

The background is a dark blue globe showing the outlines of continents. Overlaid on the globe is a complex network of glowing blue lines and nodes, representing a global network or energy grid.

Establishing an organisational framework for a high level of security of network and information systems within the Security of Supply Coordination Group

50th PHLG meeting, Vienna, 21 June 2018

Cyberattacks in the Energy Community are reality...

- ✓ Growing number of cyberattacks on the energy sector in the last years
- ✓ 2015 and 2017 Cyberattacks in Ukraine hit electricity sector

2015 – 30 substation disconnected, more than 200k people in 8 regions affected for several hours

...but also future...

Energy transition brings opportunities but also new challenges –

Moving towards more digitalised, decentralised and decarbonised systems with an increased number of new players, new services, new market places and enhanced cross-border cooperation, is bringing manifold challenges to the security of energy supply and safe operation of the energy infrastructure.

Ensuring cybersecurity in times of increasing application of information and communication technologies (ICT) in the energy sector is one of challenges

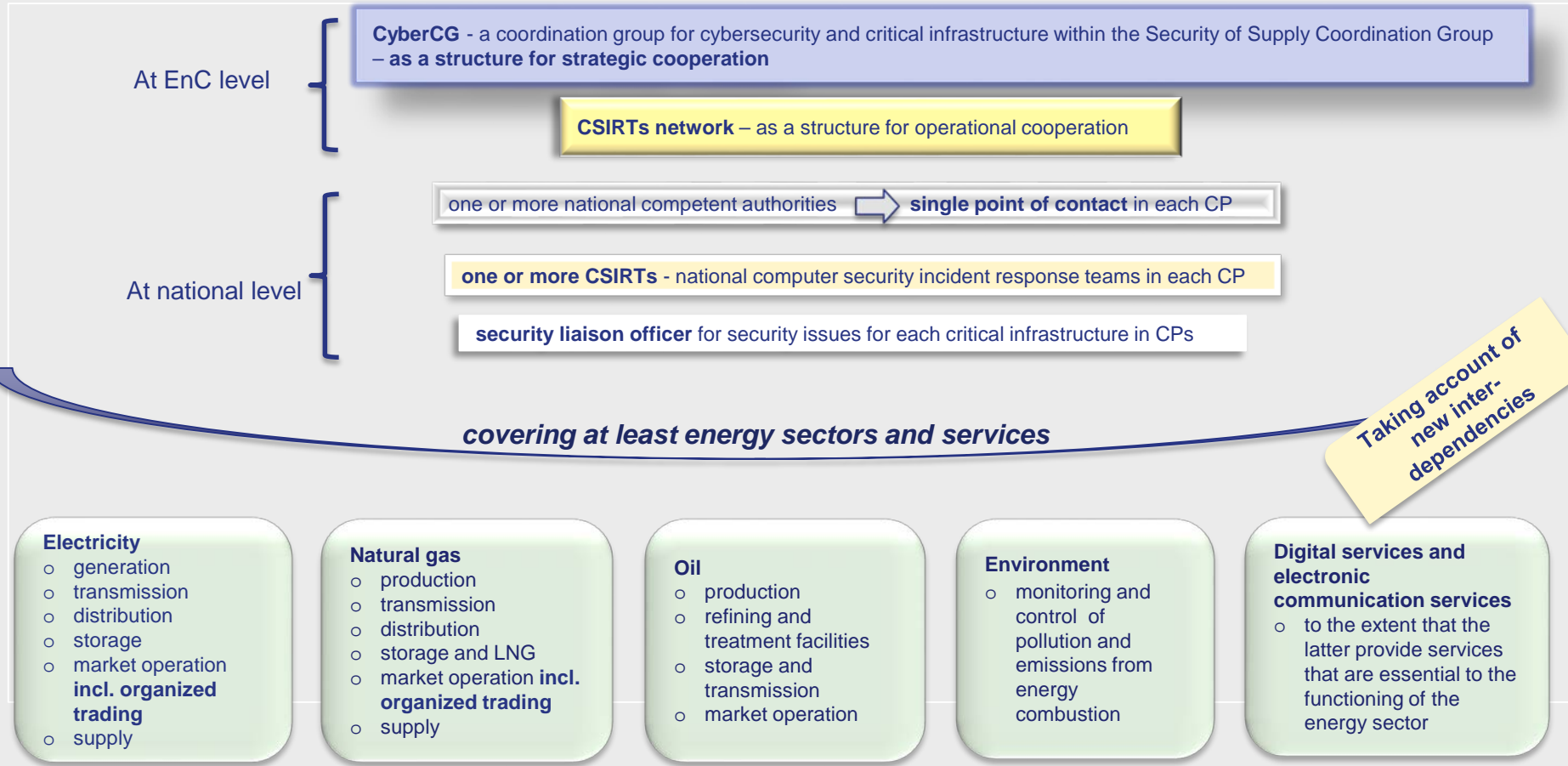


- ✓ **Proliferation of highly interconnected and poorly secured information and communication technologies (ICT) and services**
- ✓ **Outsourcing** of infrastructures and services
- ✓ **Increased interdependency** among market players
- ✓ **Protection concepts and design rules of energy facilities** not reflecting current cyber threats and risks
- ✓ **Dependence on foreign security technologies** (integrity of components used in energy systems)
- ✓ Cross-border interconnected energy network – the ***'weakest link' problem*** and the ***'cascade effect'***
- ✓ Constraints imposed by cybersecurity measures in contrast to **real-time/availability requirements**
- ✓ Availability of **human resources** and their competences
- ✓ **Evolving cybercrime business models**
- ✓ **Blurring lines between state and non-state actors**

Energy Community-added value in facing cyber challenges and risks



- Capability to build and develop platforms for the exchange of information and best practice, for research and development, for building skills and capacities, for raising awareness, and improving preparedness of CPs
- Opportunity to share among the CPs the rarely available human resources with adequate technical expertise on the energy sector-specific challenges
- Knowledge of sector-specific requirements and challenges, as well as of the regional context
- Ability to develop trust and confidence among CPs' and stakeholders
- Better positioned for response coordination in cases of cross-border incidents affecting more than one CPs or CPs and interconnected MSs
- Ability to enhance effective cooperation among CPs within already tested common structures (e.g. Security of Supply Cooperation Group – SoS CG)



The CyberCG consists of

- competent authorities and single point of contacts of CPs
- the CSIRTs network
- security liaison officers
- the Secretariat
- the European Commission
- the ENISA (if possible)
- representatives of Observer and Participant countries
- representatives of the relevant stakeholders

Tasks

- **exchange information and best practice**, discuss modalities, on risks and incidents; on identification of operators and critical infrastructures, on awareness-raising, education programmes and training; research and development
