Meeting Conclusions

From:	*Simon Uzunov*
Date	*11.04.2019*
Location:	*Am Hof 4/6, 1010 Vienna*
Subject:	*CyberCG Meeting # 1*

Introduction

The first Meeting of the Energy Community Coordination Group for Cybersecurity and Critical Infrastructures (**CyberCG**) took place in Vienna, on 11 April 2019, attended by 30 representatives of the Energy Community Contracting Parties (**CP**) – ministries, national regulatory authorities (**NRA**), energy operators and companies in the electricity and gas sectors, and computer security incident response teams (**CSIRT**). Representatives from the European Union (**EU**) – Commission (DG ENER), ENTSO-E, ENISA, CEER, and the team of experts working on the ECS Study on Cybersecurity in the Energy Community, took part in the discussions.

The Energy Community Secretariat (**ECS**) hosted the meeting as the third session in the *Cybersecurity Day in the Energy Community*[1]. The meeting was conducted in accordance with the announced *Agenda*[2].

The main reason for convening the meeting was to make the CyberCG operational and discuss:

- its composition, mode of operation and communication,
- areas and framework of activity and tasks,
- targets and actions to fulfil them.

Energy Community established CyberCG aiming to improve and enhance cybersecurity in energy in line with the European model. Its performance, structure, activities and tasks are stipulated in the Energy Community Procedural Act (**PA**) 2018/PA/2/MC-EnC[3] and the Terms of Reference (**ToR**) provided in annex, adopted by the Energy Community Ministerial Council in November 2018. The PA identifies the stakeholder groups and defines their role in the CyberCG cooperation agenda.

The PA also identifies the main sources of the legal framework relevant for cybersecurity (applied in energy): the Directive 2002/21/EC[4], Directive 2008/114/EC[5], Directive 2016/1148/EU[6], and definitions from Regulation No 1025/2012/EU[7]. Another source of cybersecurity criteria, discussed at the meeting, are the ISO 27000 Standards[8].

In December 2018 ECS has launched a *Study on Cybersecurity in the Energy Community* (**Study**) aimed to provide basic information on the legal compliance, risk analysis, gap analysis and draft proposals for bringing the legal and regulatory frameworks on Cybersecurity in the Energy Community CPs, and a roadmap for development of regional cooperation and communication platform.

In accordance with Article 5.1 of the ToR, CyberCG shall support implementation of cybersecurity legal provisions, monitoring and regulation mechanisms, establishment of communication channels and cooperation platforms among the CPs, identification and nomination of critical infrastructures and essential services, coordination in the domain of cybersecurity standards, capacity building, and CP participation in cybersecurity on the EU level.

---

[1] https://www.energy-community.org/news/Energy-Community-News/2019/04/12.html
[2] https://www.energy-community.org/dam/jcr:23a32f92-e7e4-49c0-9b9f-9fdee9bbdc60/Cyber_Agenda_042019.pdf
[3] https://www.energy-community.org/dam/jcr:a9163c92-fb05-40c3-a74c-acca91fe94c1/PA_02_2018_MC-EnC_CSCG_112018.pdf
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002L0021
[5] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32008L0114
[6] https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG
[7] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012R1025
[8] https://www.iso.org/isoiec-27001-information-security.html

The present Conclusions have been drafted on the basis of Articles 7.2 of the ToR.

Conclusions

Tasks of the Energy Community Secretariat

1. Based on Article 5.2 of the ToR ECS, by 30 June 2019 will draft a biannual Working Program (**WP**) on the structure, principles of operation, procedures and framework of activities of the CyberCG.

   The WP shall include platform for cooperation with relevant EU institutions active in cybersecurity domain (EC, CEER, ENISA, ENTSO-E, ENTSOG), with relevant EU Member States, and with related cooperation groups in the Energy Community (ECRB, security of supply coordination groups for electricity and gas, coordination group of electricity distribution system operators – ECDSO, etc.).

2. Pursuant Article 7.3 of the ToR, by 30 September 2019 ECS, in consultation with the competent EU bodies and other stakeholders will propose to the CyberCG a *Program for capacity building on cybersecurity* (legal and regulatory matters, policy and best practices) – for the Ministries responsible for energy, NRAs and other relevant state authorities.

3. By 31 October 2019, ECS will draft an annual report pursuant to Article 5.4 of the ToR, addressing the developments in the CyberCG establishment, the findings of the Study and the steps and initiatives taken, and submit it to the Group for comments. The annual report will become part of the Secretariat's general reporting.

