THE ENERGY COMMUNITY

CYBERSECURITY IN THE ENERGY SECTOR

VIENNA 11-12-2019

Energy Community Security of Supply CG ELECTRICITY – 7th Meeting

MAIN AREAS OF WORK

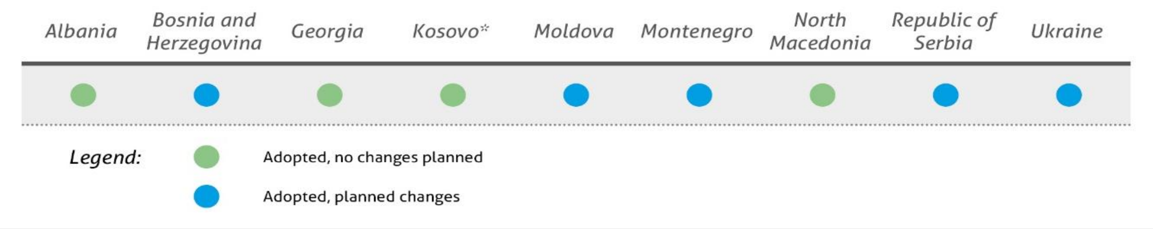
- Statistics
- Electricity
- Renewable energy
- Value added tax
- Competition/ state aid
- Environment
- Cyber security
- Regulator
- Gas
- Climate
- Energy efficiency
- Oil
- Security of energy supply
- General services

Cybersecurity Study of the Energy Community

- 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

Cybersecurity Study – level of implementation

Cybersecurity legislation



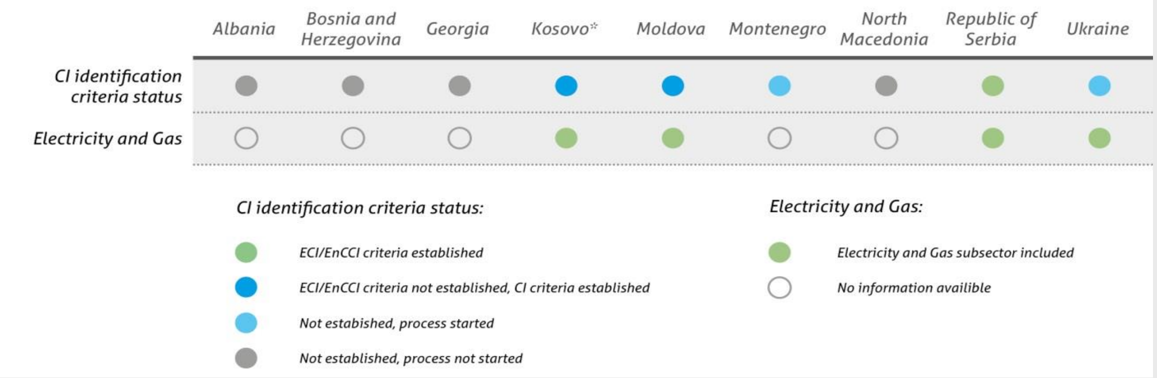
Albania	Bosnia and Herzegovina	Georgia	Kosovo*	Moldova	Montenegro	North Macedonia	Republic of Serbia	Ukraine
🟢	🔵	🟢	🟢	🔵	🔵	🟢	🔵	🔵

Legend:

🟢 Adopted, no changes planned

🔵 Adopted, planned changes

Critical Infrastructures



	Albania	Bosnia and Herzegovina	Georgia	Kosovo*	Moldova	Montenegro	North Macedonia	Republic of Serbia	Ukraine
CI identification criteria status	⚫	⚫	⚫	🔵	🔵	🔹	⚫	🟢	🔹
Electricity and Gas	○	○	○	🟢	🟢	○	○	🟢	🟢

CI identification criteria status:

🟢 *ECI/EnCCI criteria established*

🔵 *ECI/EnCCI criteria not established, CI criteria established*

🔹 *Not estabished, process started*

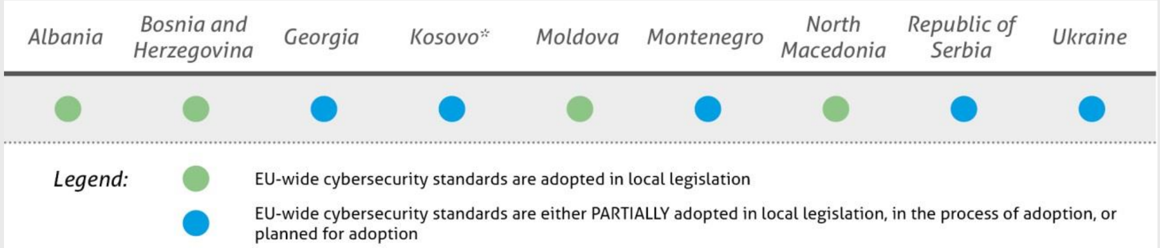
⚫ *Not established, process not started*

