Study on Cybersecurity in the energy sector of the Energy Community

Cybersecurity Study – 3rd Workshop

Blueprint Energy Solutions GmbH

Vienna, 10.12.2019

Cybersecurity Study – 3rd Workshop

- 10:00 – 10:10 Workshop and Study Introduction by ECS
- 10:10 – 10:30 Introduction into the Study, targets
  Elena B. Kovacs, Ales Hvala
- 10:30 – 11:00 Cyber threats and Risk analysis
  Peter Grasselli & Szabolcs Hallai
- 11:00-12:15 Contracting Party Reports on cybersecurity in energy
  Peter Grasselli
- 12:15 – 12:30 Coffee break
- 12:30 – 13:30 Recommendations & Discussion
  dr. Ferenc Suba

Introduction

Main objective of the Study was to assess and develop proposals for improving the energy-specific cybersecurity capabilities in EnC at national and regional/pan-European levels

- Legal framework
- Standards
- Institutional framework
- Cross-border initiatives
- Training programmes
- Cyber threats and risks
- Propose individual as well as EnC recommendations and roadmap

Looking back

In order to provide valid and viable results key methodology underlying principles were

- Interaction with stakeholders
  - Workshops, on site visits
- Confirmation of information
- Discussion/verification of current state assessment with stakeholders
  - Workshops

Study at a glance

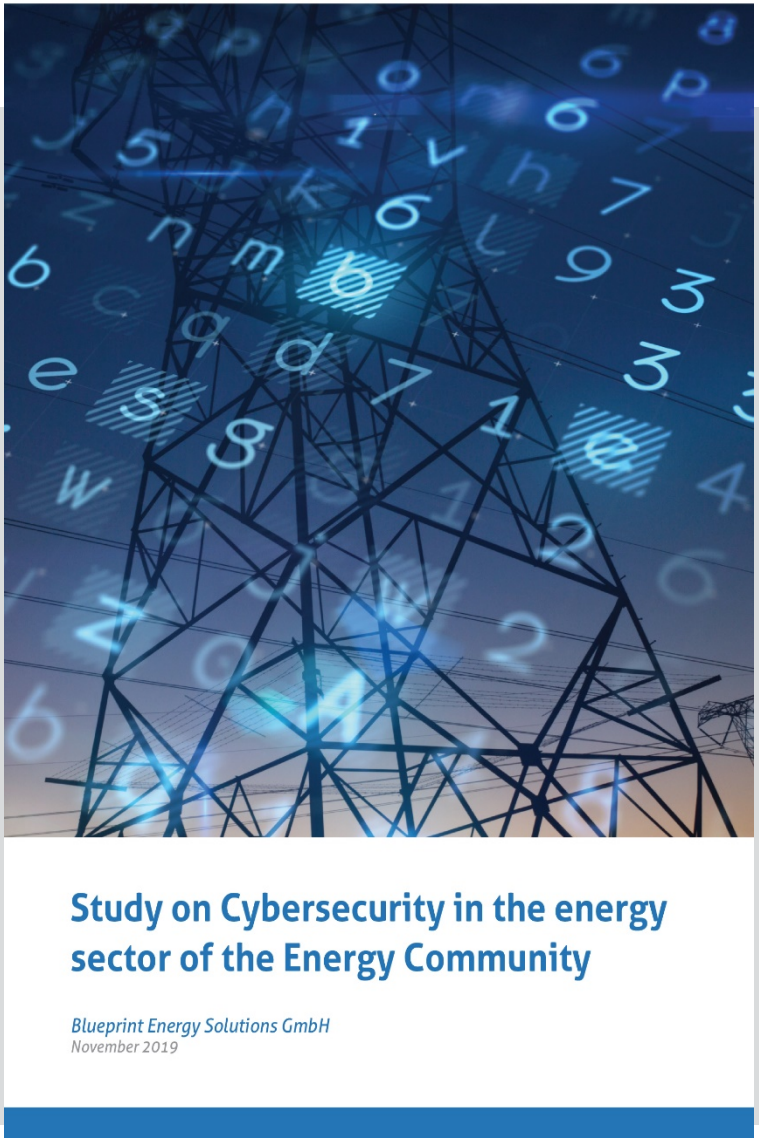
The starting point of this study was an assessment of the current state of development of the Contracting Parties with respect to the EU cybercrime legal framework &

The need to explore the incorporation of the NIS Directive into the **Energy Community acquis** (*)

Information sharing and trust are key elements in cybersecurity. The Procedural Act also established a Cybersecurity Coordination Group. The scope of the study was also to support this strategic body in providing guidance for assisting in building the capabilities of the Energy Community Contracting Parties

In cybersecurity, one size does not fit all. While there are common themes in the energy-related cybersecurity space, the specific vulnerabilities of each Contracting Party were analysed.

An overview for each Contracting Party, as well as a summary overview, risk assessment, followed by recommendations and roadmap was prepared.



(*) as cybersecurity was not explicitly recognized as an instrument for enhancing security of supply

Study at a glance

Main highlights:

The legal and policy context is complex and fragmented. There is a l**ack 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/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**.

Few good practices have been identified on the subject, and the current information sharing initiatives lack visibility within companies in the energy sector. Leveraging the activities of the Cybersecurity Coordination Group, it is proposed that EU cybersecurity legislation should be adapted and integrated into the EnC, which would provide a basis for **harmonising the cybersecurity approach at the EnC level**.

EU Legislation - Overview

Budapest Convention, Directive 2013/40/EU

On attacks against information systems - if action against integrity of IS is not a criminal offence in one of the countries then there is no ground toprosecute it

NIS Directive, EU Directive 2016/1148

Concerning measures for a high common level of security of network and information systems across the Union with identification of Operators of Essential Services, Country CSIRT, CSIRT Network, ENISA, Incident reporting/information sharing, National Strategy...

ECI Directive, Directive 2008/114

identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection

Directive 2013/40/EU of the European Parliament and of the Council

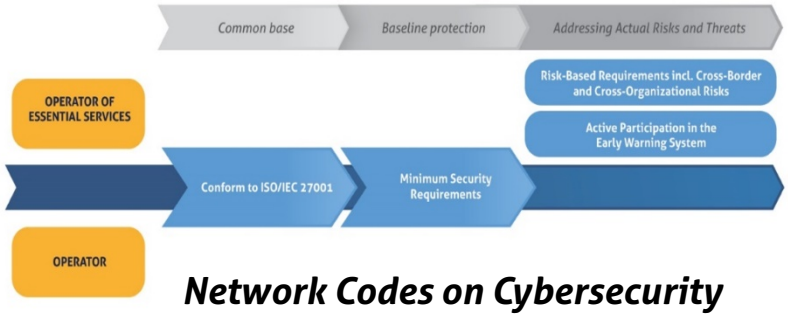
"On attacks against information systems" new rules harmonising criminalisation & penalties for a number of offences

Standards and Good Practice

Energy Community Procedural Act related to cybersecurity

EXPERT CYBER SECURITY PLATFORM

- Standardisation
- Full coverage regulatory requirements
- Information sharing (CERT, CSIRT, ISAC)



Network Codes on Cybersecurity

EU Commission Recommendation on Cybersecurity in Energy (April 2019)

