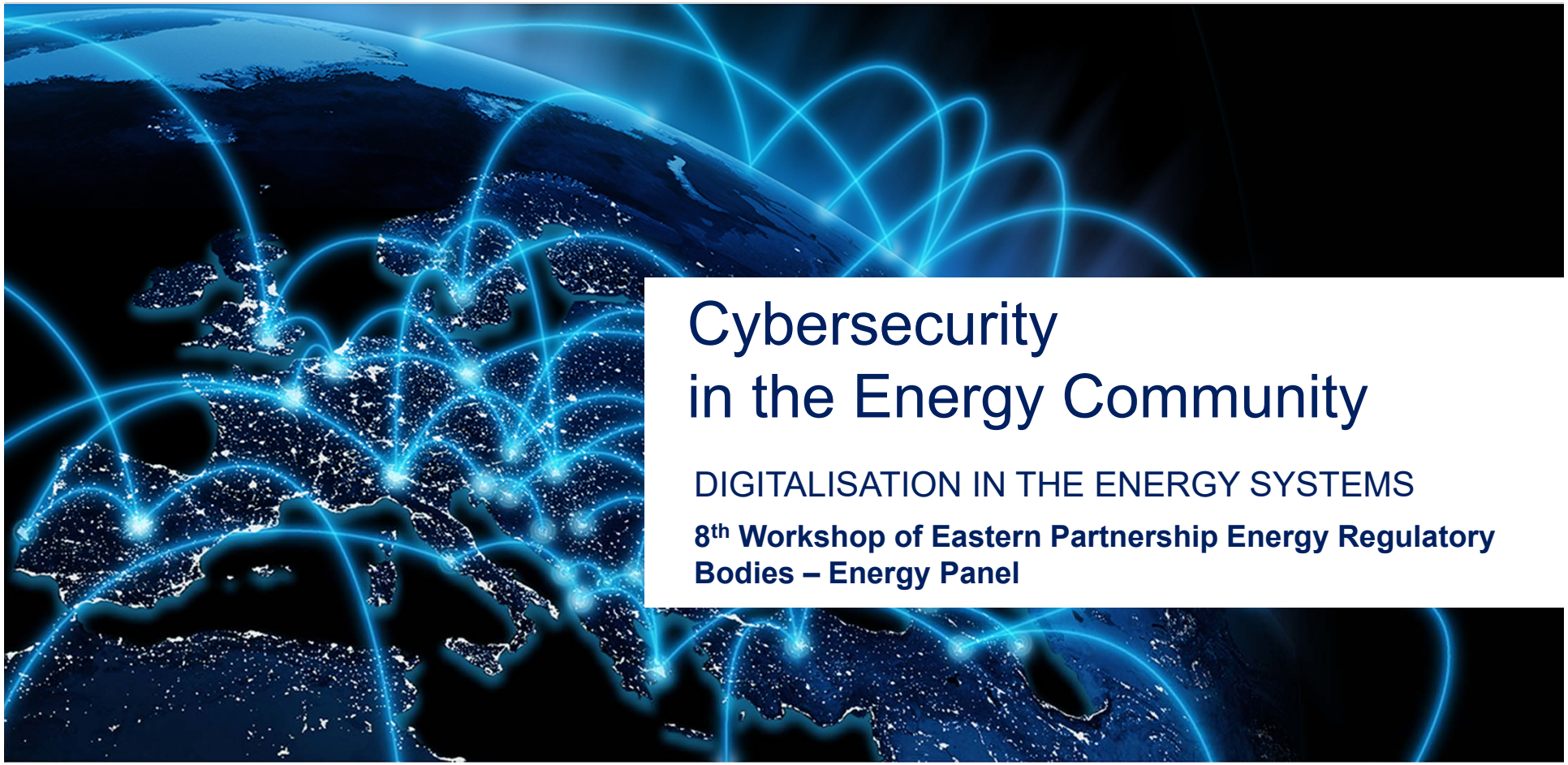


Cybersecurity in the Energy Community

DIGITALISATION IN THE ENERGY SYSTEMS

8th Workshop of Eastern Partnership Energy Regulatory Bodies – Energy Panel