Electricity and Gas:

🟢 *Electricity and Gas subsector included*

○ *No information availible*

Technical standards



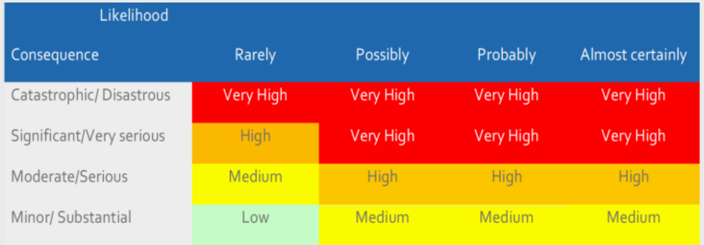
Albania	Bosnia and Herzegovina	Georgia	Kosovo*	Moldova	Montenegro	North Macedonia	Republic of Serbia	Ukraine
🟢	🟢	🔵	🔵	🟢	🔵	🟢	🔵	🔵

Legend:

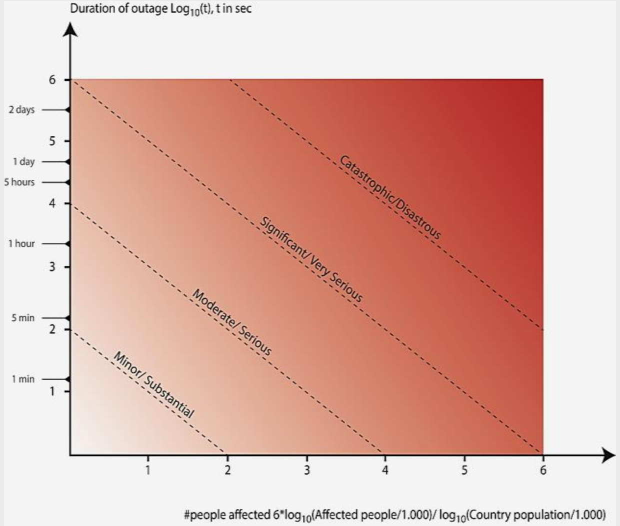
🟢 EU-wide cybersecurity standards are adopted in local legislation

