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 – risk assessment methodology

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Consequence</th>
<th>Rarely</th>
<th>Possibly</th>
<th>Probably</th>
<th>Almost certain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic/Disastrous</td>
<td>Very High</td>
<td>Very High</td>
<td>Very High</td>
<td>Very High</td>
<td></td>
</tr>
<tr>
<td>Significant/Very serious</td>
<td>High</td>
<td>Very High</td>
<td>Very High</td>
<td>Very High</td>
<td></td>
</tr>
<tr>
<td>Moderate/Serious</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>Minor/Substantial</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td></td>
</tr>
</tbody>
</table>

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
## Risk Assessment

### - Prioritisation in terms of likelihood and impact

<table>
<thead>
<tr>
<th>Cyber Threat</th>
<th>Malware</th>
<th>Web Based Attacks/Web application attacks</th>
<th>Social engineering/Phishing/Spam</th>
<th>Denial of Service (DoS)</th>
<th>Insider Threat</th>
<th>Cyber Espionage Cyberwarfare</th>
<th>Ransomware</th>
<th>Botnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEDIUM RISK for CA/NRA</td>
<td>NOT APPLICABLE for CA/NRA</td>
<td>HIGH RISK for CA/NRA</td>
<td>HIGH RISK for CA/NRA</td>
<td>HIGH RISK for CA/NRA</td>
<td>CRITICAL RISK for CA/NRA</td>
<td>MEDIUM RISK for CA/NRA</td>
<td>MEDIUM RISK for CA/NRA</td>
<td></td>
</tr>
<tr>
<td>LOW RISK in cascading effect to other energy stakeholder</td>
<td>MEDIUM RISK in cascading effect to other energy stakeholder</td>
<td>LOW RISK in cascading effect to other energy stakeholder</td>
<td>HIGH RISK in cascading effect to other energy stakeholder</td>
<td>LOW RISK in cascading effect to other energy stakeholder</td>
<td>HIGH RISK in cascading effect to other energy stakeholder</td>
<td>MEDIUM RISK in cascading effect to other energy stakeholder</td>
<td>LOW RISK in cascading effect to other energy stakeholder</td>
<td></td>
</tr>
</tbody>
</table>

