Energy Community

THE ENERGY COMMUNITY

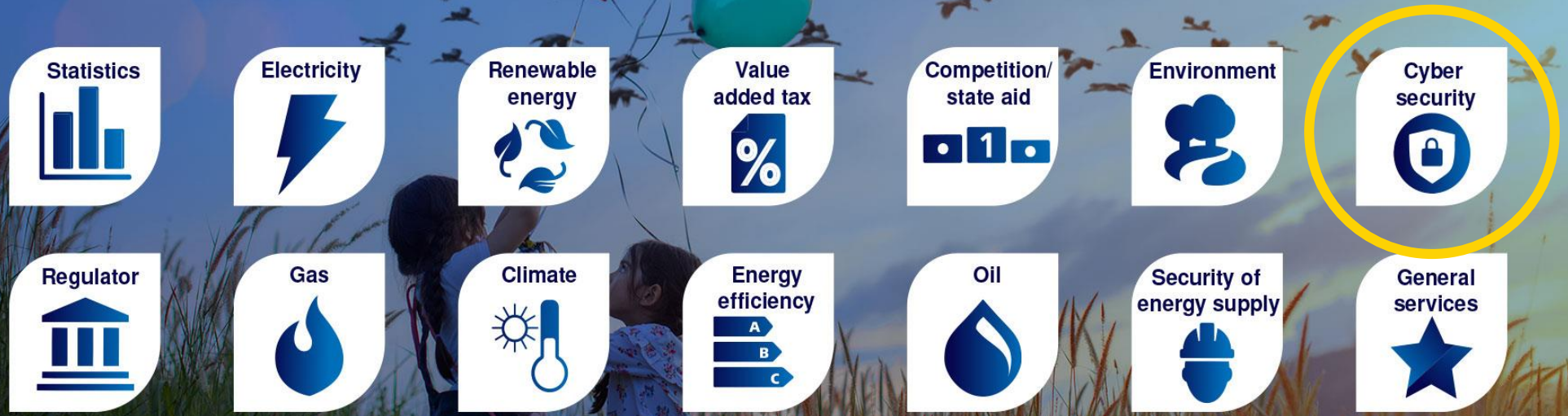
Cybersecurity in the GAS sector

15th Security of Supply Coordination Group – GAS Subgroup

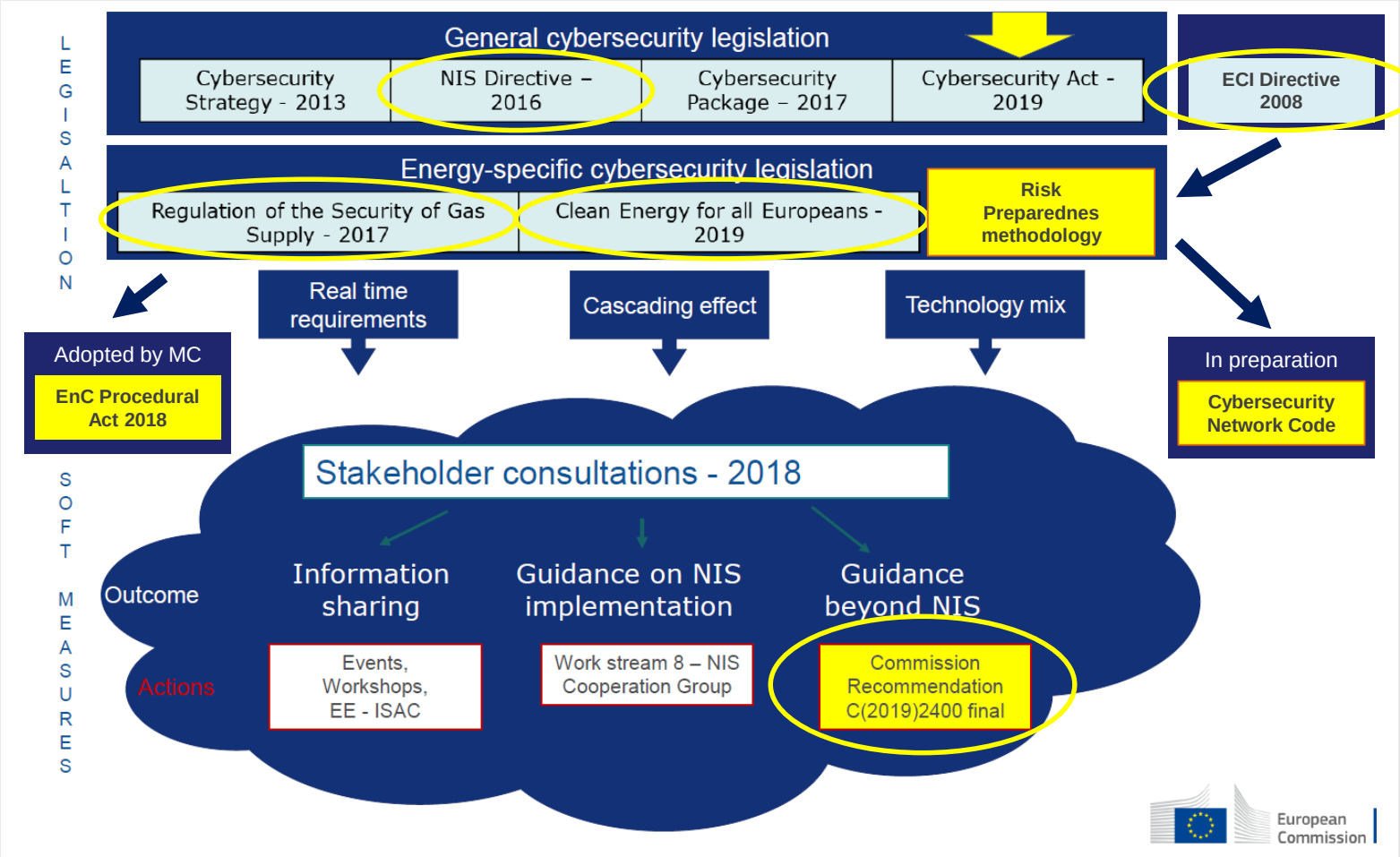
21 October 2020 – Part 4: Cybersecurity in the Energy Community