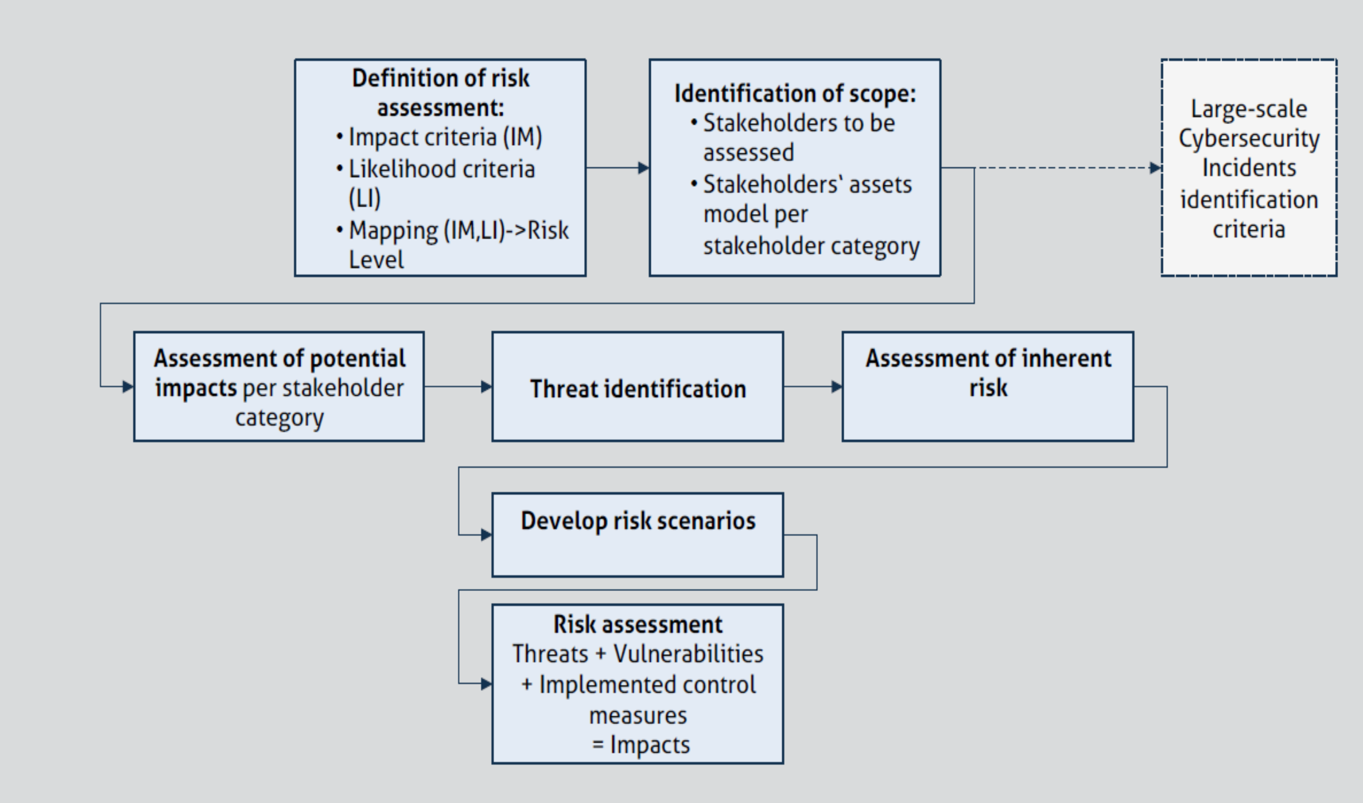
🔵 EU-wide cybersecurity standards are either PARTIALLY adopted in local legislation, in the process of adoption, or planned for adoption

Cybersecurity Study – risk assessment methodology



Likelihood				
Consequence	Rarely	Possibly	Probably	Almost certainly
Catastrophic/ Disastrous	Very High	Very High	Very High	Very High
Significant/Very serious	High	Very High	Very High	Very High
Moderate/Serious	Medium	High	High	High
Minor/ Substantial	Low	Medium	Medium	Medium





Definition of risk assessment:
- Impact criteria (IM)
- Likelihood criteria (LI)
- Mapping (IM,LI)->Risk Level

Identification of scope:
- Stakeholders to be assessed
- Stakeholders' assets model per stakeholder category

Large-scale Cybersecurity Incidents identification criteria

Assessment of potential impacts per stakeholder category

Threat identification

Assessment of inherent risk

Develop risk scenarios

Risk assessment
Threats + Vulnerabilities
+ Implemented control measures
= Impacts