European cybersecurity-standards

"ISO/IEC 27002:2017 Code of practice for information security controls" and "ISO/IEC 27001:2017

Information security management systems - Requirements" are the most relevant

ENTSO-E and ENTSO-G cybersecurity activities and recommendations

ENTSO-G

- Started collaborating in Gas Infrastructure Europe (GIE) Cybersecurity Taskforce to build a common understanding of key areas of importance for strengthening cybersec network codes for the gas sector
- Started developing solutions for data communication harmonization which introduces cybersecurity measures for security of information and data.
- Programme on cybersecurity includes the development and implementation of policies, controls and governance
- - Cybersecurity will become more important topic in the coming years, since ENTSO-G in planning to conduct survey regarding the implementation status of the NIS regulation among the ENTSOG/GIE members

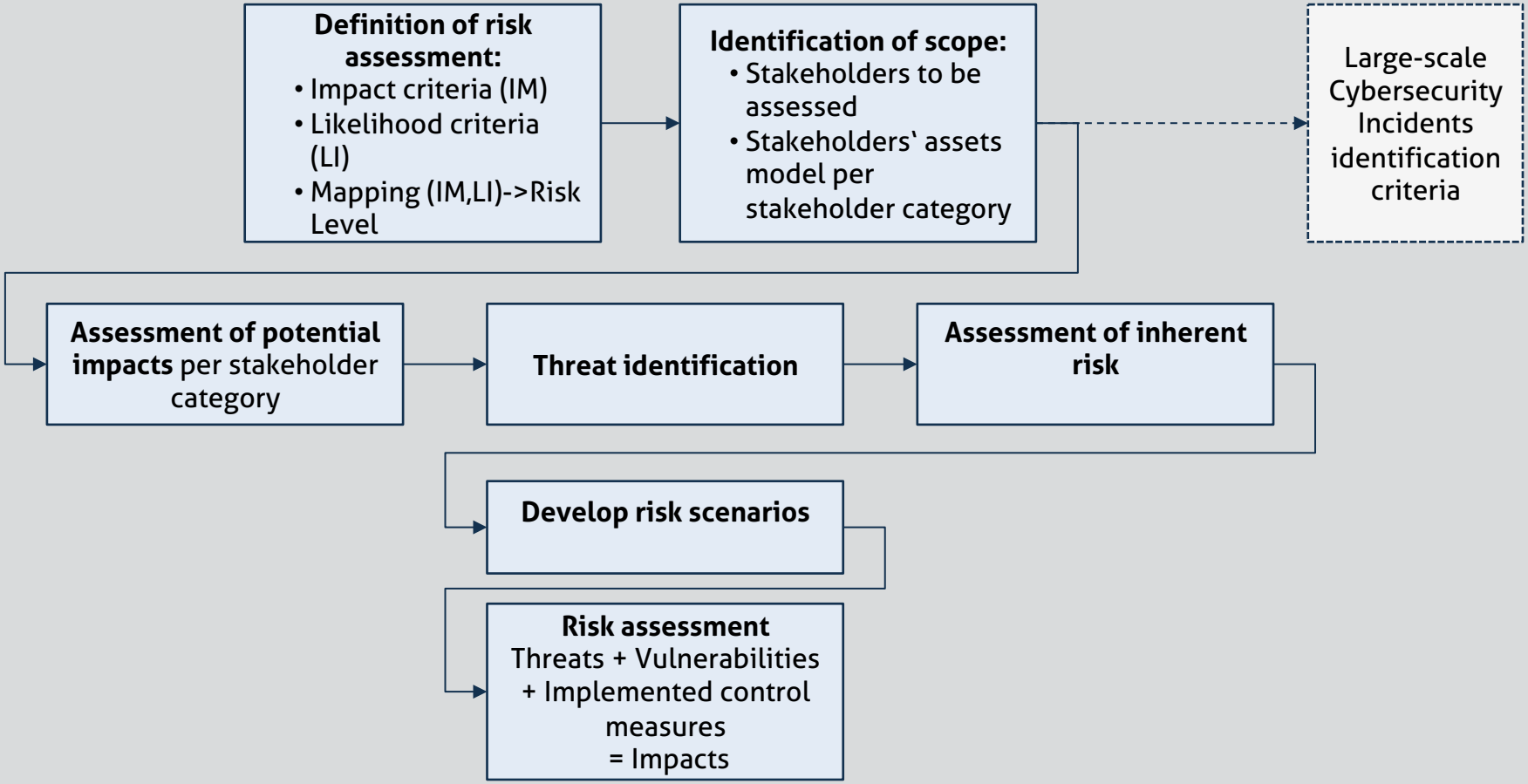
ENTSO-E

- It has been a platform for best experience and practice sharing between TSOs' for strengthening of cybersecurity.
- With adoption of Security Plan it addressed cybersecurity recommendations for operational planning data environment platform which encompasses a number of EnC Contracting Parties as well (*not available for public)
- Planning to address risk management and development of guidelines and recommendations for IT architecture, training and resilience building in the future.
- In the process of elaborating cyber-security strategy & supports operational training and organizes practical "red-blue team" exercises for TSOs' operational staff

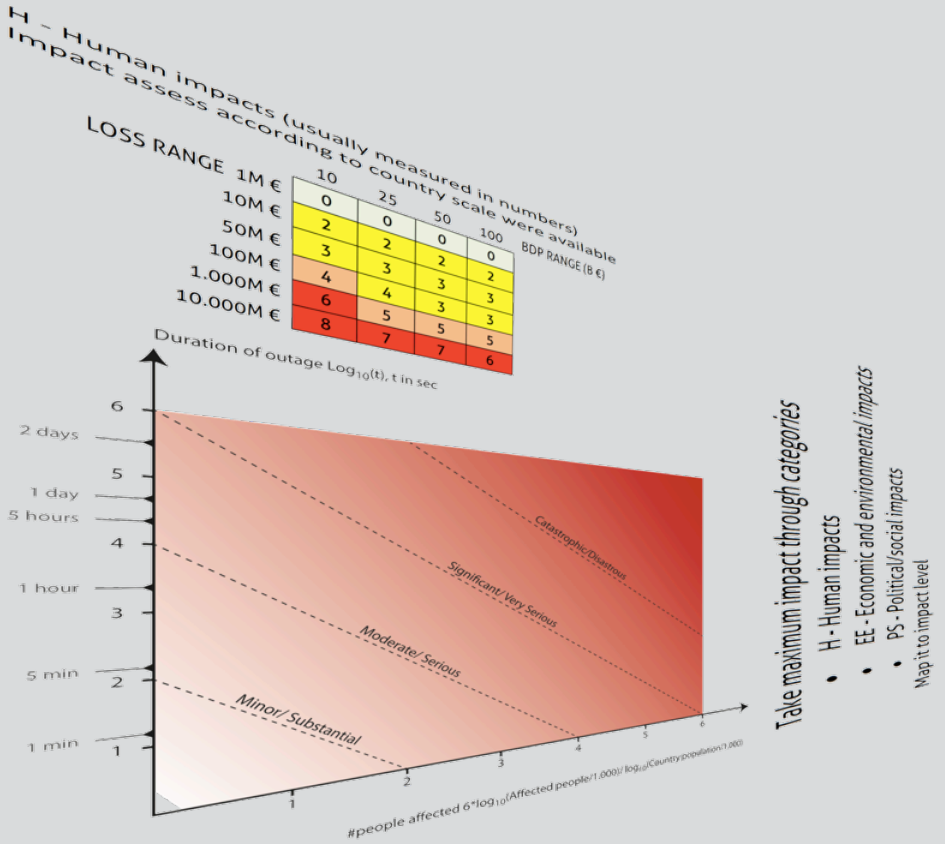
Cyber treats and Risk analysis

- Methodology
- Assessment context
  - Criteria, scope, threats
- Large scale incident criteria
- Case Study

