E.DSO ENCS enisa entsoe in partnership with EE-ISAC

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

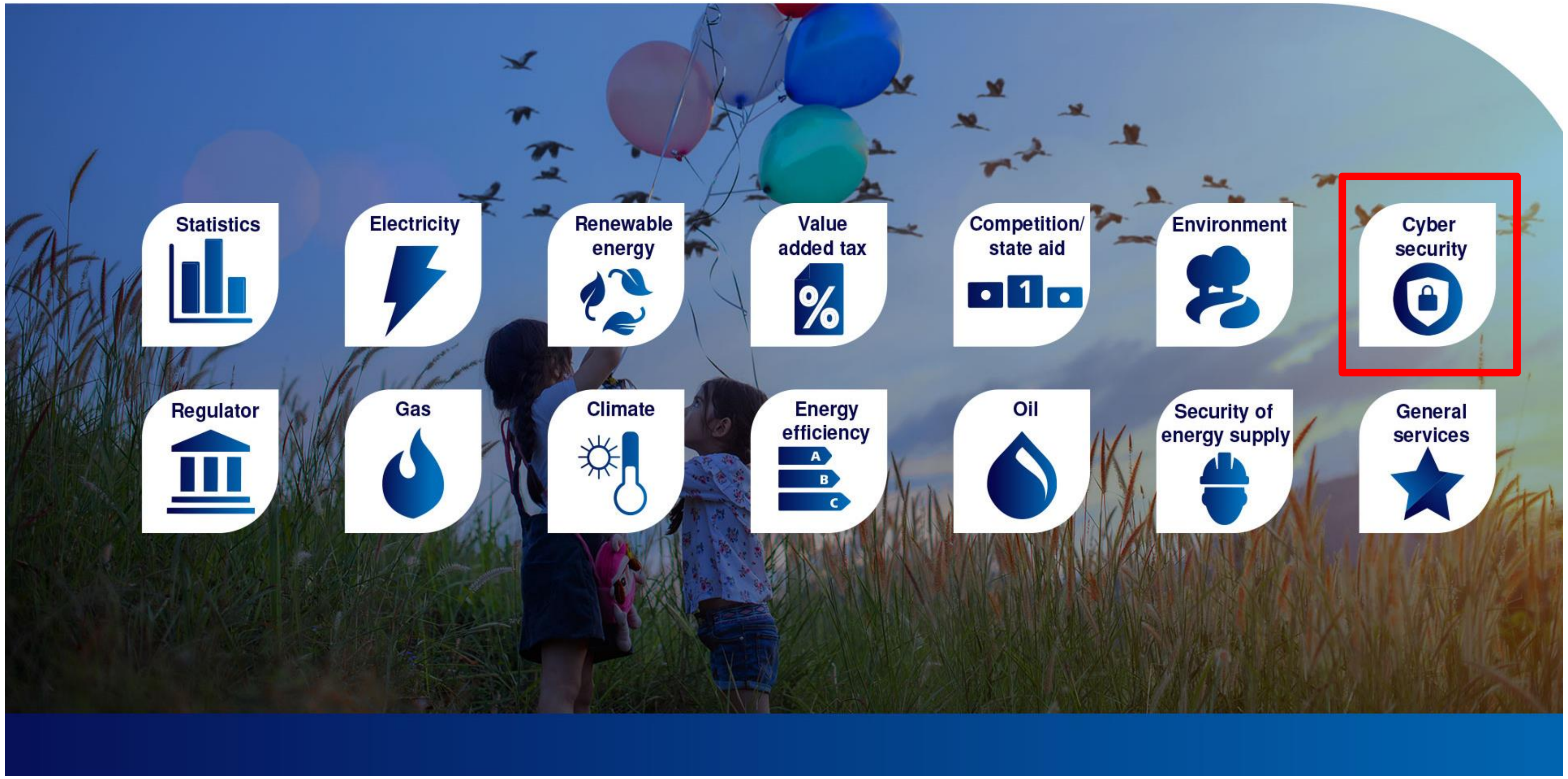
21 September 2023
10H00 to 16H00 EEST (09H00 to 15H00 CEST)