Cybersecurity Study – risk estimation in the energy sector

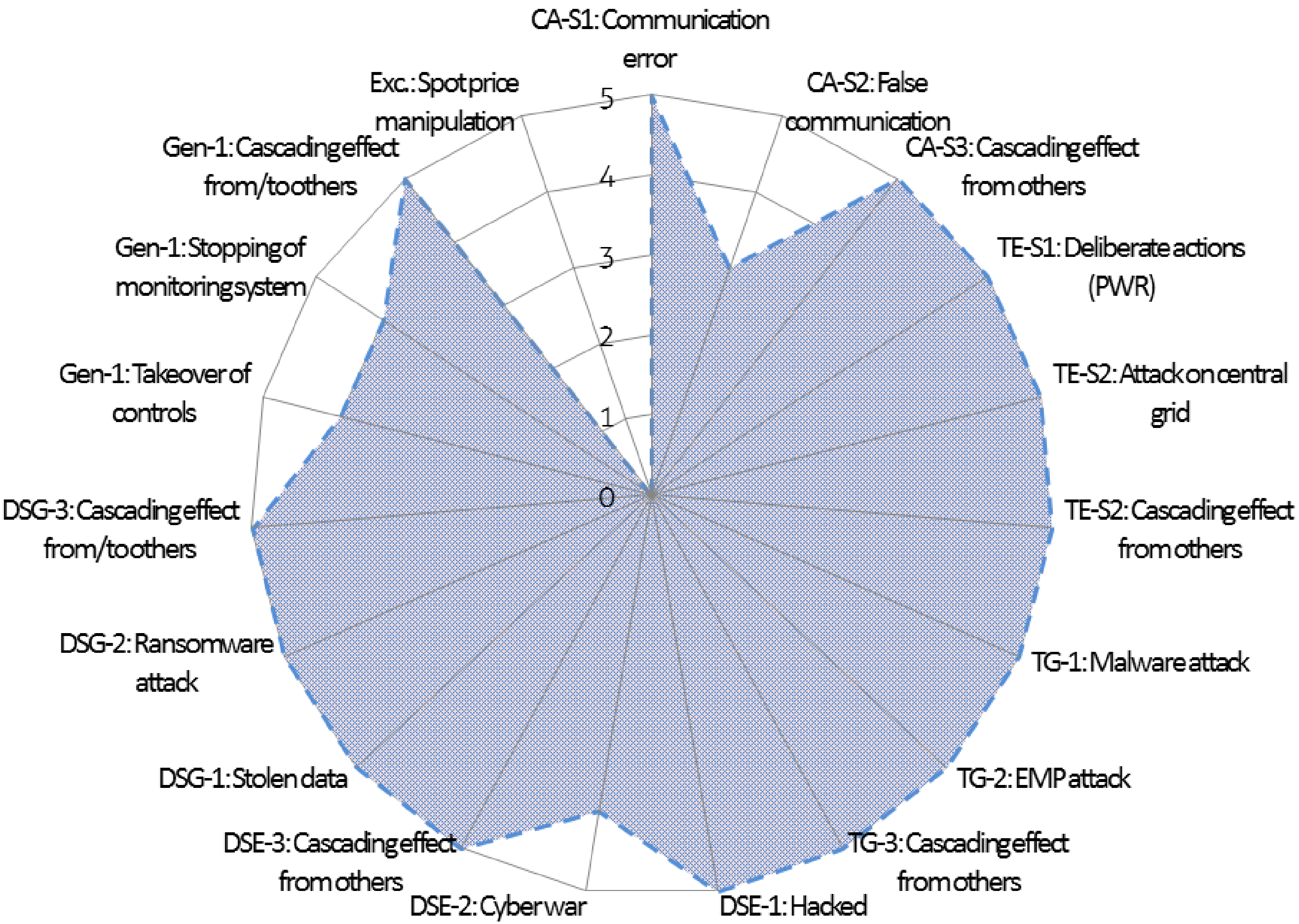
Risk Assessment

- Prioritisation in terms of likelihood and impact
- Distribution according to type of stakeholder