Methodology



Criteria



Take maximum impact through categories

- H - Human impacts
- EE - Economic and environmental impacts
- PS - Political/social impacts

Map it to impact level

	The stakeholder is exposed to this threat; incidents based on this threat occurred in the country; such events occurred in the region in the last years	The stakeholder is exposed to this threat on a yearly basis; incidents based on this threat occurs in the country on regularly (e.g. several times a year); such events occurs in the region on monthly basis	The stakeholder is exposed to this threat several times a year; incidents based on this threat occurs in the country regularly (e.g. on monthly basis)	The stakeholder is exposed to this threat on a daily basis; common threats (e.g. malicious code);
	once in several years	yearly	monthly	daily
	Rarely	Possibly	Probably	Almost certainly
Catastrophic/ Disastrous	Very High	Very High	Very High	Very High
Significant/ Very serious	High	Very High	Very High	Very High
Moderate/ Serious	Medium	High	High	High
Minor/ Substantial	Low	Medium	Medium	Medium

Large-scale cyber incident criteria

Incident scope

Number of affected countries / Party risk level	1	2	3-5	More than 5
Beyond ability for country to handle	Large-scale	Large-scale	Large-scale	Large-scale
High		Large-scale	Large-scale	Large-scale
Medium			Large-scale	Large-scale

Assessment of cross border impacts (criteria)

- Bilateral
- ISAC

Cumulative impact assessment

- Aggregation
- Criteria/Analysis
- Sharing (warning structure/CSIRT)

Large-scale cyber incident criteria

Criteria sharing	Avgerage (1-4)
Criterial established only for consequences	3,0
Criterial established encompassing probability and impact (potential consequences)	3,6
Incident warning/information is shared on bilateral basis	3,6
Incident warning/information is shared at EnC level (central collection and distribution)	3,7

Incident information and assessment	Feasibility	Effectiveness	Wish to have
Information about impact criteria is not shared, shared is only incident information for incidents that are assessed as having significant/high impact in originating state (CP)	2,6	2,5	2,2
Information about impact criteria is shared between states concerned by a particular critical infrastructure, incident information is shared on the same basis	3,2	3,2	3,1
Information about impact criteria and incidents is shared with CSIRT/warning structure on EnC level	3,4	3,6	3,4
Information about impact criteria is not shared, however incident information is shared and assessed on EnC level based on aggregated impact and good practice – assessment information is than shared with CPs	2,6	2,6	2,9

Large-scale cybersecurity incident criteria type	Approach is feasible	Approach is appropriate
Data about (potential) consequences (e.g. number of affected consumers) is shared, aggregated and assessment is performed on the aggregated data	85%	65%
Shared is technical information about incident and CP's risk assessment (level of risk) performed according to CPs' criteria	74%	68%

Cumulative large-scale cybersecurity criteria	Avgerage (1-4)
Importance of identification of large scale incidents on cumulative (EnC) level	3,8

Scope (stakeholders and systems)

- Country cybersecurity authority (CA) and/or National Regulatory Agency (NRA)
- Transmission System Operators (TSO) Electricity
- Transmission System Operators (TSO) Gas
- Distribution System Operators (DSO) Electricity
- Country Distribution System Operators (DSO) Gas
- Generation/production
- Energy Exchange

- Determination of asset groups (e.g. SCADA, gas pressure balancing controls, office systems)

Threat identification

- Malware
- Web Based Attacks/Web application attacks
- Social engineering/Phishing/Spam
- Cyber Espionage/Cyberwarfare
- Denial of Service (DoS)
- Insider Threat (PWR)
- Botnet
- Ransomware

Inherent risk and impacts

GTSO stakeholder processes/ w systems	Human impacts (casualities)	Economic Impacts	Political/societal impacts	Highest Possible Impact	Comment
Operations controls processes (operations center, SCADA servers, etc.)	4	5	5	5	
Gas reception controls processes (SCADA front-end, PLCs etc.), transmission pipe lines, Corrosion Protection System	3	4	3	4	
Gas Pressure Balancing controls (Balance control, SCADA), Gas Market Monitoring (TSOs Data Exchange system)	3	4	4	4	
Gas Storages (load, capacity)	2	3	2	3	Due to moderate impact possibility we will not further develop scenario for this process/system but calculate it in other TSO scenarios as a possible distraction point
Office/Consumer processes (office systems, ERP, smart metering)	0	2	2	2	Due to moderate impact possibility we will not further develop scenario for this process/system but calculate it in other TSO scenarios as a possible distraction point

Generalized Impact scenarios	
IS1	A distruction in the TSO SCADA operations processes cause control and command system halted. After recovery period TSO operation processes transfer to manual handling.
IS2	Explosion caused outage, TSO is disrupted, due to low level of gas in storage facility. Outages lasts for 2 weeks. It is assumed that at least 50% of small consumers can switch to electric heating during the outage.
IS3	A cross-sectoral cascading electricity blackout paralyses the electricity DSO large consumer (gas TSO is one of them) delivery for 7 days. The GAS TSO data exchange system is down during that period.
IS4	Gas storage system - note: Due to moderate impact possibility we will not further develop scenario for this process/system but calculate it in other TSO scenarios as a possible distraction point
IS5	Office/consumer processes system - note: Due to moderate impact possibility we will not further develop scenario for this process/system but calculate it in other TSO scenarios as a possible distraction point

Sample of impact assessment (Gas TSO)

Overall cyber threat – relevance check

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

BLUEPRINT energy SOLUTIONS

Inherent risk analysis – scenario development

Scenario1 – Communication error	CA/NRA
Due to a cyberattack performed towards the telecommunication operators in the country, the telecommunication networks, including both wired and wireless communication networks, cease to operate. As a result of this outage in the telecommunication services the CA/NRA is not able to declare a state of emergency and inform the responsible parties about the incident and consequently no CSIRT is enforcing the necessary countermeasures to protect the TSOs and DSOs in their area of responsibility. Moreover, TSOs and DSOs that use the under-attack telecommunication networks, also suffer from a lack of communication with their remotely operated systems and Intelligent Electronic Devices. This results in TSOs and DSOs not being able to communicate with their crews, as well as not being in the position to perform critical remote operations, in most of the cases. In some cases, where the TSOs and DSOs operate their own telecommunication networks or the third-party networks were not affected by the cyberattack, they succeed to perform the necessary transmission and distribution network management, but in some parts of the country there was and outage for more than 8 hours and the gas transports to a neighbour was stopped for at least two days.	

