6th E.DSO–ENCS–ENISA–ENTSO-E Cybersecurity Event
"European energy grids' security in a changed landscape – closing the skills gap and getting prepared"
in partnership with EE-ISAC

21 September 2023
10H00 to 16H00 EEST (09H00 to 15H00 CEST)

Session: Testimonial from Eastern Countries experience

Davor Bajs, Energy Community Secretariat

Energy Community Secretariat

Areas of work

Energy Community Coordination Group for Cyber-Security and Critical Infrastructure (CyberCG)

- 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

Overview of cyber-security issues in the Contracting Parties

	Law on Cybersecurity (2017), Regulation on Cybersecurity of Critical Infrastructures in the Power Sector (2020), National Strategy for Cybersecurity (2020)
	No state law, no common CSIRT structure, the working group on cybersecurity works on the Roadmap for the security of network and information systems in the energy sector
	The Law on Information Security (2012/2021), Digital Governance Agency (DGA) established in 2020, hosting the national CERT of Georgia (CERT-GOV-GE)
	The Law on Critical Infrastructure (2018), CyS strategy for the energy sector 2023 – 2027 drafted, the Law on security of networks and information systems (2023)
	The Cybersecurity Programme 2016 – 2020, Law on CyS (2023)

Overview of cyber-security issues in the Contracting Parties

The Law on Information Security (2010/16/20/21), The Law on Designation and Protection of Critical Infrastructure (2019) , Draft Law on Information Security, Cybersecurity Strategy 2022-2026

The Cybersecurity Strategy 2018 – 2022, Law on Critical Infrastructure was drafted in 2022, amendments to the Energy Law addressing cybersecurity mechanisms in the energy sector are in preparation

Law on Information Security (2016), The Strategy for Development of Information Security for the period 2017 – 2020

Cybersecurity Strategy (2016), Cybersecurity Law (2017), Cybersecurity Requirements Resolution (2019), Critical Infrastructure Resolution (2020)

- Under more or less intensive cyber attacks since 2015 (attacks intensified after February 2024)
- Starting from this date enhanced cyber security measures are being implemented (the number of DDOS and other types of attacks has increased)

Topics and questions

- (How) does the war in Ukraine affect neighbouring countries? Have information sharing and collaboration changed due to the war?
  - ➢ Cooperation and coordination between EnC countries is still limited.
  - ➢ Common legislative framework needed (NCCS planned to be adapted and adopted).

- What are the lessons learnt from the Ukraine war that would help in the future to eliminate such energy crisis caused by external factors?
  - ➢ Awareness must be further increased / Risk preparedness plans must include detail elaboration on cyber-security.
  - ➢ Better organization is needed, activities should be coordinated between different entities.
  - ➢ Future wars will include a cyber-space and one of the main targets will be energy infrastructure (especially electricity).

Topics and questions

- What are the main cyberthreats emerging from the conflict and how is the energy community/industry building resilience to fight them?
  - Cyber attacks may seriously damage energy infrastructure and cause blackouts.
  - Electricity infrastructure has not been designed to be resilient to simultaneous outages.
  - Cyber-security measures will be one of the most important ways of protecting the power systems.

- What are the capabilities that you considered as a top priority for neighbouring countries that EU can support the development in the short term?

  - The National Cyber Authorities and regulatory agencies should develop and prescribe a requirements certification scheme for the energy sector stakeholders.

  - Contracting Parties should establish bilateral cooperation at the level of energy incident response teams and ISAC with neighbouring countries to address cascading risks.

  - For energy sector companies, it is of utmost importance for successful management of cybersecurity risks to completely and successfully complete the unbundling process and implement interconnections as well as integration of IT and operational technology systems according to modern cybersecurity standards and practice.

  - The system operators (both electricity and gas) should continue to implement the IS27000 framework in their own processes and establish continuous management of risks based on at least a yearly regular assessment.

- What are the challenges concerning energy related cybersecurity policy development and implementation in the neighboring countries (e.g. lessons learnt from NIS1)?

  - ✓ The legal and policy context is complex and fragmented.
  - ✓ Gaps in legislative requirements.
  - ✓ Cybersecurity is prioritised at the horizontal level without focused activities in the energy sector.
  - ✓ Energy security issues are often addressed only at the country level with a national focus only.
  - ✓ There is a need to create public-private partnerships when sharing information.

in partnership with

Thank you for your attention

Davor Bajs, PhD
Electricity Infrastructure Expert

Energy Community

Energy Community Secretariat
Am Hof 4, Level 5,
1010 Vienna, Austria

Phone +43 (0)1 535 2222-236
Mobile +43 (0)664 883 68 541
Email davor.bajs@energy-community.org
Web www.energy-community.org