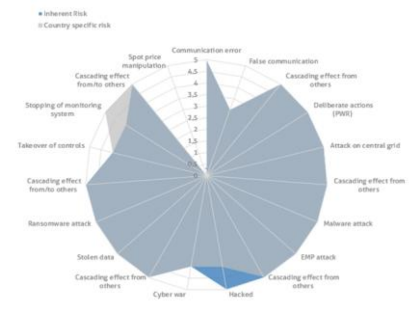
Cyber Threat							
Malware	Web Based Attacks/Web application attacks	Social engeneering/Phising/ Spam	Denial of Service (DoS)	Insider Threat	Cyber Espionage Cyberwarfare	Ransomware	Botnet
MEDIUM RISK for CA/NRA LOW RISK in cascading effect to other energy stakeholder	NOT APPLICABLE for CA NRA	HIGH RISK for CA/NRA MEDIUM RISK in cascading effect to other energy stakeholder	HIGH RISK for CA/NRA LOW RISK in cascading effect to other energy stakeholder	HIGH RISK for CA/NRA HIGH RISK in cascading effect to other energy stakeholder	CRITICAL RISK for CA/NRA HIGH RISK in cascading effect to other energy stakeholder	MEDIUM RISK for CA/NRA MEDIUM RISK in cascading effect to other energy stakeholder	MEDIUM RISK for CA/NRA LOW RISK in cascading effect to other energy stakeholder
HIGH RISK for TSO MEDIUM RISK in cascading effect to other energy stakeholder	MEDIUM RISK for TSO LOW RISK in cascading effect to other energy stakeholder	HIGH RISK for TSO HIGH RISK in cascading effect to other energy stakeholder	LOW RISK for TSO LOW RISK in cascading effect to other energy stakeholder	HIGH RISK for TSO HIGH RISK in cascading effect to other energy stakeholder	HIGH RISK for TSO HIGH RISK in cascading effect to other energy stakeholder	HIGH RISK for TSO HIGH RISK in cascading effect to other energy stakeholder	HIGH RISK for TSO HIGH RISK in cascading effect to other energy stakeholder
MEDIUM RISK for DSO MEDIUM RISK in cascading effect to other energy stakeholder	MEDIUM RISK for DSO LOW RISK in cascading effect to other energy stakeholder	HIGH RISK for DSO MEDIUM RISK in cascading effect to other energy stakeholder	LOW RISK for DSO LOW RISK in cascading effect to other energy stakeholder	MEDIUM RISK for DSO LOW RISK in cascading effect to other energy stakeholder	HIGH RISK for DSO MEDIUM RISK in cascading effect to other energy stakeholder	HIGH RISK for DSO HIGH RISK in cascading effect to other energy stakeholder	HIGH RISK for DSO MEDIUM RISK in cascading effect to other energy stakeholder
LOW RISK for Generation MEDIUM RISK in cascading effect to other energy stakeholder	LOW RISK for Generation LOW RISK in cascading effect to other energy stakeholder	MEDIUM RISK for Generation LOW RISK in cascading effect to other energy stakeholder	LOW RISK for Generation MEDIUM RISK in cascading effect to other energy stakeholder	MEDIUM RISK for Generation LOW RISK in cascading effect to other energy stakeholder	MEDIUM RISK for Generation MEDIUM RISK in cascading effect to other energy stakeholder	HIGH RISK for Generation MEDIUM RISK in cascading effect to other energy stakeholder	MEDIUM RISK for Generation MEDIUM RISK in cascading effect to other energy stakeholder
LOW RISK for Exchange LOW RISK in cascading effect to other energy stakeholder	LOW RISK for Exchange LOW RISK in cascading effect to other energy stakeholder	LOW RISK for Exchange LOW RISK in cascading effect to other energy stakeholder	LOW RISK for Exchange LOW RISK in cascading effect to other energy stakeholder	LOW RISK for Exchange LOW RISK in cascading effect to other energy stakeholder	LOW RISK for Exchange LOW RISK in cascading effect to other energy stakeholder	MEDIUM RISK for Exchange LOW RISK in cascading effect to other energy stakeholder	LOW RISK for Exchange LOW RISK in cascading effect to other energy stakeholder

Risk Scenarios

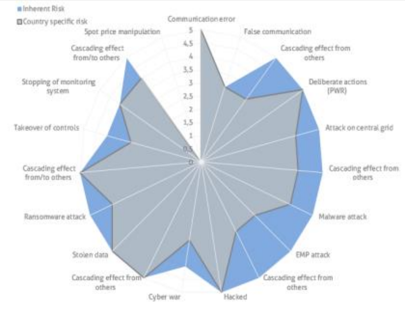
- Inherent risk pattern



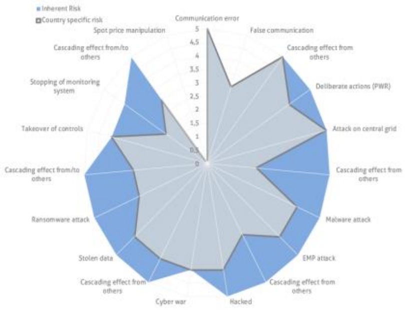
Cybersecurity Study – risk estimation in the energy sector