			Quantified Impact on Energy Sector		
Threat	***Vulnerability***	***Likelihood***	*Health/Safety*	*Economic*	*Social*
DoSattack	Lack of procedures for reporting security weaknesses/incidents	***Possibly***	***1***	***4***	***2***
	Insecure network architecture				
	Lack of procedure of monitoring of information processing facilities				
	Lack of proper allocation of information security responsibilities				

Example of risk scenario

Inherent risk analysis – scenario list

Scenario ID	Stakeholder	Scenario name (in spider charts)
CA-S1	Competent Authority	Communication error
CA-S2	Competent Authority	False Communication
CA-S3	Competent Authority	Cascading effect from others
TE-S1	Electricity TSO	Deliberate actions (PWR)
TE-S2	Electricity TSO	Attack on central grid
TE-S3	Electricity TSO	Cascading effect from others
TG-S1	Gas TSO	Malware attack
TG-S2	Gas TSO	EMP attack
TG-S3	Gas TSO	Cascading effect from others

Scenario ID	Stakeholder	Scenario name (in spider charts)
DSE-S1	Electricity DSO	Hacked
DSE-S2	Electricity DSO	Cyberwar
DSE-S3	Electricity DSO	Cascading effect from/to others
DSG-S1	Gas DSO	Stolen data
DSG-S2	Gas DSO	Ransomware attack
DSG-S3	Gas DSO	Cascading effect from/to others
Gen-S1	Generation	Takeover of controls
Gen-S2	Generation	Stopping of monitoring system
Gen-S3	Generation	Cascading effect from/to others
Exc-S1	Exchange	Spot price manipulation

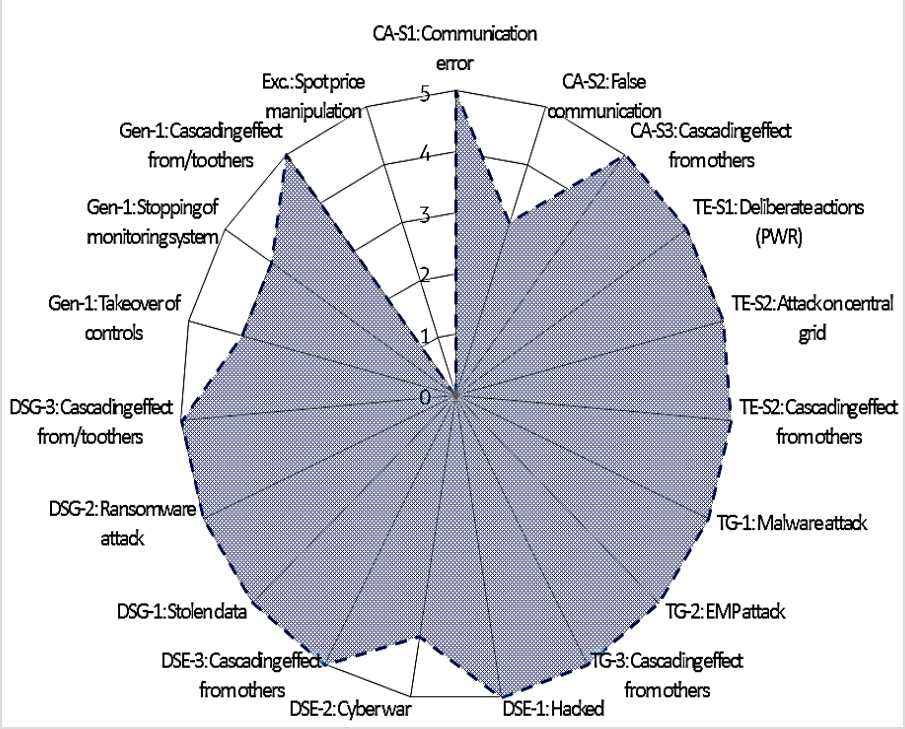
Inherent risk assessment of impact scenarios

NRA/CA

- lack of regulatory framework (TSO, DSO, PG)
- missing interoperability
- inability to communicate

TSO, DSO, PG

- infection of OT/legacy systems
- sabotage on OT (cascading effect)
- inability to react (cascading effect)



Spider chart presentation of risk scenarios – inherent risk

EnC Contracting Parties Reports on cybersecurity in energy

- Energy Community SWOT analysis
- Summary overview
- Contracting Party reports
  - Introduction
  - Overview and GAP
  - Risk assessment

Overview – EnC PA implementation

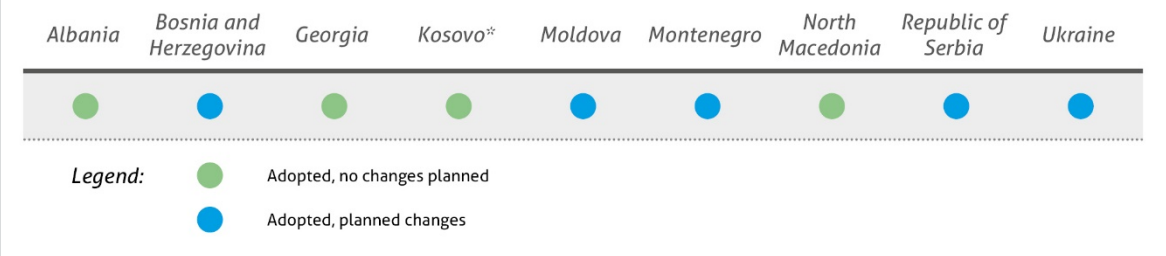
Organizational structures				
Contracting Party	National CS Authority	NIS SPoC	CI protection SPoC	CSIRT
Albania	NAECCS	NAECCS	Not established	NAECCS
Bosnia and Herzegovina	Not established	Not established	Not established	Not established
Georgia	DEA	DEA	Not established	DEA CERT
Kosovo*	KOS-CERT	KOS-CERT	Not established	KOS-CERT
Moldova	Ministry of Economy and Infrastructure	Ministry of Economy and Infrastructure	Anti-Terrorist Centre of Information And Security Service	CERT-GOV-MD
Montenegro	CIRT-ME	CIRT-ME	Not established	CIRT-ME
North Macedonia	Not established	MKD-CIRT	Not established	MKD-CIRT
Republic of Serbia	Ministry of Trade, Tourism and Telecommunications	Ministry of Trade, Tourism and Telecommunications	Ministry of Internal Affairs	RATEL CERT
Ukraine	State Service on Special Communication and Information Protection	CERT-UA	Not established	CERT-UA

Overview – EnC PA reporting

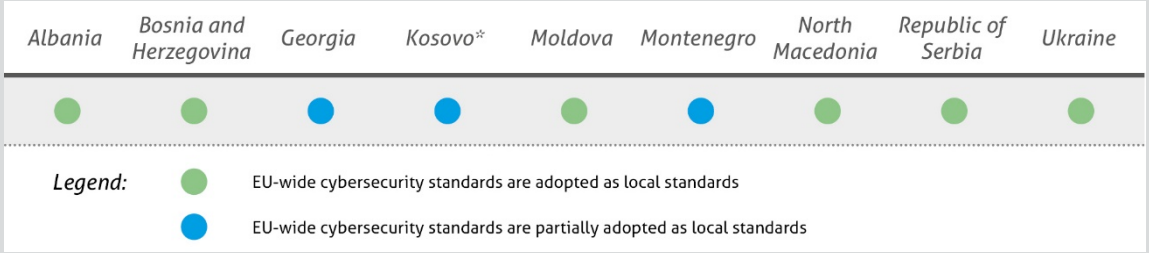
- Identification process and criteria for significance of disruption
- Identification of CI in the Contracting Party, its security measures and operator security plans implementation in accordance with ECI Directive article 5
- Operators security plans and notification requirements of EnCCI
- Security requirements for energy trading and balancing services, digital service providers and electronic communications operators necessary for energy sector CI functionality