Energy Community

MAIN AREAS OF WORK



Cybersecurity – EU legislation



Cybersecurity – technical standards

ISO/IEC 27000

- Information technology security Techniques - 49 items

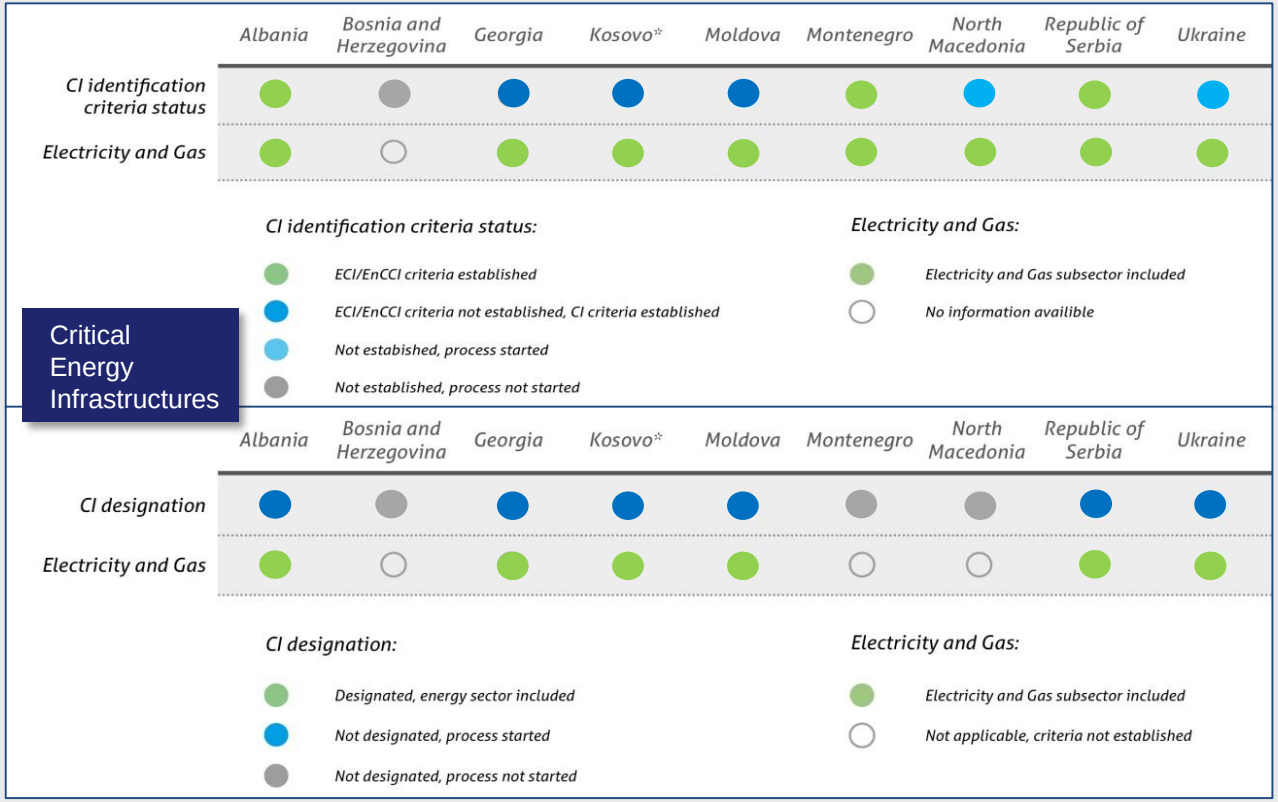