Energy Community
- Extending the EU internal energy market

Domain

South East Europe and the Black Sea Region

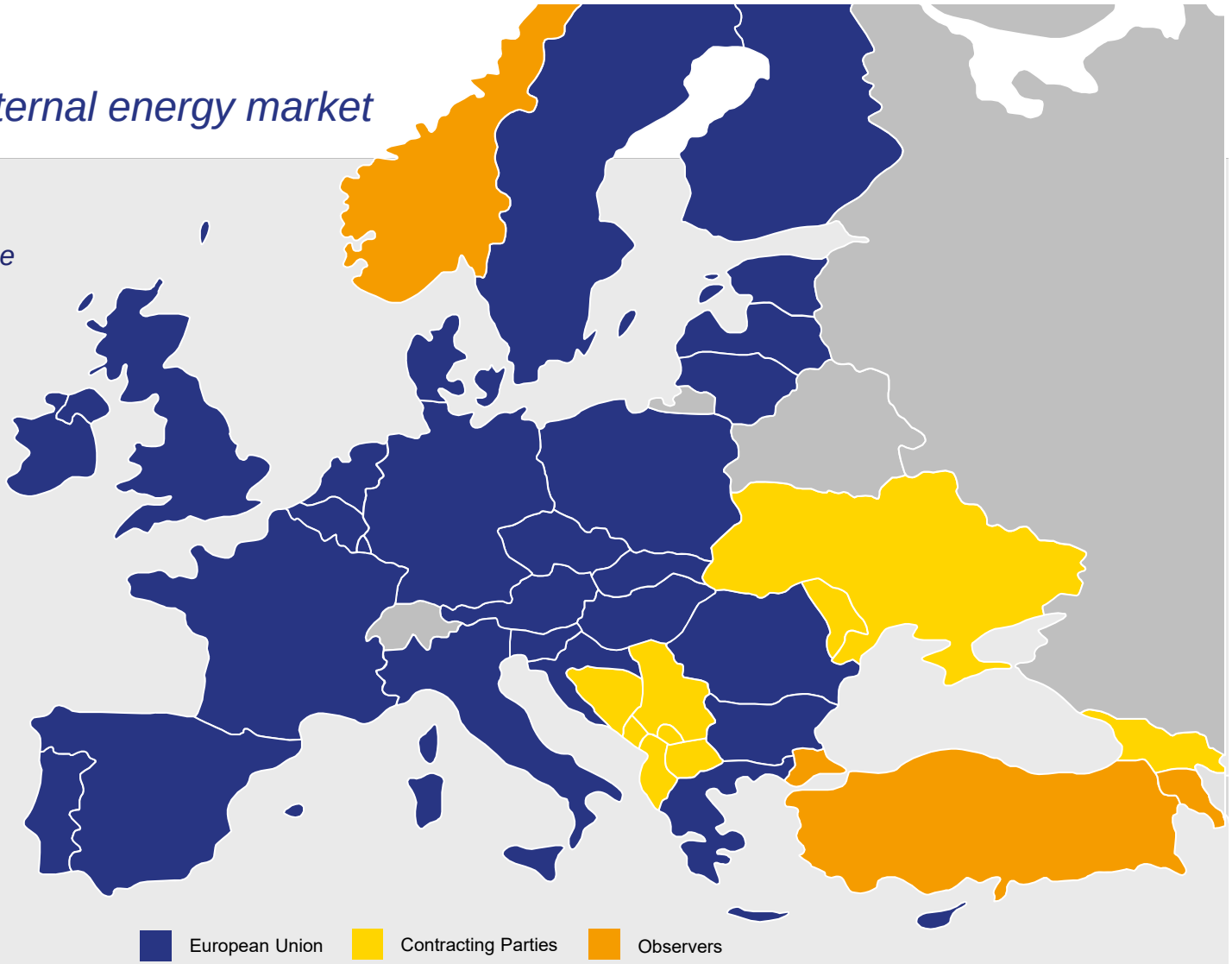
Mission

Creating a regulatory framework to increase:

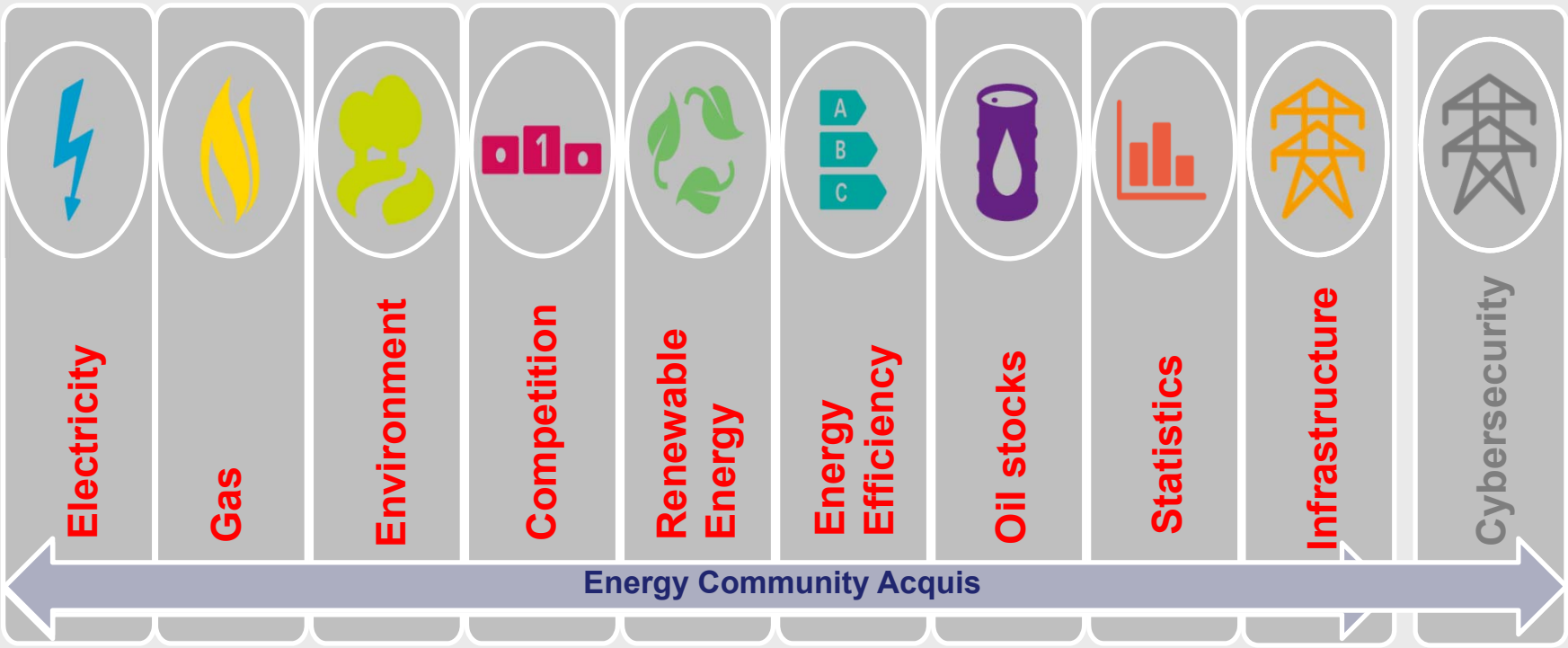
- *competition in the energy markets*
- *security of supply*
- *investments in infrastructure*
- *environment protection*

Method

Through the Rule of Law



Energy Community
- Legal framework



PHLG Recommendations (March / June 2018)

- Establish a Cooperation Group (CPs and EU - MSs)
- Identify and eliminate regulatory gaps
- Put in place common certification conditions across the Energy Community
- Initiate cooperation on the establishment of research and education programmes
- Develop a common crisis management and emergency response mechanism (Treaty - Title III / Title IV)
- Step-up public-private cooperation in cybersecurity

MC Procedural Act (29 November 2018)

on the establishment of Energy Community Coordination Group for Cybersecurity and Critical Infrastructure (CyberCG)

- Domains (of critical infrastructure / essential services in):
  - Electricity / Natural gas / Oil / pollution and combustion emissions
  - Digital and electronic communications (services provided to energy operators)
- Stakeholders
  - Ministries (energy / climate / digital communications & information technologies), NRAs
  - Operators of critical infrastructure / essential services (Production / TSOs / DSOs)
  - National CSIRTs