### - Distribution according to type of stakeholder

<table>
<thead>
<tr>
<th>Cyber Threat</th>
<th>Malware</th>
<th>Web Based Attacks/Web application attacks</th>
<th>Social engineering/Phishing/Spam</th>
<th>Denial of Service (DoS)</th>
<th>Insider Threat</th>
<th>Cyber Espionage Cyberwarfare</th>
<th>Ransomware</th>
<th>Botnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEDIUM RISK for TSO</td>
<td>MEDIUM RISK for TSO</td>
<td>HIGH RISK for TSO</td>
<td>HIGH RISK for TSO</td>
<td>HIGH RISK for TSO</td>
<td>HIGH RISK for TSO</td>
<td>MEDIUM RISK for TSO</td>
<td>MEDIUM RISK for TSO</td>
<td></td>
</tr>
<tr>
<td>MEDIUM RISK in cascading effect to other energy stakeholder</td>
<td>LOW RISK in cascading effect to other energy stakeholder</td>
<td>HIGH RISK in cascading effect to other energy stakeholder</td>
<td>HIGH RISK in cascading effect to other energy stakeholder</td>
<td>HIGH RISK in cascading effect to other energy stakeholder</td>
<td>HIGH RISK in cascading effect to other energy stakeholder</td>
<td>MEDIUM RISK in cascading effect to other energy stakeholder</td>
<td>HIGH RISK in cascading effect to other energy stakeholder</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cyber Threat</th>
<th>Malware</th>
<th>Web Based Attacks/Web application attacks</th>
<th>Social engineering/Phishing/Spam</th>
<th>Denial of Service (DoS)</th>
<th>Insider Threat</th>
<th>Cyber Espionage Cyberwarfare</th>
<th>Ransomware</th>
<th>Botnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEDIUM RISK for DSO</td>
<td>MEDIUM RISK for DSO</td>
<td>HIGH RISK for DSO</td>
<td>HIGH RISK for DSO</td>
<td>HIGH RISK for DSO</td>
<td>HIGH RISK for DSO</td>
<td>MEDIUM RISK for DSO</td>
<td>MEDIUM RISK for DSO</td>
<td></td>
</tr>
<tr>
<td>MEDIUM RISK in cascading effect to other energy stakeholder</td>
<td>LOW RISK in cascading effect to other energy stakeholder</td>
<td>HIGH RISK in cascading effect to other energy stakeholder</td>
<td>HIGH RISK in cascading effect to other energy stakeholder</td>
<td>HIGH RISK in cascading effect to other energy stakeholder</td>
<td>HIGH RISK in cascading effect to other energy stakeholder</td>
<td>MEDIUM RISK in cascading effect to other energy stakeholder</td>
<td>HIGH RISK in cascading effect to other energy stakeholder</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cyber Threat</th>
<th>Malware</th>
<th>Web Based Attacks/Web application attacks</th>
<th>Social engineering/Phishing/Spam</th>
<th>Denial of Service (DoS)</th>
<th>Insider Threat</th>
<th>Cyber Espionage Cyberwarfare</th>
<th>Ransomware</th>
<th>Botnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOW RISK for Generation</td>
<td>LOW RISK for Generation</td>
<td>MEDIUM RISK for Generation</td>
<td>LOW RISK for Generation</td>
<td>MEDIUM RISK for Generation</td>
<td>MEDIUM RISK for Generation</td>
<td>HIGH RISK for Generation</td>
<td>MEDIUM RISK for Generation</td>
<td></td>
</tr>
<tr>
<td>MEDIUM RISK in cascading effect to other energy stakeholder</td>
<td>HIGH RISK in cascading effect to other energy stakeholder</td>
<td>LOW RISK in cascading effect to other energy stakeholder</td>
<td>LOW RISK in cascading effect to other energy stakeholder</td>
<td>LOW RISK in cascading effect to other energy stakeholder</td>
<td>LOW RISK in cascading effect to other energy stakeholder</td>
<td>MEDIUM RISK in cascading effect to other energy stakeholder</td>
<td>MEDIUM RISK in cascading effect to other energy stakeholder</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cyber Threat</th>
<th>Malware</th>
<th>Web Based Attacks/Web application attacks</th>
<th>Social engineering/Phishing/Spam</th>
<th>Denial of Service (DoS)</th>
<th>Insider Threat</th>
<th>Cyber Espionage Cyberwarfare</th>
<th>Ransomware</th>
<th>Botnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOW RISK in cascading effect to other energy stakeholder</td>
<td>LOW RISK in cascading effect to other energy stakeholder</td>
<td>LOW RISK in cascading effect to other energy stakeholder</td>
<td>LOW RISK in cascading effect to other energy stakeholder</td>
<td>LOW RISK in cascading effect to other energy stakeholder</td>
<td>LOW RISK in cascading effect to other energy stakeholder</td>
<td>LOW RISK in cascading effect to other energy stakeholder</td>
<td>LOW RISK in cascading effect to other energy stakeholder</td>
<td></td>
</tr>
</tbody>
</table>
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

The Energy Community Secretariat | SoS CG ELECTRICITY Meeting 7 – Vienna, 11/12/2019
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)
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
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**
### WG on ENERGY COMMUNITY CRITICAL INFRASTRUCTURES

#### 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

---

**Tasks Targets / Activities**

<table>
<thead>
<tr>
<th>2020</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1</td>
<td>Q1</td>
</tr>
<tr>
<td>Q2</td>
<td>Q2</td>
</tr>
<tr>
<td>Q3</td>
<td>Q3</td>
</tr>
<tr>
<td>Q4</td>
<td>Q4</td>
</tr>
<tr>
<td>II – CYBERSECURITY GOVERNANCE (WG-CG)</td>
<td>Tasks</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>WG on CYBERSECURITY GOVERNANCE IN THE ENERGY COMMUNITY</td>
<td>3.1 Adaptation of the ECI Directive for the Energy Community</td>
</tr>
<tr>
<td></td>
<td>3.2 Adaptation of the NIS Directive for the Energy Community</td>
</tr>
<tr>
<td></td>
<td>- adoption / application of ECI and NIS Directives in the EnC CPs</td>
</tr>
<tr>
<td></td>
<td>- Guidelines for implementation of cybersecurity acquis</td>
</tr>
<tr>
<td></td>
<td>4.1 Report on the current Cybersecurity Strategies in energy</td>
</tr>
<tr>
<td></td>
<td>4.2 Cybersecurity Strategy of the Energy Community</td>
</tr>
<tr>
<td></td>
<td>- common cybersecurity planning methodology</td>
</tr>
<tr>
<td></td>
<td>- draft regional cybersecurity strategy</td>
</tr>
</tbody>
</table>
### WG on CYBERSECURITY GOVERNANCE IN THE ENERGY COMMUNITY

