THE ENERGY COMMUNITY

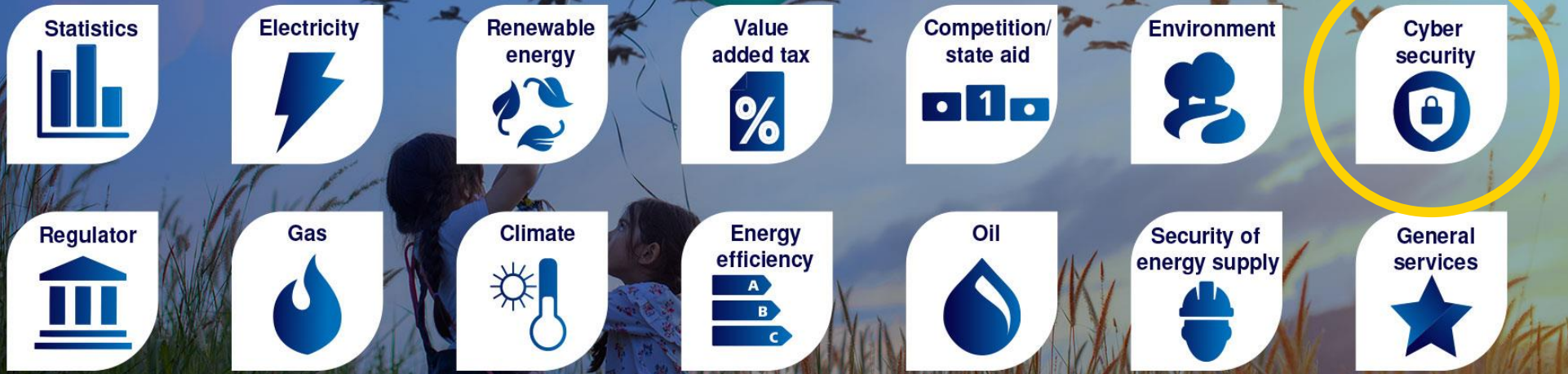
cybersecurity framework for critical energy infrastructures: recommendations for Ukraine

MINISTRY OF ENERGY of UKRAINE

Energy Sector Working Group – Subgroup on Cybersecurity: 1st Meeting, 11-08-2020

Energy Community

MAIN AREAS OF WORK



Cybersecurity – EU legislation relevant to the energy sector

Energy Community

- **PA 2018/02/MC-EnC** (November 2018) on the establishment of Energy Community Coordination Group for Cybersecurity and Critical Infrastructure **(CyberCG)**

Existing EU Legislation

- **ECI** Directive (2008 / 114) on European critical infrastructures
- **NIS** Directive (2016 / 1148) on security of network and information systems
- **EC Recommendation** (2019 / 2400 – April 2019) on cybersecurity in energy
- EU Regulation (2019 / 881) on ENISA technology certification (Cybersecurity act)
- Risk Preparedness Regulation (2019 / 943)

Next generation of cybersecurity acts

- Network Code on Cybersecurity

Cybersecurity – Directive on European critical infrastructure (ECI)

- 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)

- 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

Clean Energy Package - Risk Preparedness Regulation

ENTSO-e Methodology for identification of regional electricity crisis scenarios

https://consultations.entsoe.eu/system-operations/risk-preparedness-regulation-methodology-for-ident/supporting_documents/Methodology%20for%20Identification%20of%20Regional%20Electricity%20Crisis%20Scenarios.pdf

TSO
ENTSO-E
all

Article 7 Identify national electricity crisis scenarios → **Article 8** Identify regional electricity crisis scenarios → **Article 9** Evaluate regional scenarios at a national level → **Article 10** Rank regional scenarios by impact → **Article 11** Presentation of scenarios

Article 13 Handling of sensitive information

Article 12 Review

Classification	Events per year	1 x in … years	Description/example of initiating event
Very likely	≥ 0.5	2 or less	event expected practically every year, e.g. extreme winds/storms causing multiple failures of overhead lines may be expected nearly every year in some areas
Likely	0.2-0.5	2-5	event expected once in a couple of years, e.g. extreme heat wave causing limits on output of open-loop water-cooled power plants, low water levels at hydro plants, higher load, etc.
Possible	0.1-0.2	5-10	event expected or taken into consideration as a potential threat, e.g. cyber or malicious attack
Unlikely	0.01-0.1	10-100	very rare event with potentially huge impact, e.g. simultaneous floods causing unavailability of generation, distribution and transmission infrastructure
Very unlikely	≤ 0.01	100 or more	event not observed but potentially disastrous, e.g. earthquake causing a huge destruction of transmission, distribution and generation infrastructure