Tasks on national level

4. As requested by letter from the Secretariat dated 20 December 2018, and according to Articles 1.2 and 1.3 of the PA, Contracting Parties will complete the nomination of "Focal Points" in the CyberCG by 30 May 2019. Focal Points may be representatives from national competent authorities (Ministries, NRAs), represents from national CSIRTs, or Security Liaison Officers from the operators of critical infrastructures appointed pursuant to Article 11.1 of the ToR.

5. The same authorities, operators and CSIRTs will provide support and all the relevant information to the expert team engaged by the Secretariat for completion of the Study on Cybersecurity in the Energy Community.

6. In all applicable cases, the CPs will include cybersecurity criteria in their tendering rules and criteria related to new energy infrastructures.

7. By 30 September 2019, the CPs, through their Focal Points shall communicate to ECS candidates for the Chairperson of CyberCG according to Article 6 of the ToR. The Chairperson will be appointed at its next meeting.

Tasks of the CyberCG

8. The CyberCG establishes a Working Group (**WG**) on Critical Infrastructures – aimed to monitor, report, coordinate and support, as applicable, the process of identification and nomination of critical energy infrastructures (**CI**) in the Energy Community. Main stakeholders shall be the representatives of authorities responsible for CI identification and nomination – NRA and Ministries, supported by individual liaison officers, as required.

   By 30 October 2019, ECS will develop a corresponding Work Plan defining the format of the WG, specific tasks, domain of activity, obligations and targets, and propose it to the CyberCG. The WG shall provide annual progress report to the CyberCG. Ultimately, the WG tasks should extend over the NIS Directive requirements referring to providers of essential services.

9. Based on Article 5.1 of the ToR, the CyberCG establishes a Working Group on governance. The WG aims to coordinate: (1) the adoption of relevant legislation, common security policies and regulatory rule in cybersecurity applied by the authorities and NRA; and (2) considerations

of security and technical standards (in particular ISO 27000) to be applied by the operators of critical infrastructures and energy companies. The goal is to streamline the discussions and facilitate both policy decisions and standardization process in the CPs, including phased approach and prerequisites for full application.

By 30 September 2019, ECS will draft the Work Plan for the WG, with the format in both areas, specific tasks, obligations and targets, and propose it to the CyberCG.

10. Based on Articles 8 and 9 of the ToR, the CyberCG shall establish a permanent Panel for discussion on CSIRT operation in energy. Topics shall include links between CSIRT community and energy sectors, communication channels and standards, threat analysis, early warning systems, resilience criteria, best practices in cybersecurity, CSIRT network in energy, etc. Format shall include continuous update and exchange of information, consultative meetings, policy papers, workshops and training sessions, etc. Ultimately, the Panel shall target to define and establish an Energy CSIRT structure in the Energy Community.

    By 30 September 2019, ECS will draft the Work Plan for the Panel.

11. In the domain of building communication networks, by 30 October 2019 ECS shall develop and propose to CyberCG a draft Program for training and capacity building in Cybersecurity, following the obligations of Article 5.1 of the ToR. The Program will include workshops and specific training sessions for: (1) policy authorities and NRAs – on the legal framework, enforcement, data protection, cybersecurity policies in energy, achievements and best practices on cybersecurity in EU, etc.; and (2) for operators of critical infrastructure – on cybersecurity risk management, criteria and policy for standardization, building of communication networks, threat analysis, etc. Training shall involve cooperation with CSIRT community and experts from the relevant EU authorities.

12. The CyberCG will aim at establishing a platform for cooperation on cybersecurity with ENISA. Cooperation shall address the scope of questions of common interest, format of communication and the domain of stakeholders included, protocols, restrictions and targets.

Next activities of the CyberCG

14 Data communication and progress of the Study shall be presented on a workshop in June 2019, the findings and recommendations in October 2019. The findings and proposals shall serve as references and inputs for the draft work programs defining the CyberCG activities.

15 Next meeting shall be scheduled in October 2019. It shall aim to set the structure (Focal Points, chair, co-chairs), establish the Working Groups, adopt a 2-year Work Program for the CyberCG and Work Plans for the Working Groups and other forms of cooperation, define the short-term activities and targets, take stock of the Study findings and recommendations and discuss the draft Report.

16 Communication and coordination of the activities within CyberCG shall be facilitated by the Secretariat.