Session: Testimonial from Eastern Countries experience

Davor Bajs, Energy Community Secretariat

#CyberGrids23

Energy Community Secretariat



in partnership with

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

- **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

Contracting Parties of the EnC - ALBANIA

- Law on Cybersecurity (2017) partially transposes NIS1 but cross-border and regional cooperation missing
- The National Authority for Electronic Certification and Cyber Security (NAECCS) was established as a cybersecurity authority responsible for all sectors of the economy, including energy and it acts as:
  - national focal point,
  - cybersecurity regulator and
  - single Computer Security Incident Response Team
- All Critical Information Infrastructure (CII) operators are required to establish CSIRT teams and adopt minimum security measures (including OST, OSSH and KESH)
- Regulation on Cybersecurity of Critical Infrastructures in the Power Sector (2020)
- National Strategy for Cybersecurity (2020) aims to further align the national legal framework with EU directives and regulations
- Albanian electricity companies delivered self-assessments regarding cybersecurity, reviewed by the ERE
- New cybersecurity strategy is under preparation
- Huge cyber attacks last year, but not influencing the energy sector

Contracting Parties of the EnC - BiH

- No state law on cybersecurity or protection of critical infrastructure
- The Law of Republika Srpska on Information Security and the rulebooks on information security measures and standards lay down a set of broad obligations (but fail to transpose the NIS)
- The Law on Security of Critical Infrastructure adopted in 2019 transposes Directive 2008/114/EC on the identification and designation of European critical infrastructures in one entity (RS)
- Cybersecurity developments in Federation of Bosnia and Herzegovina are fragmentary and delayed
- There is no common CSIRT structure in Bosnia and Herzegovina
- The computer emergency response structure in Republika Srpska is CERT-RS (from 2015)
- Recently, the working group has been established on cybersecurity and works on the Roadmap for the security of network and information systems in the energy sector
- Information system of one energy company (Sarajevogas) was attacked and the lesson learnt is that better organisation is needed

Contracting Parties of the EnC - GEORGIA

- The Law on Information Security (2012/2021) partially transposes NIS Directive and the key provisions of Directive 2008/114/EC in the context of critical information and communication infrastructures
  - divides different entities and institutions in 3 categories of cybersecurity importance (2 for the public and 1 for the private sector)
  - critical infrastructure is determined and entities have been categorised
- No specific cybersecurity regulation regarding energy companies
- The main cybersecurity authority is the Digital Governance Agency (DGA) established in 2020, hosting the national CERT of Georgia (CERT-GOV-GE) acting as focal point for cybersecurity response
- The energy regulatory authority GNERC has no specific cybersecurity tasks or powers
- No cyber incidents in the energy sector recently (at least not reported to the Secretariat)

Contracting Parties of the EnC – KOSOVO*

- The Law on Critical Infrastructure of 2018 transposes Directive 2008/114/EC in detail
- The main focal point and coordinator in critical infrastructure protection is the Ministry of Interior
- The National Cybersecurity Strategy of Kosovo* 2016 – 2019 roughly outlines the responsible parties and objectives in cybersecurity management, threat assessment, protection of critical information infrastructure, building institutional capacity for incident response
- The Kosovar Regulator has drafted CyS strategy for the energy sector 2023 – 2027
- The Law on security of networks and information systems was adopted in February this year, appointing the Ministry of Economy as the leading institution regarding this law and implementing NIS directive
- The Regulatory Authority for Electronic and Postal Communications (ARKEP) hosts the national KOS-CERT, acting as the main computer emergency response unit, providing support, notification and exchange of information related to cyber events, also covering the energy sector
- There were no attacks in the electricity networks

Contracting Parties of the EnC – MOLDOVA

- The Cybersecurity Programme 2016 – 2020 is the basic policy act addressing provisions of NIS Directive
- The Information Technology and Cybersecurity Service (STISC) is the national competent authority responsible for developing information and communication infrastructure of the public administration and implementing cybersecurity policies
- National CERT (CERT-GOV-MD) acts as a contact point for reporting, coordinating and assisting in the response to incidents and providing cybersecurity services to the public administration including the energy sector
- The energy regulator ANRE is authorised to approve the expenses for anti-terrorism protection in the energy sector. However, the current legislation fails to grant the regulator competences over specific aspects of cybersecurity
- Law on CyS was approved this year
- Cybersecurity agency will be established
- Moldelectrica and Energopro has been supported in the cybersecurity issues by the USAID