Classification	EENS%* (of annual demand)	LOLE* [hours]
Disastrous	≥0,25%	≥168
Critical	≥0,05% and <0,025%	≥48 and <168
Major	≥0,01% and <0,05%	≥12 and <48
Minor	≥0,002% and <0,01%	≥3 and <12
Insignificant	<0,002%	<3

Impact		Likelihood				
EENS%	LOLE	Very likely	Likely	Possible	Unlikely	Very unlikely
Disastrous	Disastrous	Disastrous	Disastrous	Critical	Major	Minor
Disastrous	Critical	Disastrous	Critical	Critical	Major	Minor
Critical	Disastrous	Disastrous	Critical	Critical	Major	Minor
Disastrous	Major	Disastrous	Critical	Major	Major	Minor
Major	Disastrous	Disastrous	Critical	Major	Major	Minor
Disastrous	Minor	Disastrous	Critical	Major	Major	Minor
Minor	Disastrous	Disastrous	Critical	Major	Major	Minor
Disastrous	Insignificant	Disastrous	Critical	Major	Major	Minor
Insignificant	Disastrous	Disastrous	Critical	Major	Major	Minor
Critical	Critical	Disastrous	Critical	Major	Minor	Minor
Critical	Major	Critical	Critical	Major	Minor	Minor
Major	Critical	Critical	Critical	Major	Minor	Minor
Critical	Minor	Critical	Major	Major	Minor	Minor
Minor	Critical	Critical	Major	Major	Minor	Minor
Critical	Insignificant	Critical	Major	Major	Minor	Minor
Insignificant	Critical	Critical	Major	Major	Minor	Minor
Major	Major	Critical	Major	Major	Minor	Insignificant
Major	Minor	Major	Major	Minor	Minor	Insignificant
Minor	Major	Major	Major	Minor	Minor	Insignificant
Major	Insignificant	Major	Major	Minor	Minor	Insignificant
Insignificant	Major	Major	Major	Minor	Minor	Insignificant
Minor	Minor	Major	Minor	Minor	Insignificant	Insignificant
Minor	Insignificant	Major	Minor	Minor	Insignificant	Insignificant
Insignificant	Minor	Major	Minor	Minor	Insignificant	Insignificant
Insignificant	Insignificant	Minor	Minor	Insignificant	Insignificant	Insignificant

ENTSO-E Criteria on Cyber Risk Mitigation

Challenges I : Regulation

Obstacles for effective trans-national cooperation

- **Country-level** regulations may forbid sharing of information
- Problems between **EU** and **NON-EU** members

Challenges II : Organization

Fragmentations in network architecture

- **Complexity** of the ENTSO-E power system
- Connection of facilities (generators, loads) with extreme **diversity** in size and technology
- Large **stakeholder setup** – entanglement between large operators (TSO, RSC, DSO)

Policy:

inter-TSO and - RSC cybersecurity measures

- **Security** – prevention control and compliance with standards
- **Resilience** – incident monitoring, detection, response and recovery

Energy Community Cybersecurity Study – gap analysis

https://www.energy-community.org/dam/jcr:db8e479d-b423-40c9-9ff9-998c7d9045ef/Blueprint_cyber_122019.pdf

Critical Energy Infrastructures

	Albania	Bosnia and Herzegovina	Georgia	Kosovo*	Moldova	Montenegro	North Macedonia	Republic of Serbia	Ukraine
CI identification criteria status	●	●	●	●	●	●	●	●	●
Electricity and Gas	○	○	○	●	●	○	○	●	●

CI identification criteria status:

- ECI/EnCCI criteria established
- ECI/EnCCI criteria not established, CI criteria established
- Not estabished, process started
- Not established, process not started

Electricity and Gas:

- Electricity and Gas subsector included
- No information availible

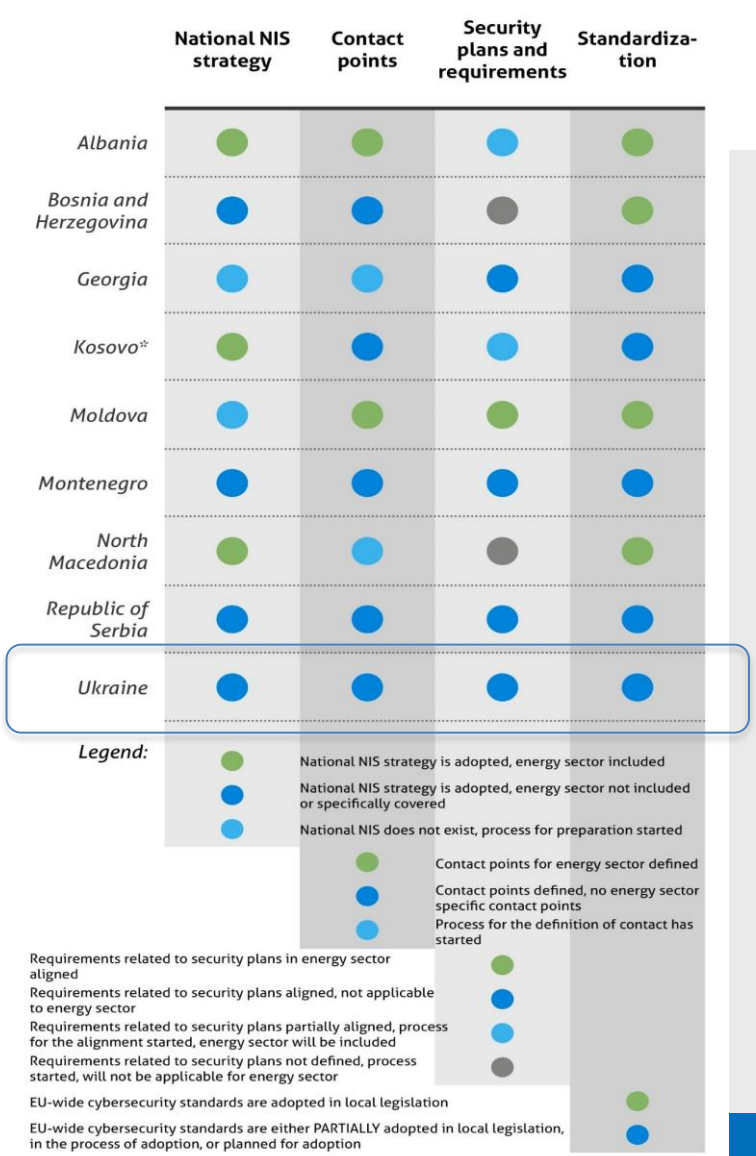
	Albania	Bosnia and Herzegovina	Georgia	Kosovo*	Moldova	Montenegro	North Macedonia	Republic of Serbia	Ukraine
CI designation	●	●	●	●	●	●	●	●	●
Electricity and Gas	○	○	○	●	●	○	○	●	●

CI designation:

- Designated, energy sector included
- Not designated, process started
- Not designated, process not started

Electricity and Gas:

- Electricity and Gas subsector included
- Not applicable, criteria not established



Energy Community Cybersecurity Study – overall risk assessment

https://www.energy-community.org/dam/jcr:db8e479d-b423-40c9-9ff9-998c7d9045ef/Blueprint_cyber_122019.pdf

- Prioritisation in terms of likelihood and impact
- Distribution according to type of stakeholder

	Cyber Threat							
	Malware	Web Based Attacks/Web application attacks	Social engeneering/Phising/ Spam	Denial of Service (DoS)	Insider Threat	Cyber Espionage Cyberwarfare	Ransomware	Botnet
	MEDIUM RISK for CA/NRA	NOT APPLICABLE for CA NRA	HIGH RISK for CA/NRA	HIGH RISK for CA/NRA	HIGH RISK for CA/NRA	CRITICAL RISK for CA/NRA	MEDIUM RISK for CA/NRA	MEDIUM RISK for CA/NRA
	LOW RISK in cascading effect to other energy stakeholder		MEDIUM RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	HIGH RISK in cascading effect to other energy stakeholder	HIGH RISK in cascading effect to other energy stakeholder	MEDIUM RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder
	HIGH RISK for TSO	MEDIUM RISK for TSO	HIGH RISK for TSO	LOW RISK for TSO	HIGH RISK for TSO	HIGH RISK for TSO	HIGH RISK for TSO	HIGH RISK for TSO
	MEDIUM RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	HIGH RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	HIGH RISK in cascading effect to other energy stakeholder	HIGH RISK in cascading effect to other energy stakeholder	HIGH RISK in cascading effect to other energy stakeholder	HIGH RISK in cascading effect to other energy stakeholder
	MEDIUM RISK for DSO	MEDIUM RISK for DSO	HIGH RISK for DSO	LOW RISK for DSO	MEDIUM RISK for DSO	HIGH RISK for DSO	HIGH RISK for DSO	HIGH RISK for DSO
	MEDIUM RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	MEDIUM RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	MEDIUM RISK in cascading effect to other energy stakeholder	HIGH RISK in cascading effect to other energy stakeholder	MEDIUM RISK in cascading effect to other energy stakeholder
	LOW RISK for Generation	LOW RISK for Generation	MEDIUM RISK for Generation	LOW RISK for Generation	MEDIUM RISK for Generation	MEDIUM RISK for Generation	HIGH RISK for Generation	MEDIUM RISK for Generation
	MEDIUM RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	MEDIUM RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	MEDIUM RISK in cascading effect to other energy stakeholder	MEDIUM RISK in cascading effect to other energy stakeholder	MEDIUM RISK in cascading effect to other energy stakeholder
	LOW RISK for Exchange	LOW RISK for Exchange	LOW RISK for Exchange	LOW RISK for Exchange	LOW RISK for Exchange	LOW RISK for Exchange	MEDIUM RISK for Exchange	LOW RISK for Exchange
	LOW RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder

Energy Community Cybersecurity Study – stakeholder-specific risk assessment

https://www.energy-community.org/dam/jcr:db8e479d-b423-40c9-9ff9-998c7d9045ef/Blueprint_cyber_122019.pdf

- Lack of regulatory framework (missing critical infrastructure / essential services regulation)

NRA/CA

- Missing interoperability with other organisations, a cascading effect high risk (Insider Threat, Cyberwarfare)
- Inability to provide sufficient expertise in case of an incident, a cascading effect critical risk (DoS, Social engineering)

TSO

- Infection of OT systems (SCADA) and legacy systems through IT network (Malware, Ransomware, Botnet)
- Sabotage on OT, a cascading effect high risk (Insider Threat, Cyberwarfare, Ransomware, Botnet)
- Inability to react in a case of an incident, a cascading effect high risk (DoS, Social engineering, Phishing, Spam, Ransomware)

DSO

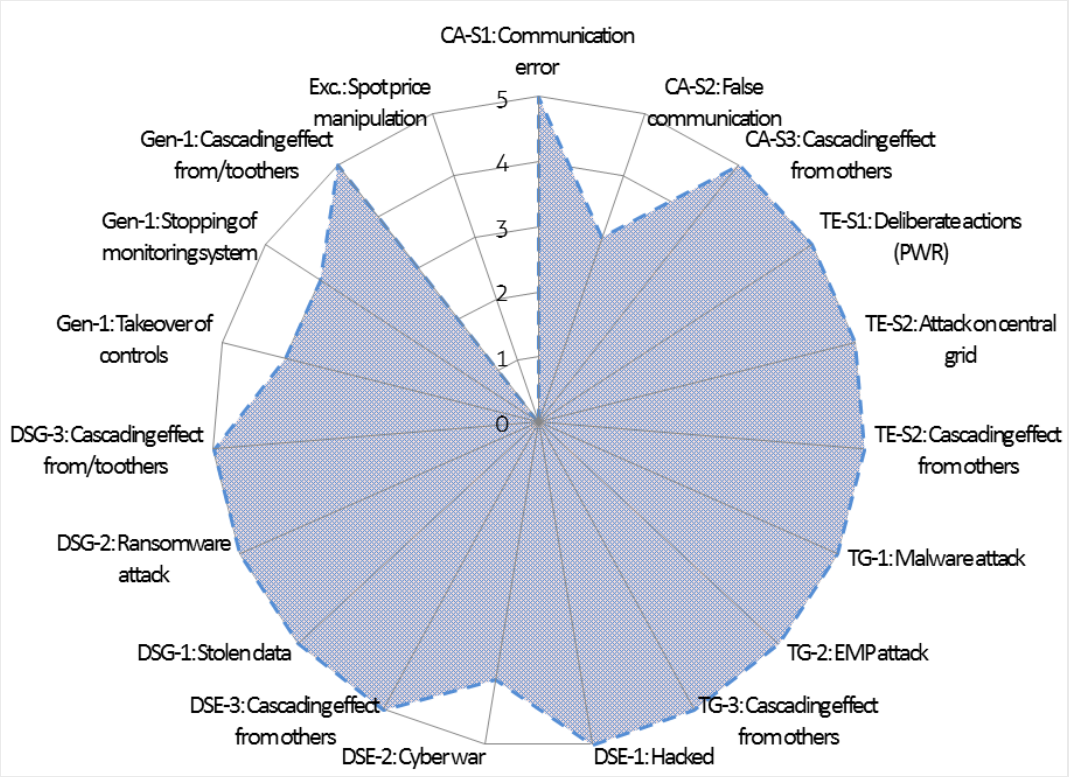
- Sabotage on OT, a cascading effect high risk (Ransomware)
- Inability to react in a case of an incident (Social engineering, Phishing, Spam, Ransomware)