- **discuss capabilities and preparedness of the CPs**, evaluate national strategies, assist CPs in building capacity
- **provide strategic guidance** for the CSIRTs the CSIRTs network
- **engage in discussions** with CPs and MSs on whose territory a potential critical infrastructure is located, and other affected CPs and MSs
- **support** operators of critical infrastructures with best practices, methodological guidelines
- **encourage the use of European or internationally accepted standards and specifications**; discuss them with relevant stakeholders and with relevant organizations

biennial work programmes / A yearly report


Meetings

- twice a year or more, upon a motion of the Chairperson, the Chairperson of SoS CG, the Secretariat
- take part in meetings and activities of the SoS CG

Action at EU level shall inspire further measures in the Energy Community



Participation of the Energy Community CPs in the ENISA
Eliminate regulatory gaps across the single market
Develop an operational pan-European cooperation framework through, inter alia, Title III or Title IV measures
Put in place a common certification framework across the single market
Supply chain integrity of components
Join forces in research and development (e.g., Cloud computing, IoT..)
Building skills, raising hygiene and awareness, education, training programs
Pan-European common exercises and simulations
Quantification and economic regulation of costs of cybersecurity
Insurance sector and coverage of risks arising from cybersecurity
International alliances and diplomacy

The background is a satellite-style image of the Earth at night, showing city lights. Overlaid on this are numerous glowing blue lines that represent energy transmission paths, connecting various points across the globe.

*Thank you for your
attention!*

www.energy-community.org

CSIRTs Network – a structure for operational cooperation at Energy Community level

- The CSIRTs network composed of representatives of the Contracting Parties CSIRTs and the Secretariat

Tasks

- exchange information on CSIRTs' services, operations and cooperation capabilities
- exchange and discuss non-commercially sensitive information related to incidents and associated risks
- at the request of CP's CSIRT, discuss and, where possible, identify a coordinated response to an incident;
- discuss, explore and identify further forms of operational cooperation
- inform the CyberCG of its activities and of the further forms of operational cooperation
- discussing lessons learnt from cyber exercises, including from experience shared by ENISA
- at the request of an individual CSIRT, discuss the capabilities and preparedness of that CSIRT
- issue guidelines in order to facilitate the convergence of operational practices and operational cooperation
- develop a blueprint for cooperation at Energy Community level in case of incidents or crisis affecting one or more CPs

- produces an annual report to the CyberCG
- build on best practice, and where possible, assistance from ENISA

Closed-CSIRT network (within the CSIRT network)

- ✓ composed of a representative from each CPs with an appropriate level of security vetting and clearance for handling classified information
- ✓ make use of specific certified communication means

Tasks

- treat such a threat and incidents considered as classified information by the CPs concerned

Single points of contact in each CP