Contracting Parties of the EnC – MONTENEGRO

- Cybersecurity Strategy 2018 - 2021 defines objectives in the cybersecurity domain, including boosting incident response capacity, protection of critical information infrastructure and public awareness
- The Law on Information Security (2010/16/20/21) partially transposes NIS Directive
- CIRT-ME is established as a unit within the National Security Authority and provides cybersecurity services and coordinates assistance in case of cybersecurity incidents
- The Law on Designation and Protection of Critical Infrastructure (2019) transposes Directive 2008/114/EC
- The Law on Critical Infrastructure defines a general set of criteria related to the development of security plans and appointment of security coordinators and outlines the basic obligations for the operators of critical infrastructures
- Draft Law on Information Security from 2023 is in line with the NIS2 Directive (2022/2555)
- Cybersecurity Strategy 2022-2026, the leading institution is the Ministry of Interior
- Regulatory energy and water supply authority does not have legislative obligations to deal with CyS
- Draft Law on Information Security envisages the establishment of the Cyber Security Agency
- State infrastructure (not energy) was exposed to coordinated cyber attack in August 2022

Contracting Parties of the EnC – N.MACEDONIA

- The Cybersecurity Strategy 2018 – 2022 aims to provide resilient information and communication technology (ICT) infrastructures, and boost cybersecurity capacity and culture, cyber defence, international cooperation and exchange of information
- Law on Critical Infrastructure was drafted in 2022
- Based on the Law on Electronic Communications, the responsible authority is the Agency for Electronic Communications, hosting the MKD-CIRT
- Amendments to the Energy Law addressing cybersecurity mechanisms in the energy sector, enforcing identification and designation of critical energy infrastructures and providing cybersecurity competences to the energy regulatory authority, are in preparation
- The establishment of a specific energy CIRT is foreseen in a draft Cybersecurity Law
- The Energy Regulatory Commission (ERC) has adopted Recommendations including criteria for identification of critical energy infrastructures in the electricity sector in cooperation with MKD-CIRT and the Ministry of Economy

in partnership with

Contracting Parties of the EnC – SERBIA

- Law on Information Security (2016) sets the concept of information and communication (ICT) systems of special importance including the energy sector and it gives the comprehensive overall legal and institutional framework for cybersecurity
- The Strategy for Development of Information Security for the period 2017 – 2020 is linked to the implementation of Directive 2016/1148/EC (NIS Directive), introducing the principles and defining the objectives in security of the ICT systems of special importance, as well as fights against cybercrime
- Risk assessment is defined in the Law on Information Security and in the Regulation on More Detailed Contents of Enhancement on Security of ICT of Special Significance, performed by the national computer emergency response team (SRB-CERT)
- Starting in 2019, inspection and supervision of information and communications technologies (ICT) has been performed on an annual basis by the Department for Information Security and Electronic Business within the Sector of Information Society and Information Security of the Ministry of Trade, Tourism and Telecommunications
- Inspection and supervision were carried out for energy companies (TSO e&g, DSO, GEN company)

Contracting Parties of the EnC – UKRAINE

- 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)
- Basic principles to ensure cybersecurity were proposed by Ukrainians as follows:
    - One server is for one service
    - Using of blocking non-standard activity (firewall) on the server
    - Responds only to the ports necessary for the operation
    - Monitoring and updating of software servers
    - Monitoring of the activity of mail servers, detecting and blocking of spam
    - Constant monitoring of activity and loading of external communication channels
    - Logging in
    - Web server traffic encryption, TLS protection
    - Single access point for administration
    - Control of external user access, stable VPN access encryption (L2TP + Ipsec)
    - Users access only to the data necessary to perform work
    - Updating of PC software and antivirus protection

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 (for example NCCS).

- 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. Cyber-security should be organized by coordinating activities 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?

  Malware like INDUSTROYER 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. Basic principles should be organized with respect to:

  - prevention,
  - protection,
  - mitigation,
  - response and
  - recovery.

- 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, together with 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. There is a lack of provisions related to critical infrastructure and essential services identification in Contracting Parties and consequently gaps in legislative requirements related to operator security plans and communication and reporting mechanisms.

All Contracting Parties have prioritized cybersecurity at the national level and are in the process of developing support measures. However, this is often being done at the horizontal level without focused activities in the energy sector.

Contracting Parties have specific and different levels of risks largely depending on their respective geopolitical situations. Energy security issues are often addressed only at the country level, maintaining for example a national focus only, without considering the complexity of the interdependence of EnC CPs and EU member states in multiple aspects of the energy area, including cybersecurity.

There is a need to create public-private partnerships when sharing information. Under existing legislation, cybersecurity requirements differ between the public and private stakeholders identified.

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