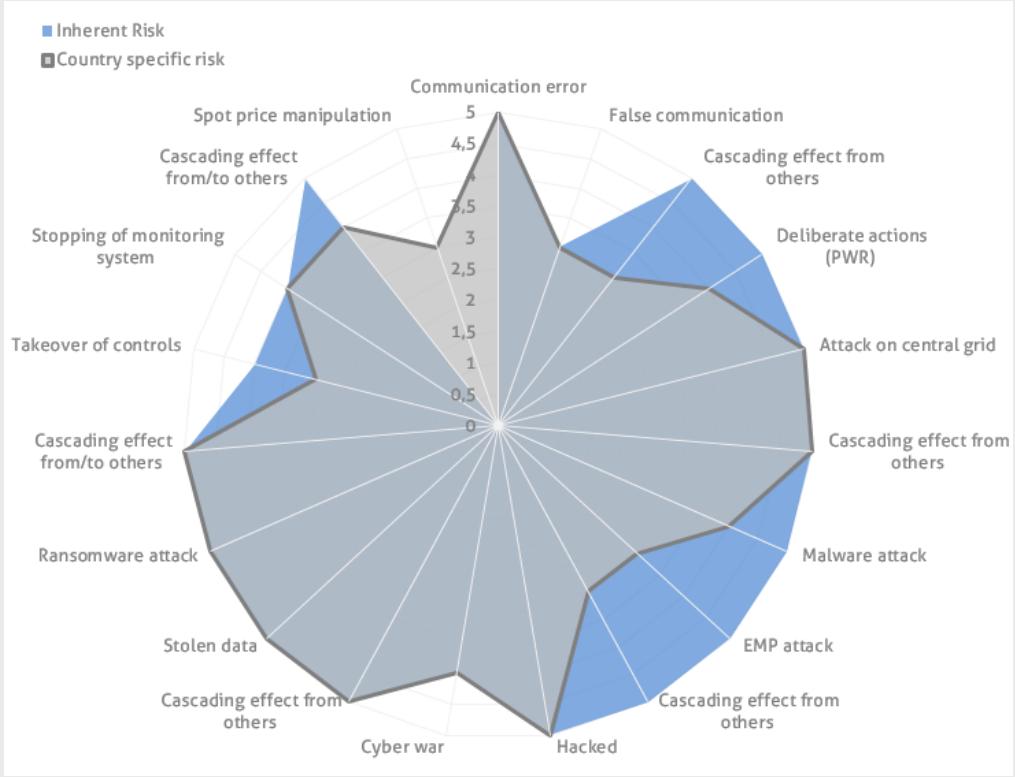
Power generation

- Infection of OT systems (SCADA) and legacy systems through IT network (Malware, Ransomware, Botnet)

Energy Community Cybersecurity Study – inherent risk pattern

https://www.energy-community.org/dam/jcr:db8e479d-b423-40c9-9ff9-998c7d9045ef/Blueprint_cyber_122019.pdf





Energy Community Cybersecurity Study – general recommendations for Competent Authorities

https://www.energy-community.org/dam/jcr:db8e479d-b423-40c9-9ff9-998c7d9045ef/Blueprint_cyber_122019.pdf

- The CA (Competent Authorities), the NRA, and the responsible Ministries start as soon as possible with the implementation of the legal framework and to provide sufficient budgetary resources during implementing laws, legal documents and strategies.

- The CA organizes a sector specific CSIRT (or allocate sufficient resources in existing CERT infrastructure to address energy- specific incidents in real time). The CSIRT should be operating 7/24 with a primary task to help TSOs and DSOs in resolving all types of cyber-related incidents with a special focus on legacy systems and their disaster recovery procedures.

- The CA should be responsible to establish an online communication channel with the responsible Ministry and the NRA to enable a sound reporting and feedback line with all members of the energy sector. The CA should establish the system for early warning and exchange of information on cyber threats / provision of assistance in energy.