Other security standards:

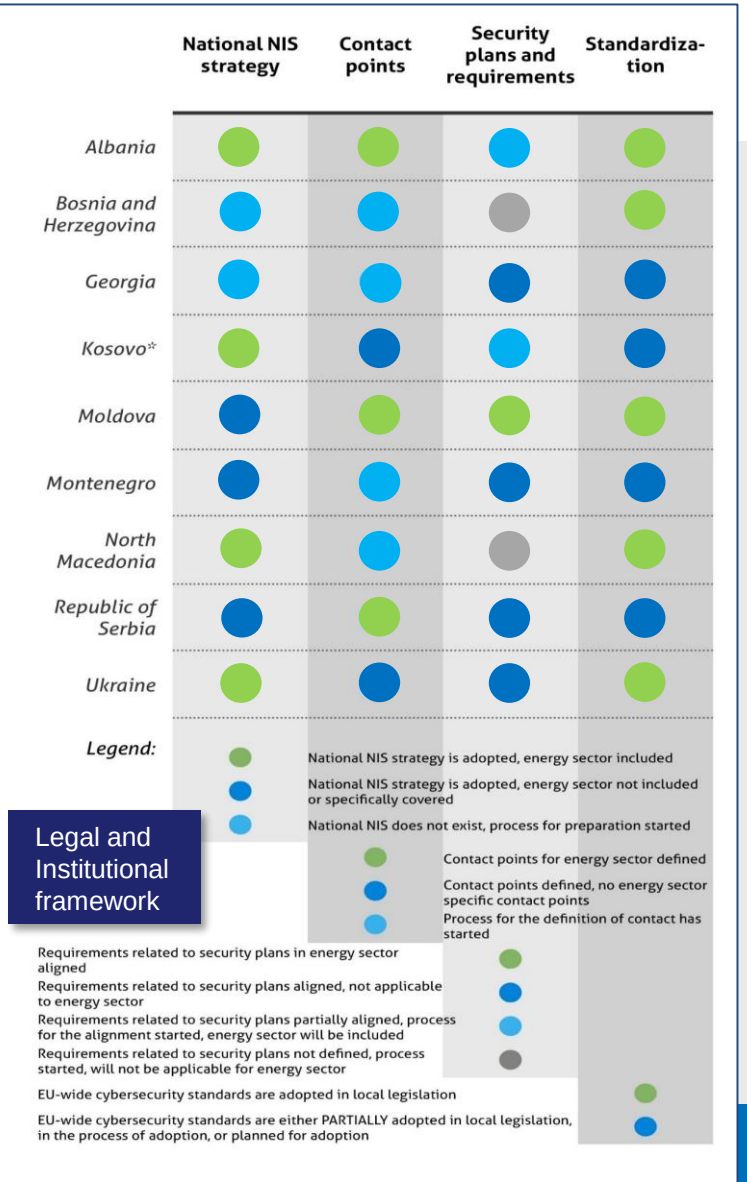
- ITU - International Telecommunications Union
- ANSI - American National Standards Institute (USA)
- NIST – National Institute of Standards and Technology (USA)