MC Procedural Act (29 November 2018)

on the establishment of Energy Community Coordination Group for Cybersecurity and Critical Infrastructure (CyberCG)

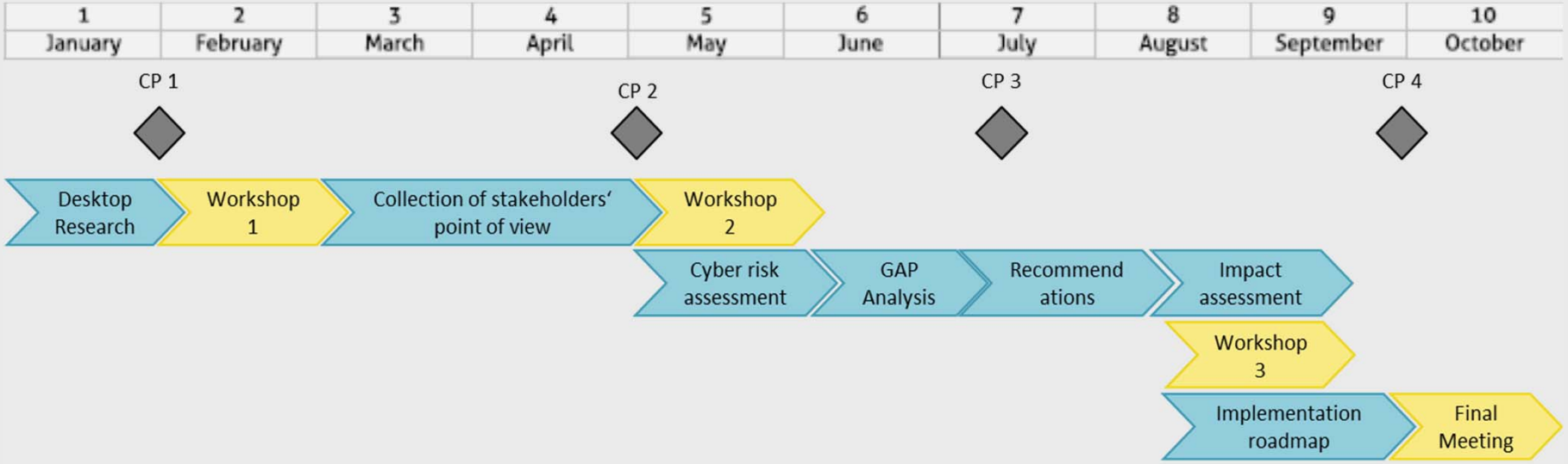
- Relevant EU *acquis* provisions
  - on Electronic communications networks and services - Directive 2002/21/EC
  - on Critical infrastructures (identification / designation / protection) - Directive 2008/114/EC
  - on security of network and information systems (essential services) - NIS Directive - Directive (EU) 2016/1148
  - European standardization in information security - Regulation No. 1025/2012/EU

MC Procedural Act (29 November 2018)

on the establishment of Energy Community Coordination Group for Cybersecurity and Critical Infrastructure (CyberCG)

- Tasks
  - establish administrative and operational environment (focal points / liaison officers)
  - communicate information (reports / strategies / measures) and knowledge (training / research and development / public awareness)
  - Develop and apply EU-coherent methodologies for risk assessment / security criteria / identification and designation of essential services and critical infrastructures,
  - apply EU standards on information security and relevant technologies,
  - establish a CSIRTs network (security incidents and threats / capacity building / blueprint for cooperation and early warning / mutual assistance)
  - facilitate cooperation with EU MSs / gaining observers' status in ENISA

- Domain: all EnC Contracting Partiers
- Scope: electricity / gas authorities, NRA, operators (TSO / DSO), producers, public domain
- Timeline:
  - Inception Report: 22 February 2019
  - First Workshop: 11 April 2019
  - Final Deadline: October 2019