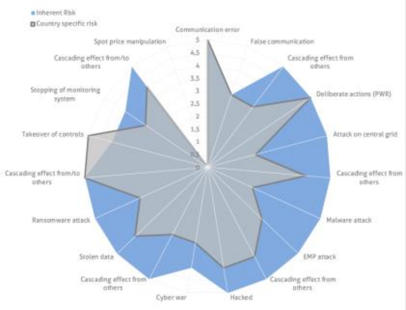
Albania



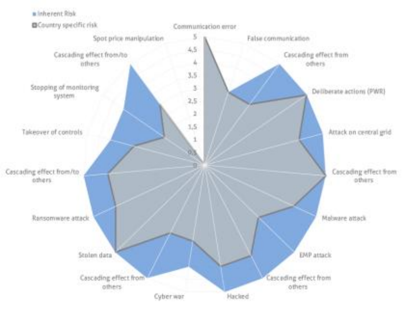
Bosnia and Herzegovina



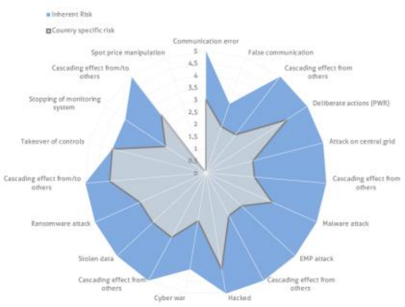
Georgia



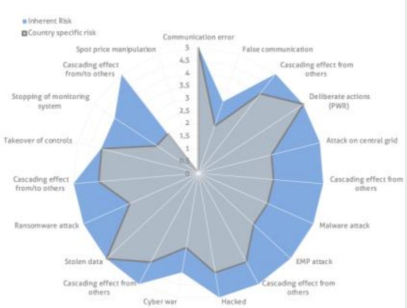
Kosovo*



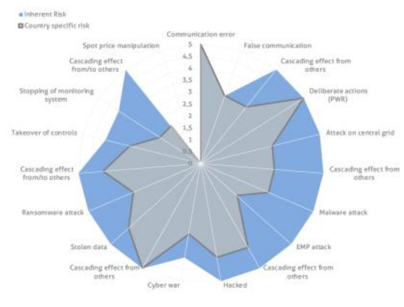
Moldova



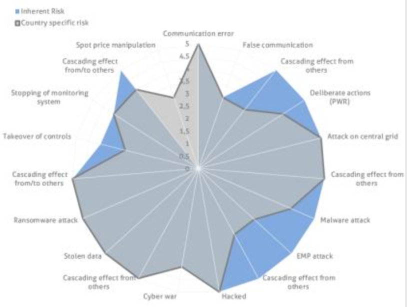
Montenegro



North Macedonia



Serbia



Ukraine

Lack of regulatory framework (missing critical infrastructure / essential services regulation)

NRA/CA

- Missing interoperability with other organisations, a cascading effect high risk (Insider Threat, Cyberwarfare)
- Inability to provide sufficient expertise in case of an incident, a cascading effect critical risk (DoS, Social engineering)

TSO

- Infection of OT systems (SCADA) and legacy systems through IT network (Malware, Ransomware, Botnet)
- Sabotage on OT, a cascading effect high risk (Insider Threat, Cyberwarfare, Ransomware, Botnet)
- Inability to react in a case of an incident, a cascading effect high risk (DoS, Social engineering, Phishing, Spam, Ransomware)

DSO

- Sabotage on OT, a cascading effect high risk (Ransomware)
- Inability to react in a case of an incident (Social engineering, Phishing, Spam, Ransomware)

Power generation

- Infection of OT systems (SCADA) and legacy systems through IT network (Malware, Ransomware, Botnet)

CyberCG – establishment and mandate

MC Procedural Act (29 November 2018) on the establishment of Energy Community Coordination Group for Cybersecurity and Critical Infrastructure (CyberCG)

- Domains (critical infrastructure / essential services)
  - 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 infrastructures / essential services in energy (production / storage / TSO / DSO / PX / RSC)
  - National CSIRTs

CyberCG – establishment and mandate

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) and identification and designation of essential services / critical infrastructures
  - apply the relevant EU technical 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 closer relations with ENISA

CyberCG Work Programme 2020 – 2021 – WG critical infrastructure

Tasks	Targets / Activities	2020												2021											
		Q1			Q2			Q3			Q4			Q1			Q2			Q3			Q4		
WG on ENERGY COMMUNITY CRITICAL INFRASTRUCTURES																									
I – ENERGY COMMUNITY CRITICAL INFRASTRUCTURES (WG-ECCI)	***1.1 Report on the status of Energy Critical Infrastructures / Essential Services***	▓	▓	▓	▓																				
	1.2 Common platform for regional designation of ECCI	▓	▓	▓	▓	▓	▓																		
	2.1 Guidelines for OSP - Operator Security Plans					▓	▓	▓	▓	▓															
	2.2 Regional Implementation of OSP										▓	▓	▓	▓	▓	▓	▓	▓	▓	▓	▓	▓	▓	▓	▓
	- guidelines on regional risk analysis													░	░	░	░	░	░						
	- regional mechanisms for ECCI resilience support																			░	░	░	░	░	░

CyberCG Work Programme 2020 – 2021 – WG cybersecurity governance (min.)