Overview

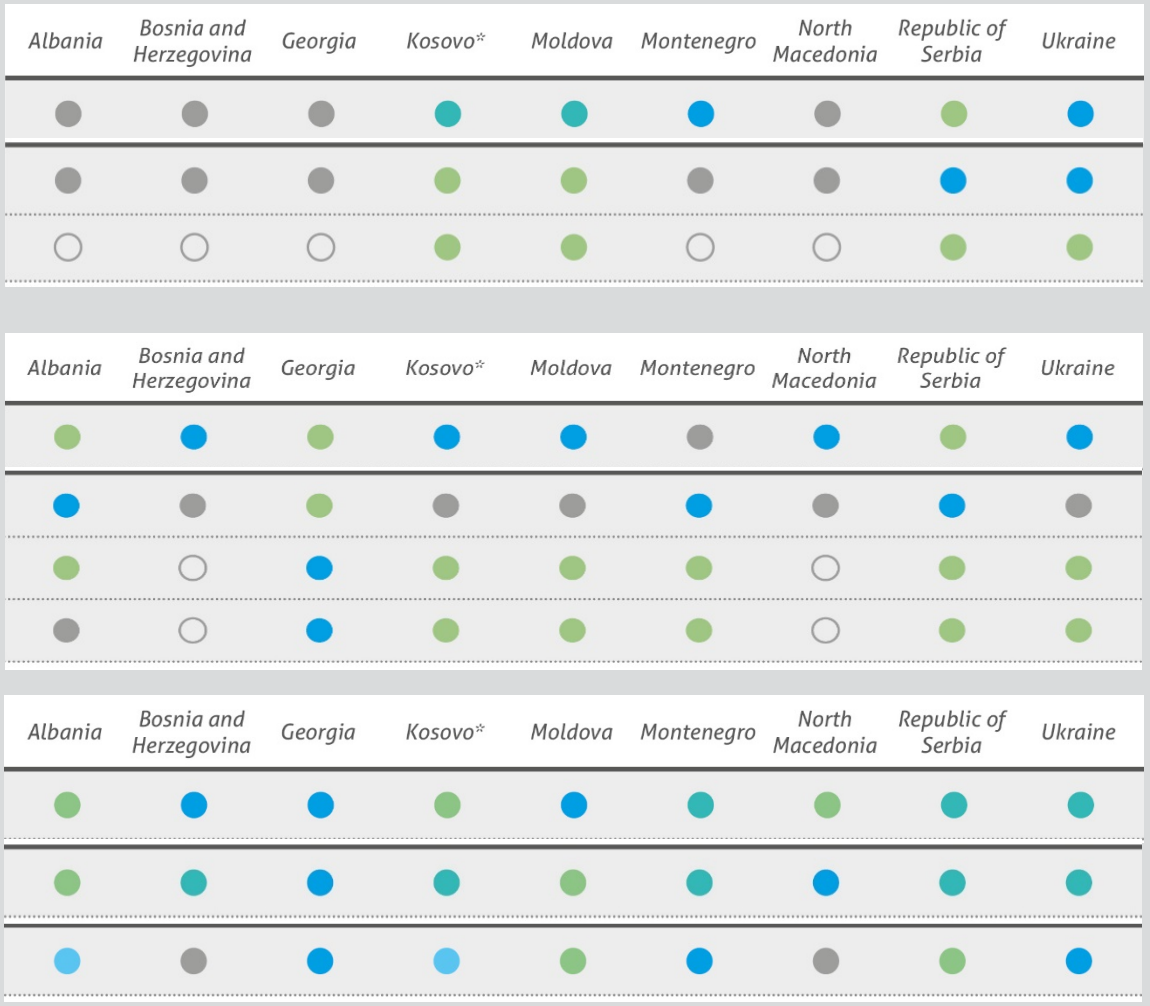
Cybercrime legislation



Standardisation



Overview


Albania
Bosnia and Herzegovina
Georgia
Kosovo*
Moldova
Montenegro
North Macedonia
Republic of Serbia
Ukraine
CI/EnCCI Identification Criteria
CI designation
Electricity/Gas
CII/OES Identification Criteria
Designation
Electricity
Gas
NIS Strategy
Contact points
Security plan

Energy Community

Energy Community

BLUEPRINT energy SOLUTIONS

Albania

Energy Community

BLUEPRINT energy SOLUTIONS

Albania

Identification of EnCCI/OES		
	Sectorial identification of CII/III (TSO/DSO SCADA) Disruption based identification criteria*	EnCCI not addressed Gas sector not identified Designation not yet performed

NIS strategy		
	National Policy Paper on Cybersecurity (2015-2017) New strategy in development	Follows NIS strategy requirements

Contact points					
	CS authority	NIS SPoC	CI protection SPoC	CSIRT	
	NAECCS	NAECCS	Not established	NAECCS	

CI operators/OES cybersecurity requirements		EE,EG-O
	ISM and CSS roles Risk management and ISMS (IT and OT) Reporting (measures, incidents)	Requirements follows EU good practice
	Legislation cybersecurity requirements follows good practice (e.g. ISO)	

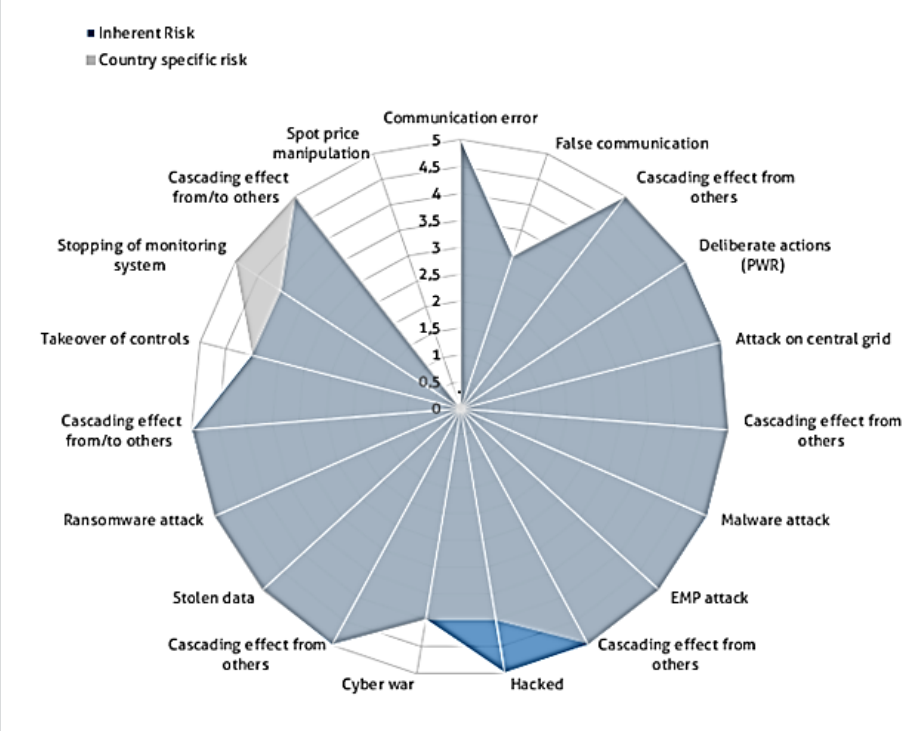
Country specific risk - Albania

Sources

- National Security Strategy 2014
- National Policy Paper on CS (2015-2017)
- Public data / state of overall CS in energy