- The CA shall conduct an overall sector specific risk assessment for the country based on the collected relevant information about assets, vulnerabilities and threats. The assessment should include cascading cross sectorial and cross-border risks and is ought to be standardized to have proper measurement for the country continuously. The newly discovered risks must be managed through enforcing TSOs and DSOs in implementing action plans as well as controlling the management process. The processes should be defined as in ISO 27001 standard.

- For the smaller DSOs, generators or new type of market participants the CA should organize an energy ISAC as a source of information, analysis and remediation solutions. All the low and medium risks should be addressed at least on this way especially those which are not managed through incident handling procedures of the CSIRT. The services given through the ISAC should be on-time and with a value to the users on an expert level.

Energy Community Cybersecurity Study – general recommendations for NRA

https://www.energy-community.org/dam/jcr:db8e479d-b423-40c9-9ff9-998c7d9045ef/Blueprint_cyber_122019.pdf

- Cybersecurity capability of NRAs must serve as a central hub in exchange of critical infrastructure protection and cybersecurity energy related information in the CP.
- The capability development is 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), especially the cyber liaison officer.
- The cyber liaison officer must have a complete understanding of local energy market, critical infrastructure protection and also the 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 in cybersecurity and energy (in Ministries, CA's and to the local Govt. itself)
- The local NRAs must have the capability to understand 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 also have a 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.

Cybersecurity – technical standards overview

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

Energy Community Cybersecurity Study – specific technical recommendations for UKRAINE

https://www.energy-community.org/dam/jcr:db8e479d-b423-40c9-9ff9-998c7d9045ef/Blueprint_cyber_122019.pdf

- Ukraine is in state of hybrid war - available data is often obscure (of national security reasons). If some of the proposals and recommendation are in place, we suggest further improvement in a continuous PDCA (plan–do–check–adjust) cycle.
- Energy related governmental organisations and private companies must provide sufficient budget for developing more complex cyber defences (such as APT defence, OT systems high security authorisation infrastructure etc.), as well as an energy security simulator platform for exploring/modelling cyber warfare tactics in energy infrastructure.
- Ukrenergo (TSO) and Energorynok (MO) must develop and adopt ISO27k based secure processes for data exchange, acquiring and deploying new software systems which we recommend should be developed in security by design framework lifecycle. We propose to the NRA to make Ukrainian Energy Exchange implementing ISO 27k, ISO 27019, ISO 31000 based processes for cybersecurity so the interconnected IT systems may be certified.
- Ukaine gas TSOs Ukrtransgaz and electricity TSO Ukrenergo should implement ISO 27019 and establish a continuous management of risks, based on at least yearly regular assessment. The budget of the TSOs should be aligned with the risk management process. The key experts managing the risks should be no subcontractors but full-time employees, especially the obligatory CISO (Chief-Information-Security-Officer) position to fulfil segregation of duties controls.
- The final separation of business processes and IT systems between the GTS Operator of Ukraine, the Ukraine's gas storage facility and service departments of JSC Ukrtransgaz an ISO 27k based cyber risk analysis of the project is highly recommended for the gas TSO as ISO27k based information security management system for GTS Operator.
- As Ukraine owns Europe's most powerful network of underground gas storage facilities it is highly recommended to implement high security standards ISO 27k, ISO 27019, ISO 31000 on Naftogaz / UGS (underground-gas-storage-facilities). When purchasing and installing IT/OT strict vendor security checkout is mandatory.

Main areas (working groups)

Critical Energy Infrastructures / Essential Services

- Update on the State of affairs / recommendations / benchmark on the applied criteria (EnC) – update on the Study
- Common guidelines on the regional criteria for designation (ECS)
- Risk Preparedness Regulation (methodology) – (EC, ENTSO-e / ECS)

Legal framework (governance) – ECI Directive, NIS Directive

- Guidelines / roadmap for (early) implementation (ECS / TA)
- Cybersecurity Network Code (draft - EC)
- ECRB – application of technical standards for Cybersecurity (ToR – ECS / TA)

Energy Community ISAC (CSIRT network)

- White Paper, ToR, roadmap (ECS)
- Initial group of stakeholders (establishment) – (EnC)

Cybersecurity Academy

- Training seminars / workshops (ECS / TA)

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

THANK YOU

FOR YOUR ATTENTION

simon.uzunov@energy.community.org

www.energy-community.org

Ener_Community

/company/energy-community

/Ener.Community

/EnergyCommunityTV