Tasks	Targets / Activities	2020												2021											
		Q1			Q2			Q3			Q4			Q1			Q2			Q3			Q4		
WG on CYBERSECURITY GOVERNANCE IN THE ENERGY COMMUNITY																									
II – CUBERSECURITY GOVERNANCE (WG-CG)	***3.1 Adaptation of the ECI Directive for the Energy Community***	■	■	■	■	■	■																		
	3.2 Adaptation of the NIS Directive for the Energy Community	■	■	■	■	■	■																		
	- adoption / application of ECI and NIS Directives in the EnC CPs							▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒
	- Guidelines for implementation of cybersecurity acquis							■	■	■	■	■	■												
	4.1 Report on the current Cybersecurity Strategies in energy													■	■	■	■								
	4.2 Cybersecurity Strategy of the Energy Community													■	■	■	■	■	■	■	■	■	■	■	■
	- common cybersecurity planning methodology													▒	▒	▒	▒								
	- draft regional cybersecurity strategy																	▒	▒	▒	▒	▒	▒	▒	▒

CyberCG Work Programme 2020 – 2021 – WG cybersecurity governance (NRA)

Tasks	Targets / Activities	2020												2021											
		Q1			Q2			Q3			Q4			Q1			Q2			Q3			Q4		
WG on CYBERSECURITY GOVERNANCE IN THE ENERGY COMMUNITY																									
II – CUBERSECURITY GOVERNANCE (WG-CG)	***5.1 Cybersecurity in certification and tendering of new infrastructure***	■	■	■	■	■	■	■	■	■	■	■													
	5.2 Cybersecurity in regulated prices and tariffs	■	■	■	■	■	■	■	■	■	■	■													
	- guidelines on cybersecurity criteria for new infrastructure [ECS, ECRB]						▨	▨	▨	▨	▨	▨													
	5.3 Application of ISO 27000 standards in the Energy Community									■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	
	- guidelines for technical standards on cybersecurity [ECS, ECRB]																▨	▨	▨	▨	▨	▨	▨	▨	

CyberCG Work Programme 2020 – 2021 – EnC cybersecurity networks (CSIRT)

Tasks	Targets / Activities	2020												2021											
		Q1			Q2			Q3			Q4			Q1			Q2			Q3			Q4		
ENERGY COMMUNITY CYBERSECURITY NETWORKS																									
III – ENERGY COMMUNITY CSIRT NETWORK	**6.1 EnC - CSIRTs electronic platform (setup)**	▓	▓	▓	▓	▓																			
	6.2 CSIRT Panel for Cybersecurity Cooperation (setup)			▓	▓	▓	▓	▓	▓	▓	▓	▓	▓	▓	▓										
	- methodology for regional risk criteria and risk assessment			░	░	░	░	░																	
	- rules / protocol for real-time exchange of information / support					░	░	░	░	░															
	- application of the CSIRT panel protocol – test period									░	░	░	░	░	░										
	6.3 CSIRT Panel for Planning and Education (setup)	▓	▓	▓	▓																				
	- rules / protocol for cooperation in the planning activities	░	░	░	░																				
	- program for education and training / action plan (ECS, WG)			░	░																				
	6.4 Establishment of Energy Community Energy CSIRT	▓	▓	▓	▓	▓	▓	▓	▓	▓	▓	▓	▓	▓	▓	▓	▓	▓	▓	▓	▓	▓	▓	▓	▓
	- establishment / nomination of national energy CSIRT structures	░	░	░	░	░	░	░	░	░	░														
	- draft rules / protocol and program for a regional energy CSIRT						░	░	░	░	░														

CyberCG Work Programme 2020 – 2021 – EnC cybersecurity networks (E-ISAC)

Tasks	Targets / Activities	2020												2021											
		Q1			Q2			Q3			Q4			Q1			Q2			Q3			Q4		
ENERGY COMMUNITY CYBERSECURITY NETWORKS																									
IV – ENERGY COMMUNITY ENERGY ISAC	***7.1 Establishment of Energy Community Energy ISAC***	■	■	■	■	■	■	■	■	■	■														
	- rules / protocol for cooperation of energy enterprises					▨	▨	▨	▨	▨	▨														
	- program for operation of EnC E-ISAC								▨	▨	▨														
	- follow-up activities of consultation activities											▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
	7.2 Platform for support in certification											■	■	■	■	■	■								
	- guidelines on certification criteria and policy [ECS, ENISA]											▨	▨	▨	▨										
	- rules / protocol for support to certification in energy														▨	▨	▨								