- Information Security Management Systems (ISMS)
  - ISO/IEC 27000:2018 - Overview and vocabulary
  - ISO/IEC 27001:2013 - Requirements
  - ISO/IEC 27002:2013 - Code of practice for information security controls
  - ISO/IEC 27005:2018 - Information security risk management
  - ISO/IEC 27019:2017 - Information security controls for the energy industry
- Other relevant ISO/IEC standards
  - ISO/IEC 15408-1:2009 - Evaluation criteria for IT security
  - ISO/IEC 15408-2:2009 - Security functional components
  - ISO/IEC 15408-3:2009 - Security assurance components
  - ISO/IEC 18045:2008 - Methodology for IT security evaluation
  - ISO/IEC TR 19791:2010 - Security assessment of operational systems
  - ISO/IEC 30111:2019 - Vulnerability handling processes

EnC Cybersecurity Status (2020)

Energy Community – gap analysis





Cybersecurity – Directive on European critical infrastructure (ECI) December 2008

- ECI sectors: energy (Electricity, Gas, Oil), and transport
- Identification of ECI – coordinated criteria
  - Criteria - sectoral, cross-cutting, trans-boundary
  - Thresholds - severity of impact
- Designation of ECI (bilateral / regional)
  - Potential / suspected ECI, level of impact, discussions, reporting (EC), informing the operator, discretion principles
- Operator Security Plan
  - Identification of assets / threat scenarios – risk analysis / vulnerability and potential impact / security measures
  - Periodic review, supervision, community measures and compliance with agreed criteria
- Security Liaison Officers – communication mechanisms
- Threat assessment – reporting, common methodologies, classified information

- An asset, system or part thereof which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people and the disruption or destruction of which would have significant impact in a MS as a result of the failure to maintain those functions

- significant impact on at least two MSs (CPs)

Cybersecurity – Directive on Network and Information Systems (NIS) July 2016

- Build sufficient resilience capacity at national level
  - Adopt a national NIS strategy
  - Designate national cybersecurity authorities, single contact points and Computer Security Incident Response Teams (CSIRTs)
- Identify critical infrastructure, operators of essential services (OES), and relevant digital service providers
- Build structures for cross-border cooperation and exchange of information
  - At strategic level - creating a Cooperation Group of national authorities
  - At operational level - creating a network of national CSIRTs
- Cumulative conditions for identification of OES
  - Service essential for societal / economic activities, depends on network and information systems, an incident would have significant disruptive effects
- Security and notification requirements imposed on OES
- Monitoring and enforcement powers

a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;

b) the provision of that service depends on network and information systems; and

c) an incident would have significant disruptive effects on the provision of that service.

Cybersecurity – EC Recommendations on Cybersecurity in energy

- EC Recommendation C(2019)2400,
- Staff Working Paper SWD(2019)1240 :

- **Real-time requirements (IT and OT)** - some energy systems need to react so fast that standard security measures such as authentication of a command or verification of a digital signature can simply not be introduced due to the delay these measures impose.

- **Cascading effects** - electricity grids and gas pipelines are strongly interconnected across Europe and well beyond the EU. An outage in one country might trigger blackouts or shortages of supply in other areas and countries.