Risks

- high-level threat vectors
- low level of controls by EU standards
- non-proper segregation of duties
- inducing a cascading effect to others
- budgetary limits



Albania risk profile

Bosnia and Herzegovina

Energy Community

BLUEPRINT energy SOLUTIONS

Bosnia and Herzegovina

Identification of EnCCI/OES		
	Identification criteria not defined Designation process not started	Nether EnCCI nor CII/OES identification started

NIS strategy		
	Strategic Framework for Cyber Security in development	No NIS strategy

Contact points					
	CS authority	NIS SPoC	CI protection SPoC	CSIRT	
	Not established	Not established	Not established	Not established	

CI operators/OES cybersecurity requirements		EE, EG-O
	Currently no legislative requirements	

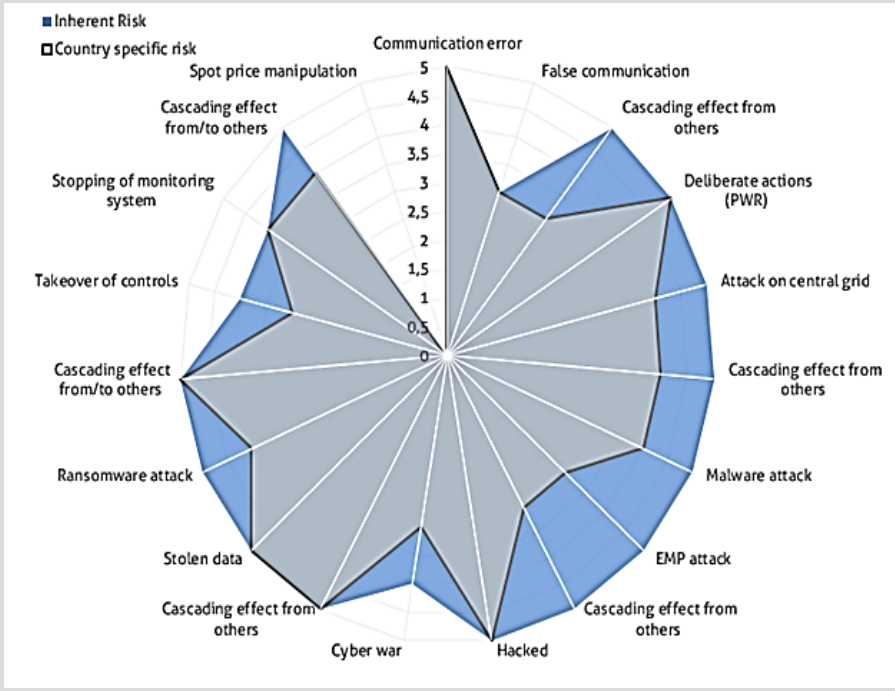
Country specific risk - Bosnia and Herzegovina

Sources

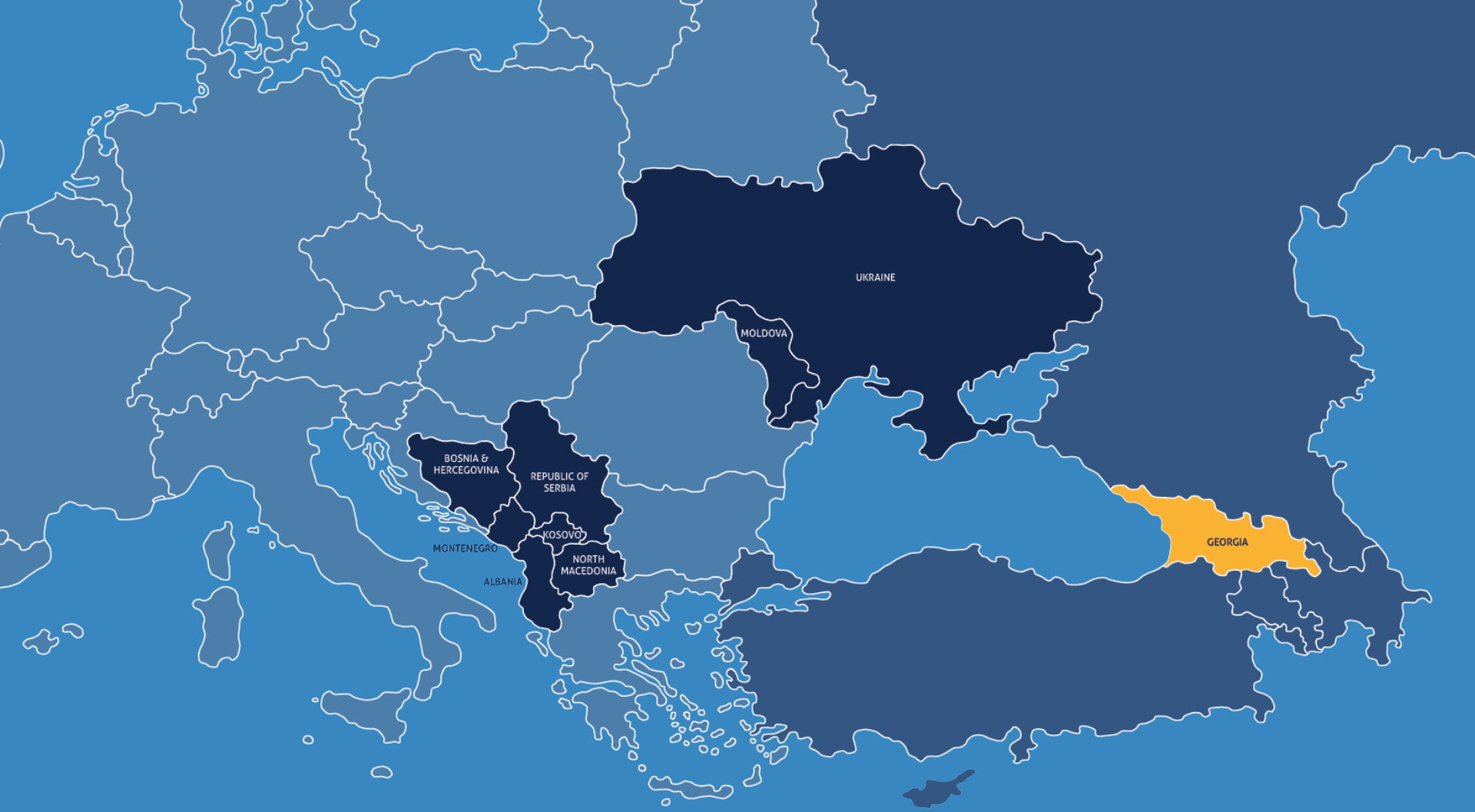
- National Security Strategy
- Defence White Paper of BiH 2005
- Stress test 2014 by EnC and EU Commission
- Public data / state of overall CS in energy