CyberCG Work Programme 2020 – 2021 – EnC Cybersecurity Academy

Tasks	Targets / Activities	2020												2021											
		Q1			Q2			Q3			Q4			Q1			Q2			Q3			Q4		
CyberCG EVENTS																									
PERIODIC EVENTS	- CyberCG plenary meetings						🟫						🟫						🟫						🟫
	- CyberCG public events				🟧					🟧							🟧					🟧			
CYBERSECURITY ACADEMY																									
EDUCATION AND TRAINING PROGRAM	- workshop on the Energy Critical Infrastructures / ES [CyberCG]				🟫																				
	- workshop on CSIRT planning / education activities [CSIRT WG]				🟫																				
	- conference on PPP and cooperation in cybersecurity [CyberCG]				🟧																				
	- TA on methodology for minimum cybersecurity criteria [ECS, ECRB]			🟩	🟩	🟩																			
	- workshop on the cybersecurity conditions in tendering [CyberCG, ECRB]					🟫																			
	- TA on methodology for cybersecurity costs in tariffs [ECS, ECRB]			🟩	🟩	🟩																			
	- workshop on methodology for cybersecurity costs [CyberCG, ECRB]					🟫																			
	- SW installation and trial operation [ECS, TA]				🟩	🟩																			
	- workshop on the EnC CSIRT communication platform [CSIRT WG]					🟫																			
	- workshop on ECCI Designation Rules and Action Plan [CyberCG]						🟫																		
	- workshop on the legal transposition of the ECI Directive [CyberCG]						🟫																		
	- workshop on the legal transposition of the NIS Directive [CyberCG]						🟫																		
	- TA on Operator Security Plans (OSP) drafting Methodology [ECS]							🟩	🟩	🟩															
	- training workshops on OSP Methodology / Guidelines [CyberCG]									🟧															
	- workshop on the mechanism for real-time assistance (CSIRT WG]									🟫															
	- TA on electronic platform for the EnC E-ISAC									🟩	🟩														
	- workshop on establishment of EnC E-ISAC										🟫														
	- workshop on the regional E-CSIRT mode of cooperation [CSIRT WG]										🟫														
	- training on regulatory treatment of cybersecurity costs [CyberCG, ECRB]											🟧													
	- TA on regional Risk Analysis Methodology [ECS]										🟩	🟩	🟩												
	- workshop on the regional risk analysis Methodology [CyberCG]												🟫												
	- workshop - application of cybersecurity acquis in energy [CyberCG]												🟧												
	- training exercise on emergency data exchange [CSIRT WG]														🟫										
	- TA on methodology and cost-benefit criteria for 27K [ECS, ECRB]													🟩	🟩	🟩									
	- workshop on ISO 27K methodology [CyberCG, ECRB]															🟫									
	- technical workshop – presentation of Strategies Report [CyberCG]																🟫								
	- workshop on cybersecurity planning methodology [CyberCG]																🟫								
	- workshop / conference on certification in the energy sector																🟧								
	- training on regional cyber threats / OSP exercise [CyberCG]																		🟧						
	- training on technical standards in cybersecurity [CyberCG, ECRB]																							🟧	
	- workshop on the regional ECCI resilience support [CyberCG]																								🟫
	- training workshop on regional cybersecurity planning [CyberCG]																								🟧
CO-ORGANIZATION OF EVENTS (proposal)	- conference on smart energy networks / services and cybersecurity					▨	▨	▨			▨	▨													
	- workshop on cybersecurity in the gas infrastructure			▨		▨	▨	▨			▨	▨													
	- workshop on energy production / storage and cybersecurity			▨		▨	▨	▨			▨	▨													
	- workshop on confidentiality of data in cybersecurity in energy										▨	▨			▨	▨		▨		▨					
	- conference on new technologies and cybersecurity										▨				▨	▨		▨		▨		▨	▨		

THANK YOU

FOR YOUR ATTENTION

simon.uzunov@energy.community.org

🌐 www.energy-community.org

Ener_Community

/company/energy-community

/Ener.Community

▶ /EnergyCommunityTV