- **Combined legacy systems with new technologies** - many elements of the energy system were designed and built well before cybersecurity considerations came into play. This legacy now needs to interact with the most recent state-of-the-art equipment for automation and control, such as smart meters or connected appliances, and devices from the Internet of Things without being exposed to cyber-threats.

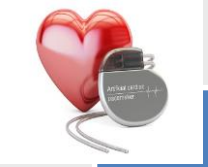
Cybersecurity – EC Recommendations on Cybersecurity in energy

Real-time Requirements

- Use international standards
- Apply physical measures
- Classify / manage your assets
- Consider privately owned communication networks, or consider specific measures
- Consider splitting systems into logical zones
- Choose secure communication and authentication

Cascading effects

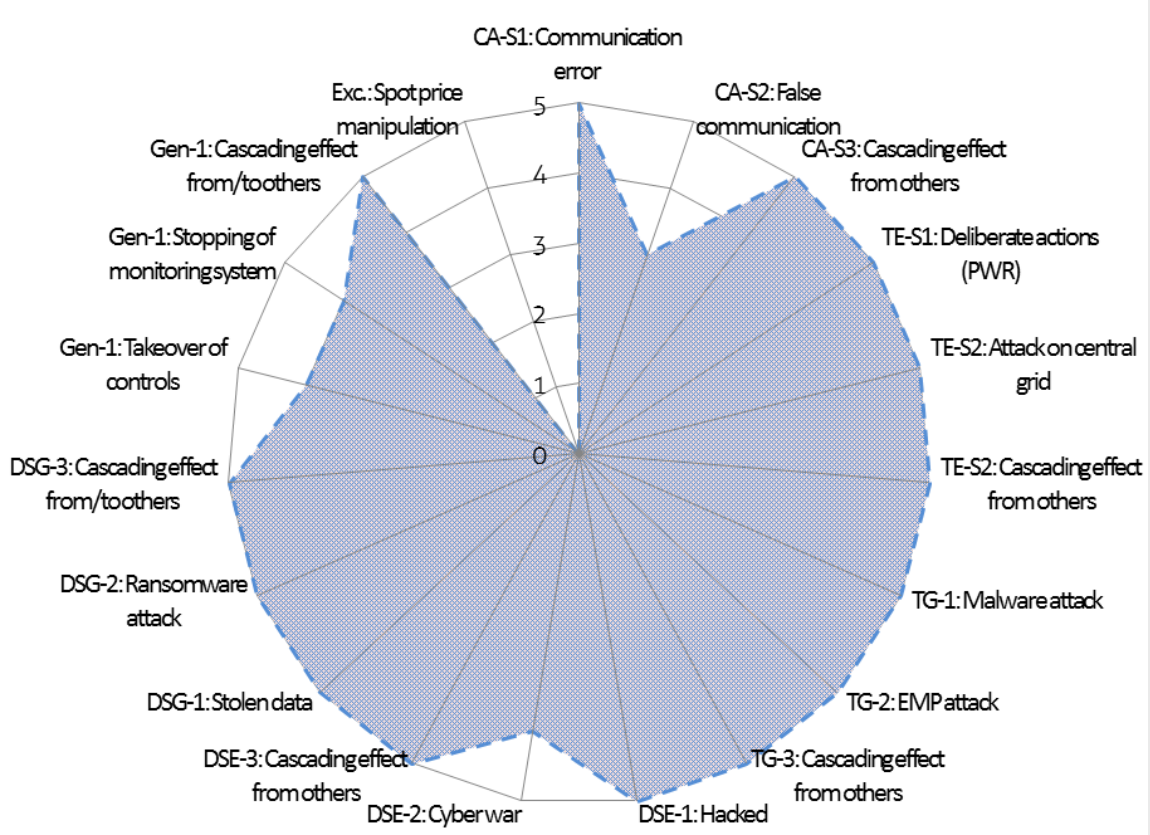
- Evaluate interdependencies
- Ensure communication framework for early warnings and to cooperate in crisis
- Ensure level of security for new devices
- Consider cyber - physical spill overs
- Establish design criteria for a resilient grid