Risks

- absence of full cooperation of BiH entities on cybersecurity matters in energy sector
- segregated energy environments (+-)
- govt. hard imperative to manage the risks as a whole and implement regulation



BiH risk profile



Georgia

Energy Community

BLUEPRINT energy SOLUTIONS

Georgia

Identification of EnCCI/OES		
	CIS identification criteria defined CIS designated, disruption based criteria Energy sector CI/OES identification under way (Q4 2019)	EnCCI not addressed Energy sector not included

NIS strategy		
	National Cyber Security Strategy (2017-2018) New strategy in adoption (2019-2022)	Follows NIS strategy requirements

Contact points					
	CS authority	NIS SPoC	CI protection SPoC	CSIRT	
	DEA	DEA	Not established	DEA CERT	

CI operators/OES cybersecurity requirements		
	ISM and CSS foreseen in legislation Operators Security plans are foreseen in legislation (not binding for energy sector)	Requirements follows EU good practice
	NRA and energy sector developed informal communication practices and share knowledge, information and experience through such means with the DEA	

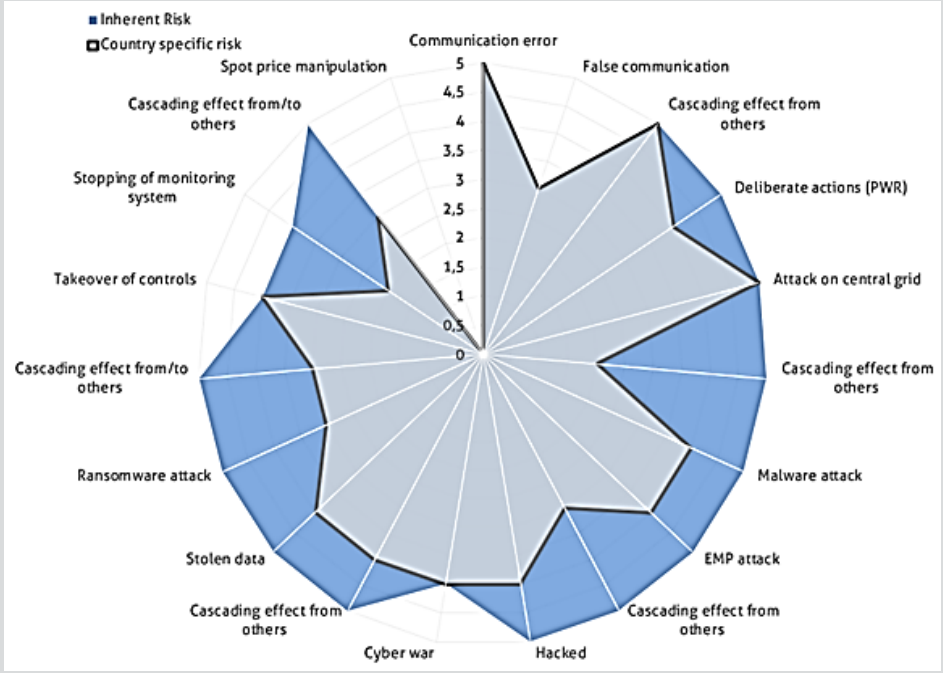
Country specific risk - Georgia

Sources

- National Security Concept
- Escalation of tension between Georgia and Russian Federation
- Public data / state of overall CS in energy

Risks

- high-risk of cyber terrorist attack
- cyberwar is a recurrent risk
- NATO cooperation (+)
- EU controls to be implemented (ISO27k)



Georgia risk profile


UKRAINE
MOLDOVA
BOSNIA &
HERCEGOVINA
REPUBLIC OF
SERBIA
KOSOVO
MONTENEGRO
NORTH
MACEDONIA
ALBANIA
GEORGIA

Kosovo*

Kosovo*

Identification of EnCCI/OES		
	CI designated (classified) Disruption based identification criteria OES not identified (foreseen in strategy, legislation not passed)	EnCCI not addressed OES criteria and identification not performed

NIS strategy		
	National Cyber Security Strategy and Action Plan 2016–2019	Follows NIS strategy requirements

Contact points					
	CS authority	NIS SPoC	CI protection SPoC	CSIRT	
	KOS-CERT	KOS-CERT	Not established	KOS-CERT	

CI operators/OES cybersecurity requirements		
	CI operators security plans	High level requirements
	High-level legislation requirements might result in different implementation levels	

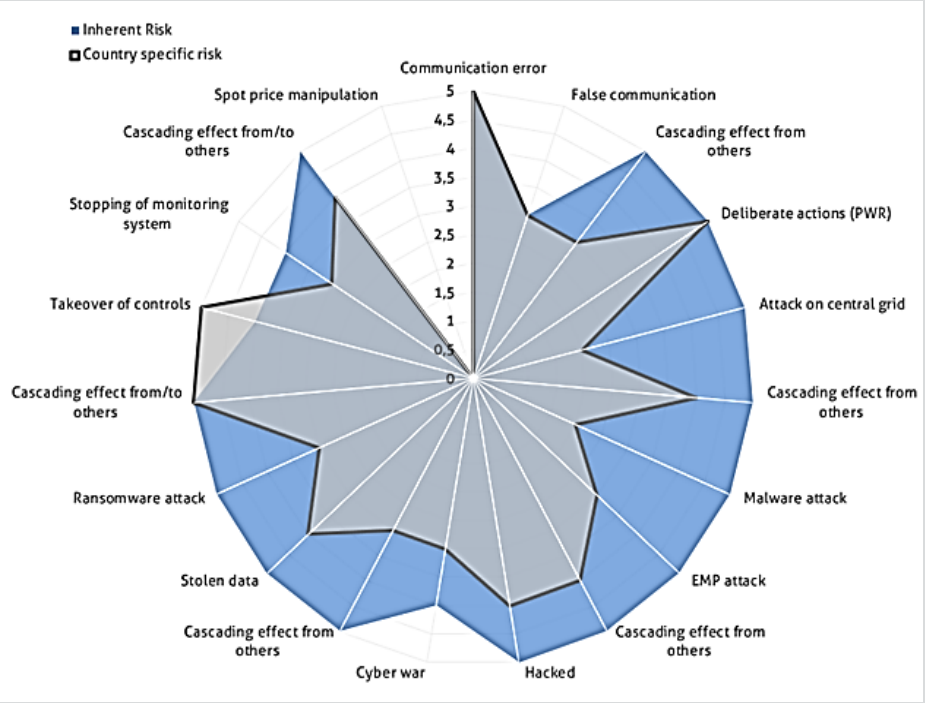
Country specific risk – Kosovo*

Sources

- Strategic Security Sector Review (2012)
- National Cyber Security Strategy 2016-19
- Public data / state of overall CS in energy

Risks

- cascading effect from/to others
- legal framework gaps
- lack of cyber controls in energy sector



Kosovo* risk profile


UKRAINE
MOLDOVA
BOSNIA & HERCEGOVINA
REPUBLIC OF SERBIA
KOSOVO
MONTENEGRO
NORTH MACEDONIA
ALBANIA
GEORGIA

Moldova

Moldova

Identification of EnCCI/OES		
	CI designated (classified) Disruption based identification criteria* OES not identified (foreseen in strategy, legislation not passed)	EnCCI not addressed OES criteria and identification not performed

NIS strategy		
	National Cybersecurity Program 2016-2020 and action plan Information Security Strategy for 2019-2024 (in adoption)	Follows relevant NIS provisions

Contact points					
	CS authority	NIS SPoC	CI protection SPoC	CSIRT	
	MEI	MEI	Anti-Terrorist Center of Information And Security Service	CERT-GOV-MD	

CI operators/OES cybersecurity requirements		EG-O
	Designate person responsible for cybersecurity Minimum Requirements in Cyber Security (decision), reporting	Requirements follows EU good practice
	Private owned CI operators of do not need to comply with the above-mentioned req.	