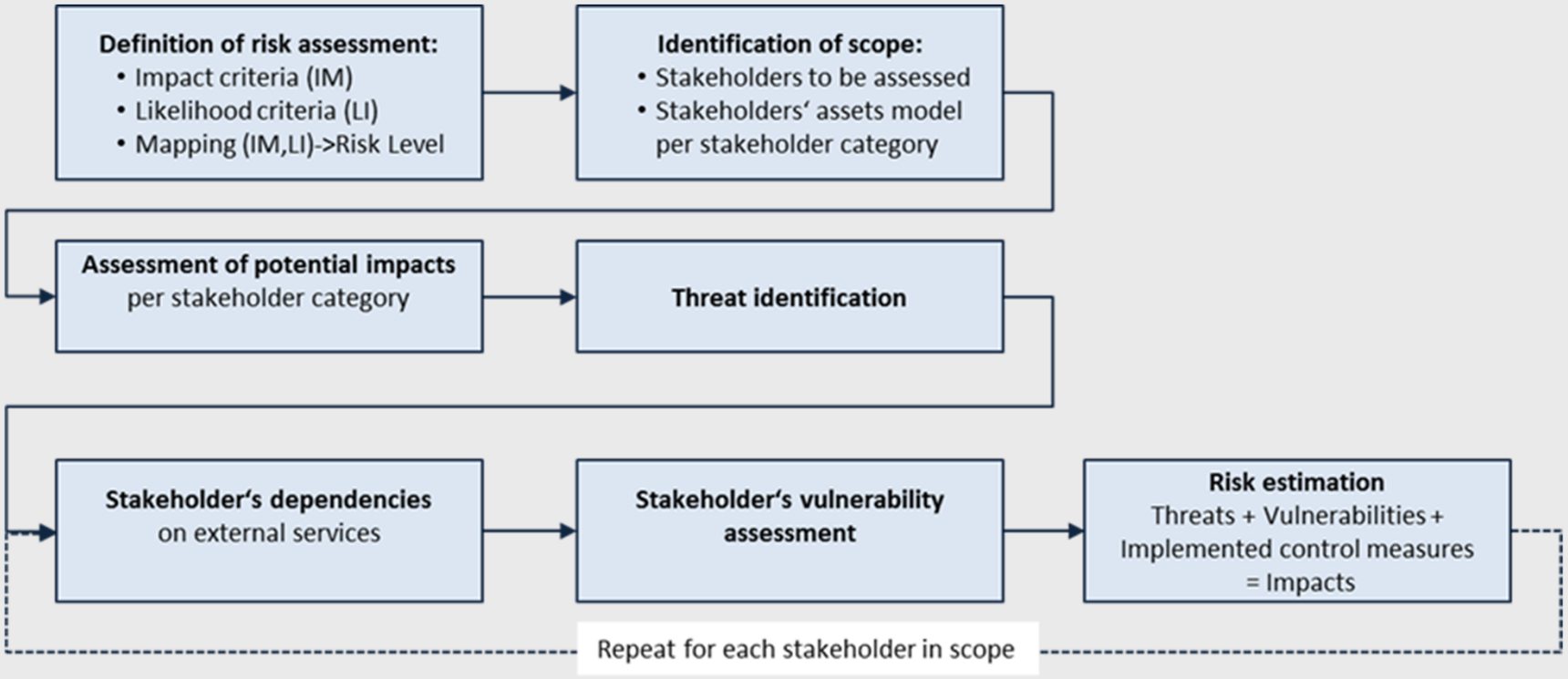
Objectives

- Assess the legal / regulatory environment and identify the regulatory gaps
- Assess the potential cyber threats and risks
- Identify the relevant provisions of the acquis and provide impact assessment of their implementation in the Energy Community
- Propose the necessary measures on national level to improve cybersecurity
- Propose a model for regional cooperation in managing cybersecurity risks and reporting incidents

- Task 1 (stocktaking) – identification and assessment (in particular)
  - Existing cybersecurity environment (legal / policy / administrative / regulatory / enforcement / market)
  - Existing measures in place (pursuant to acquis / Council of Europe Convention on Cybercrime)
  - Existing cross-border cooperation (practices / initiatives / contingencies and potential synergies)
  - the ongoing projects (national / regional) and TA related to cybersecurity
  - cybersecurity standards and certification schemes applied in Contracting Parties
  - existing education and training programmes (expert / public domain) related to cybersecurity
- Task 2 (analysis) – identification of
  - the legal and regulatory gaps inconsistencies
  - gaps in cybersecurity standards