#### II – CYBERSECURITY GOVERNANCE (WG-CG)

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Targets / Activities</th>
<th>2020</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Q1</td>
<td>Q2</td>
</tr>
</tbody>
</table>

---

#### 5.1 Cybersecurity in certification and tendering of new infrastructure

- guidelines on cybersecurity criteria for new infrastructure [ECS, ECRB]

#### 5.2 Cybersecurity in regulated prices and tariffs

- guidelines for technical standards on cybersecurity [ECS, ECRB]

#### 5.3 Application of ISO 27000 standards in the Energy Community

- guidelines for technical standards on cybersecurity [ECS, ECRB]
<table>
<thead>
<tr>
<th>Tasks</th>
<th>Targets / Activities</th>
<th>2020 Q1</th>
<th>2020 Q2</th>
<th>2020 Q3</th>
<th>2020 Q4</th>
<th>2021 Q1</th>
<th>2021 Q2</th>
<th>2021 Q3</th>
<th>2021 Q4</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENERGY COMMUNITY CYBERSECURITY NETWORKS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>III – ENERGY COMMUNITY CSIRT NETWORK</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1 EnC - CSIRTs electronic platform (setup)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.2 CSIRT Panel for Cybersecurity Cooperation (setup)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- methodology for regional risk criteria and risk assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- rules / protocol for real-time exchange of information / support</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- application of the CSIRT panel protocol – test period</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.3 CSIRT Panel for Planning and Education (setup)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- rules / protocol for cooperation in the planning activities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- program for education and training / action plan (ECS, WG)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.4 Establishment of Energy Community Energy CSIRT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- establishment / nomination of national energy CSIRT structures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- draft rules / protocol and program for a regional energy CSIRT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Energy Community Cybersecurity Networks

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Targets / Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1 Establishment of Energy Community Energy ISAC</td>
<td>- rules / protocol for cooperation of energy enterprises</td>
</tr>
<tr>
<td></td>
<td>- program for operation of EnC E-ISAC</td>
</tr>
<tr>
<td></td>
<td>- follow-up activities of consultation activities</td>
</tr>
<tr>
<td>7.2 Platform for support in certification</td>
<td>- guidelines on certification criteria and policy [ECS, ENISA]</td>
</tr>
<tr>
<td></td>
<td>- rules / protocol for support to certification in energy</td>
</tr>
</tbody>
</table>

### IV – Energy Community Energy ISAC

<table>
<thead>
<tr>
<th></th>
<th>2020</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1</td>
<td>Q2</td>
<td>Q3</td>
</tr>
<tr>
<td>IV</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The Energy Community Secretariat | SoS CG ELECTRICITY Meeting 7 – Vienna, 11/12/2019
## CyberCG Work Programme 2020 – 2021 – EnC Cybersecurity Academy

### Tasks

<table>
<thead>
<tr>
<th>Targets / Activities</th>
<th>2020</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Q1</strong></td>
<td><strong>Q2</strong></td>
<td><strong>Q3</strong></td>
</tr>
</tbody>
</table>

### CyberCG EVENTS

- CyberCG plenary meetings
- CyberCG public events

### PERIODIC EVENTS

- 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 NIS Directive [CyberCG]
- TA on methodology for cybersecurity costs in tariffs [ECS, ECRB]
- workshop on methodology for cybersecurity costs in tariffs [ECS, TA]
- workshop on methodology for real-time assistance [CSIRT WG]
- workshop on the EnC CSIRT communication platform [CSIRT WG]
- workshop on the legal transposition of the ECI 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 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 the regional ECCI resilience support [CyberCG]
- conference on smart energy networks / services and cybersecurity
- workshop on cybersecurity in the gas infrastructure
- workshop on cybersecurity planning methodology [CyberCG]
- workshop on confidentiality of data in cybersecurity in energy
- conference on new technologies and cybersecurity

### CYBERSECURITY ACADEMY

- 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 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 the regional ECCI resilience support [CyberCG]
- 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

### 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 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 the regional ECCI resilience support [CyberCG]
- 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

### CO-ORGANIZATION OF EVENTS (proposal)

- 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 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 the regional ECCI resilience support [CyberCG]
- 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