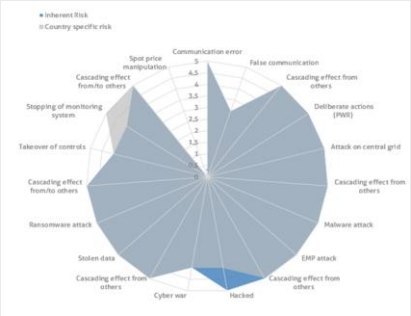
Technology mix

- Follow a cybersecurity-oriented approach when connecting devices
- Use international standards
- Establish monitoring and analysis capabilities
- Conduct specific cybersecurity risk analysis for legacy installations
- Collaborate with technology providers
- Update hardware and software

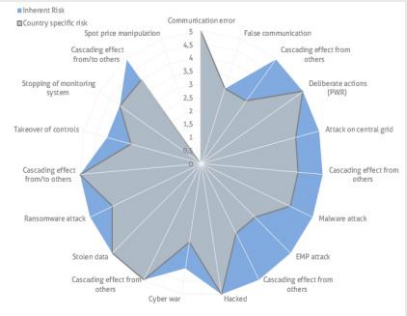
Energy Community Cybersecurity Study – inherent risk pattern



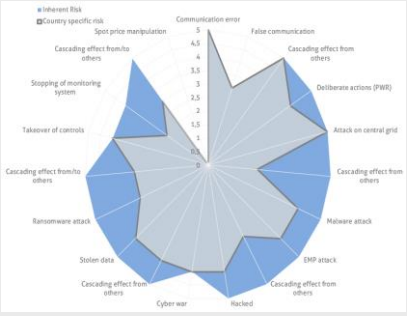
Energy Community Cybersecurity Study – inherent risk assessment



