Cybersecurity dimension of the Energy Community

Security of Supply Coordination Group
5th Meeting of the Subgroup for Electricity

Energy Community Secretariat

Vienna, 19 December 2018

Background

❖ (PHLG - March / June 2018) - Recommendations

- 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 emergency response mechanism, inter alia through Title III or Title IV measures
- Step-up public-private cooperation in cybersecurity

Cybersecurity framework

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

  - …to promote high level of security of network and information systems and of critical infrastructure
  - Domains for Essential Services / Critical Infrastructure
    - Electricity (generation, transmission, distribution, supply, storage, market operation)
    - Natural gas (production, transmission, distribution, supply, storage, market operation, LNG)
    - Oil (production, refining and treatment, transmission, market operation, storage)
    - Pollution and emission from energy combustion (monitoring, control)
    - Digital and electronic communication services (provided to operators of energy services essential to the functioning of an energy sector)
  - CyberCG Activities
    - Perform the defined **Tasks** in cybersecurity coordination
    - Liaise with a network of CSIRTs (Computer Security Incident Response Team)
    - Liaise with Security Officers for critical infrastructure

Cybersecurity framework

❖ Cybersecurity Coordination Group

- Relevant EU *acquis*
  - Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems (NIS Directive)
  - Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services
  - Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection
  - Regulation No. 1025/2012/EU on European standardization
- Stakeholders
  - Energy Ministries and regulatory authorities
  - Ministries and authorities responsible for monitoring emissions and climate protection
  - Ministries and authorities responsible for digital communication and information technologies
  - Operators of energy networks, systems, markets and critical infrastructure
  - Energy market participants, suppliers and consumers
  - National CSIRTs
  - EC, ECS, EU Agency for Information and Network Security (ENISA)

Cybersecurity framework

❖ Cybersecurity Coordination Group

- **CyberCG** tasks
  - establish administrative and operational environment (single contact points, responsible authorities, liaison officers for critical infrastructure / operators of essential services, digital service providers, CSIRTs)
  - communicate information / reports on all relevant developments (strategies, enforcement measures) related to security requirements, essential services and critical infrastructure
  - communicate knowledge for awareness rising, research and development, training
  - support EU coherent security criteria, standards, specifications and technologies, facilitate their assessment
  - support development of methodologies for risk assessment and exchange of best practices
  - facilitate and coordinate identification of essential services and designation of critical infrastructures
  - facilitate agreements between EnC CPs and EU Member States, observers status in ENISA
  - report to ECS and MC
- **CSIRT Network** tasks
  - exchange of information on security incidents, threats, and responses, lessons learned, capacity building
  - adopt protocols and develop blueprint for cooperation, provide support / early warning / mutual assistance

Cybersecurity study

❖ Study on Cybersecurity in energy

- Timeline
  - Consultant contracted: 30 November 2018
  - Kick-off meeting: 13 December 2018
  - Duration: 10 months
- Contracting Parties to:
  - Work closely with the consultant
  - Provide all the necessary data
  - Engage the relevant actors in the energy sector

Cybersecurity study

❖ Study on Cybersecurity in energy

- Task 1 (stocktaking)
  - Identify cyber threats and risks to which Contracting Parties are exposed
  - Identify the current legal and policy framework and administrative and regulatory rules and environment including competent authorities and law enforcement authorities relevant for cybersecurity in the domain of energy. In particular assess:
    - ✓ National strategies related to cybersecurity
    - ✓ Resilience measures including crisis prevention, monitoring and notification of incidents
    - ✓ Security requirements applicable in the energy and dependent sectors
    - ✓ Mechanisms for cross-border incident and crisis management
    - ✓ Public-private initiatives related to cybersecurity and existing training and education programmes
  - Assess whether Contracting Parties have measures in place transposing the NIS Directive, the Directive on European critical infrastructure and the Directive on attacks against information systems
  - Assess whether Contracting Parties took measures to implement the Council of Europe Convention on Cybercrime
  - Identify the current institutional framework for enhancing cybersecurity (authorities, market participants, CSIRTs)
  - Identify the existing cross-border cooperation initiatives
  - Identify the ongoing projects and technical assistance related to improving the governance on cybersecurity
  - Identify existing cybersecurity standards and certification schemes in Contracting Parties
  - Identify existing education and training programmes related to cybersecurity

Cybersecurity study

❖ Study on Cybersecurity in energy

- Task 2 (analysis)
  - Based on the analysis of Task 1, identify the legal and regulatory gaps, inconsistencies and diverging provisions in the Contracting Parties' existing legal, regulatory and institutional frameworks
  - Identify and prepare an overview of the gaps in cybersecurity standards between the Contracting Parties and standards applicable in the EU
- Task 3 (recommendations)
  - Propose amendments, policies, measures, procedures and recommendations necessary to implement minimum common framework addressing cybersecurity of critical infrastructure in the Energy Community
  - 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)
  - Provide recommendations how to align certification schemes and procedures as well as research, education and training programmes
  - Provide impact assessment of the implementation of the proposed acts and measures in the Energy Community
  - Develop a roadmap with the timing of the implementation of the proposed provisions and measures

www.energy-community.org