- Task 3 (recommendations)
  - Propose amendments, measures, and recommendations necessary to implement minimum common framework addressing cybersecurity of critical infrastructures
  - Propose cooperation mechanisms in the Energy Community (criteria for the identification of large-scale cybersecurity incidents, cross-border cooperation, relevant actors and standard operating procedures, participation in ENISA)
  - Provide recommendations how to align certification schemes and procedures
  - Propose mechanisms for research, education and training programmes (expert level and public domain)
  - Provide impact assessment for implementation of the proposed acts and measures
  - Develop a roadmap with the timing for the implementation

Risk assessment Methodology



Next Steps

- On-site visits (May – June)
  - Energy / cybersecurity authorities
  - NRAs
  - TSOs
  - Major DSOs / producers / stakeholders
- Risk assessment (early June)
  - Consequences (categories)
  - Capability / motivation and likelihood
  - Risk scenarios
- First Interim report (July)

Draft Conclusions – stemming from the First Meeting and the Procedural Act for establishment of the CyberCG

- **Tasks of the ECS** – before October 2019
  - Draft Biannual Work Program on the format, operation procedures and targets of CyberCG
  - Draft Program for Capacity Building in Cybersecurity (for Ministries, NRA, other authorities)
  - Draft Annual Report (establishment, operation, activities, results, Study Findings and Recommndations)

- **Tasks on National Level** – before October 2019
  - Appointment of Focal Points (Ministries, NRA, Operators of CI, CSIRTs)
  - Provide support and information for the Cybersecurity Study
  - Include Cybersecurity in Tendering Rules for new CI in the energy sector
  - Propose candidates and communicate in the selection of Chairperson of the CyberCG

Draft Conclusions – stemming from the First Meeting and the Procedural Act for establishment of the CyberCG

- Tasks of the CyberCG
  - Establish a Working Group on Critical Infrastructures consisting of Ministries, NRA, Operators – a draft Work Plan shall be developed by 30 October 2019
  - Establish a Working Group on Governance consisting of Ministries, NRA, CSIRTs – including cybersecurity legislation and technical standards (to the necessary level) – a draft Work Plan shall be developed by 30 September 2019
  - Establish a permanent Discussion Panel (network) for CSIRTs – including CSIRT communication channels, coordination I n applied methodology and standards – target to establish an Energy CSIRT cooperation structure in the Energy Community – draft Work Plan shall be developed by 30 September 2019
  - Develop a Program for training, education and capacity building for specific sectors – including (1) Policy authorities and NRA, and (2) CI Operators – draft proposal by 30 October 2019
  - Cooperation with EC, ENISA, CEER, ENTSO-E / ENTSOG

Particularities and Identified Actions

- **Real-time Requirements** – cannot be addressed by standard cyber security solutions
  - Use international standards
  - Apply physical measures
  - Classify/manage your assets
  - Consider privately owned communication networks, or consider specific measures
  - Split system into logical zones
  - Choose secure communication and authentication

- **Cascading effects** – an outage in one country might trigger black-outs in other sectors and countries
  - Evaluate interdependencies
  - Ensure communication framework for early warnings and to cooperate in crisis
  - Ensure level of security for new devices
  - Consider cyber-physical spill overs
  - Establish design criteria for a resilient grid

Particularities and Identified Actions

- Technology mix – risks from (1) legacy components and (2) from new Internet-of-Things devices
  - Follow a cybersecurity-oriented approach when connecting devices
  - Use international standards
  - Establish monitoring and analysis capabilities
  - Conduct specific cybersecurity risk analysis for legacy installations
  - Collaborate with technology providers
  - Update hard- and software

Next Steps

- Application of the Recommendation
- Preparation of a “Network Code” for electricity (cybersecurity)
- Certification of energy technologies

Challenges

- Regulation – the regulatory framework does not yet facilitate effective trans-national cooperation
  - Country-level regulations may forbid sharing of information
  - Problems between EU and NON-EU members
- Organization – diversity of sizes and technologies
  - Complexity of the ENTSO-E power system
  - Connection of extremely diverse facilities (generators, loads) in size and technology
  - Large stakeholder setup – entanglement between large operators (TSO / RSC, DSO)

Policies

- Security – prevention control and compliance with standards
- Resilience – incident monitoring, detection, response and recovery capability

simon.uzunov@energy-community.org
www.energy-community.org