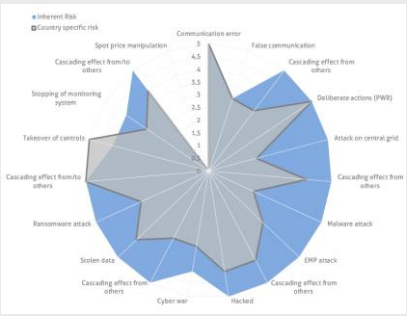
Albania



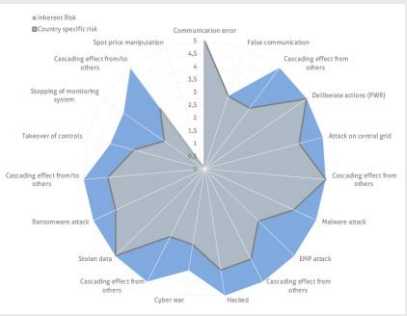
Bosnia and Herzegovina



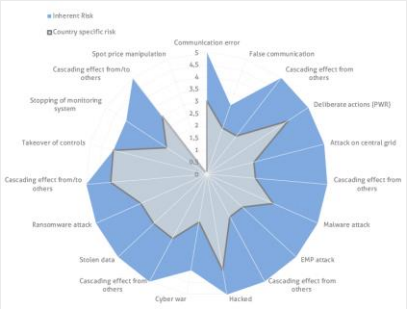
Georgia



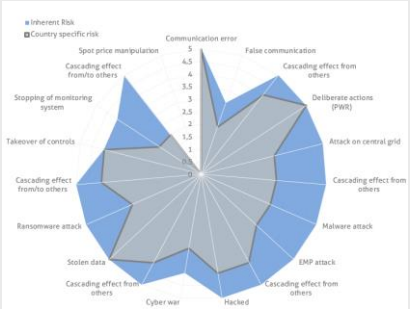
Kosovo*



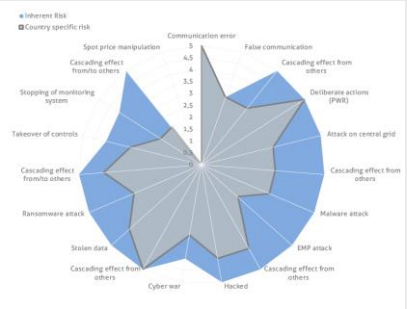
Moldova



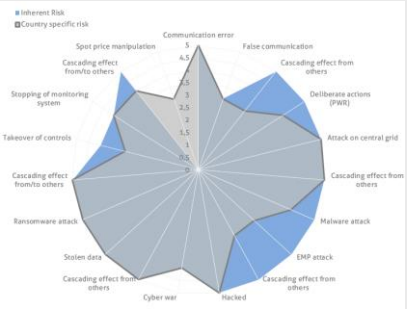
Montenegro



North Macedonia



Serbia



Ukraine

General recommendations for Ministries

- Start as soon as possible with the implementation of the legal framework and provide sufficient budgetary resources during implementing laws, legal documents and strategies.
- Organize a sector specific CSIRT (or allocate sufficient resources in existing CSIRT infrastructure to address energy- specific incidents in real time)
- Establish an online communication channel to enable reporting and feedback line with all members of the energy sector.
- Establish a system for early warning and exchange of information on cyber threats / provision of assistance in energy.
- Conduct a standardized, overall sector specific risk assessment for the country based on the collected relevant information about assets, vulnerabilities and threats (including cascading, cross sectorial and cross-border risks).
- Ensure that newly discovered risks are managed through enforcing TSOs and DSOs in implementing action plans and controlling the management process.
- If appropriate, for the smaller DSOs, generators or new type of market participants the organize a national ISAC as a source of information, analysis and remediation solutions.

General recommendations for NRA / Liaison officers

- The cybersecurity Liaison officer must have a complete understanding of local energy stakeholders, market, critical infrastructure protection and their capability to handle the most complex issues in information and cybersecurity. They would serve as a focal point between EnC CyberCG / NRA Working stream and local operational entities
- NRAs should serve as a central monitoring hub in controlling the exchange of critical infrastructure protection and cybersecurity related information.
- The capability to be supported by NRA own employees which must have international certifications in the field of information and/or cyber security (CISA, CISM, CISSP, ISO27LA).
- The local NRAs must have the capability to master the EU Critical Infrastructure Protection and NIS directive related issues and also have power to enforce changes in local energy sector regulation regarding the same.
- The local NRAs must have power to supervise by controls and/or audit the NRA licensed companies for cyber security issues in order to enforce the managing of risks on required level.

Establishment

Administrative & legal format

- An international association under the Austrian law – ToR, roadmap (ECS)
- Legal acts (AA), local legislation, enforcement, penalties
- Financing

Membership

- Members – criteria for participation, scope, restrictions
- Partners

Meetings and events

- Representatives
- Chairperson, Board
- Working groups, projects
- Role of the ECS
- Common projects (Working groups) on mutual domains of interest

Operation

Information sharing

- Classification and restricted access (WHITE / GREEN / AMBER / RED)
- Confidentiality memorandum (statement) – obligation for non-disclosure
- Publication (transparency) – regulated and coordinated

Mutual assistance and activities

- Exchange / analysis of sensitive information – direct added value, trusted environment
- Sharing human capacity / cooperation within the CSERT community
- Coordinated standards / best practices
- Partnership relations - ISACs in other regions / sectors, EU associations / authorities, public sector
- Common projects (Working groups) - mutual domains of interest
- Publications, external events

Training

- Forensic training sessions, education on risk assessment and remedies
- Specific case analysis, security plans and training exercises

Activities & Sharing Topics

Physical Info Sharing Community

- Plenary meetings
- Community meetings
- Theme based meetings
- Open house meetings

Digital Info Sharing Community

- Information requests / push
- Webinars
- Whitepaper

Topics of Information Sharing

- Vulnerabilities in OT systems and critical assets
- Threat/Risk analysis information
- Incidents
- Lessons learned / best practices
- Alerts and (patch)notifications
- Use of standards (ISO, IEC, NIST, NERC etc.)
- Research (H2020) topics

EE-ISAC

THANK YOU for your kind attention

simon.uzunov@energy.community.org

www.energy-community.org

Ener_Community

/company/energy-community

/Ener.Community

/EnergyCommunityTV