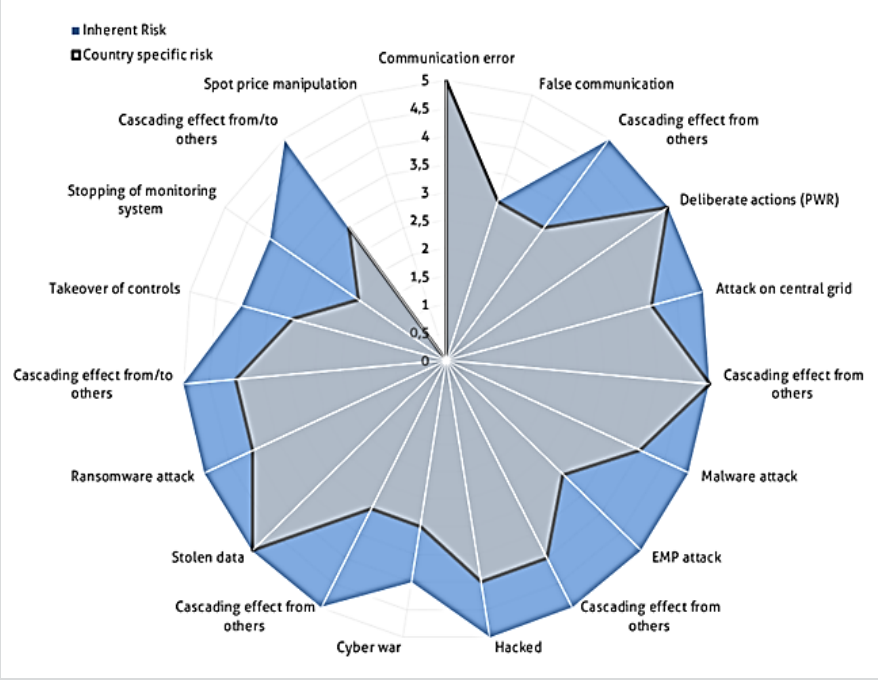
Country specific risk – Moldova

Sources

- National Security Concept 2005
- National Defence Strategy 2018
- Information Security Strategy 2019-2024
- Public data / state of overall CS in energy

Risks

- geopolitical risks / cyberwar-cyberterrorism
- NATO cooperation (+)
- legislative / control environment gaps
- cascading risks (from others)



Moldova risk profile


UKRAINE
MOLDOVA
BOSNIA & HERCEGOVINA
REPUBLIC OF SERBIA
KOSOVO
MONTENEGRO
NORTH MACEDONIA
ALBANIA
GEORGIA

Montenegro

Montenegro

Identification of EnCCI/OES		
	Law on CI in adoption Methodology for identification of CII, Sectorial list of CII Designation of CII operators ongoing	CI identification not performed CII/OES designation ongoing

NIS strategy		
	Cyber Security Strategy of Montenegro 2019-2021	Follows relevant NIS provisions

Contact points					
	CS authority	NIS SPoC	CI protection SPoC	CSIRT	
	CIRT-ME	CIRT-ME	Not established	CIRT-ME	

CI operators/OES cybersecurity requirements		EE
	Decree on IS - applicable only to public sector and data processing organisations, Regulation on standards - ISO 27K mandatory standards for implementation – but requirements not applicable to CII/OES	Based on EU good practice
	SCADA systems are identified as CII without any connection to sector	

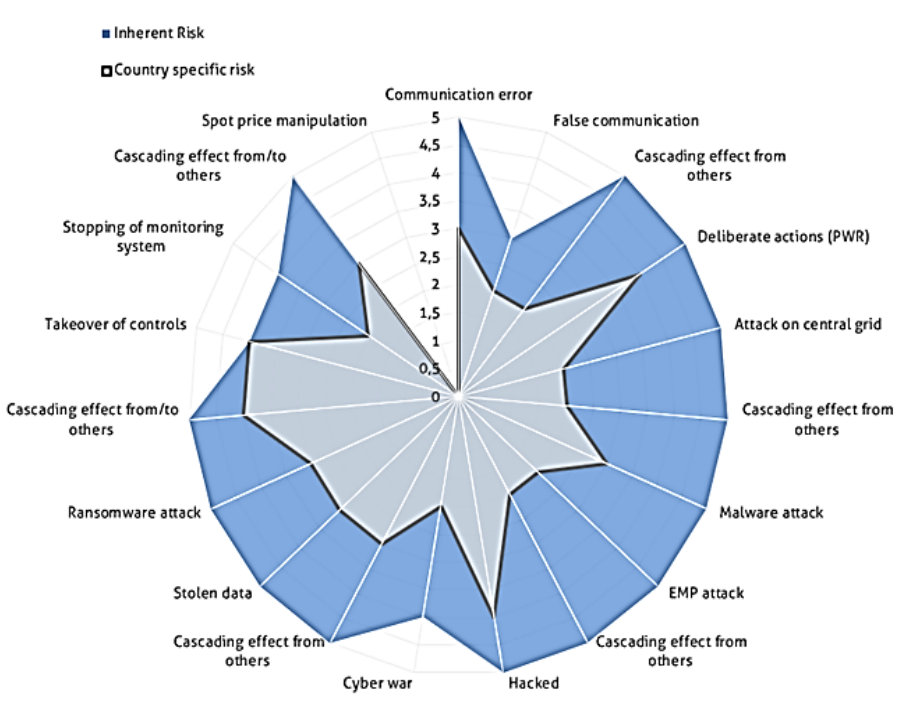
Country specific risk – Montenegro

Sources

- National Security of Montenegro in 2008
- Cyber Security Strategy of Montenegro 2018
- Public data / state of overall CS in energy

Risks

- ISO27k implementation (+)
- active cyber resilience during 2018/9 (+)
- cascading risks (from others)



Montenegro risk profile

North Macedonia

Energy Community

BLUEPRINT energy SOLUTIONS

North Macedonia

Identification of EnCCI/OES	
CI legislation in development (Q3) Study for the identification of CII/OES operators ongoing	CI identification not started OES designation ongoing (Q2 2019)

NIS strategy	
National Cyber Security Strategy for 2018-2022 Action Plan	Follows relevant NIS provisions

Contact points				
CS authority	NIS SPoC	CI protection SPoC	CSIRT	
Not established	MKD-CIRT	Not established	MKD-CIRT	

CI operators/OES cybersecurity requirements	EE, EG-O
No legislative requirements regarding cybersecurity	
CI legislation development and CII/OES identification	

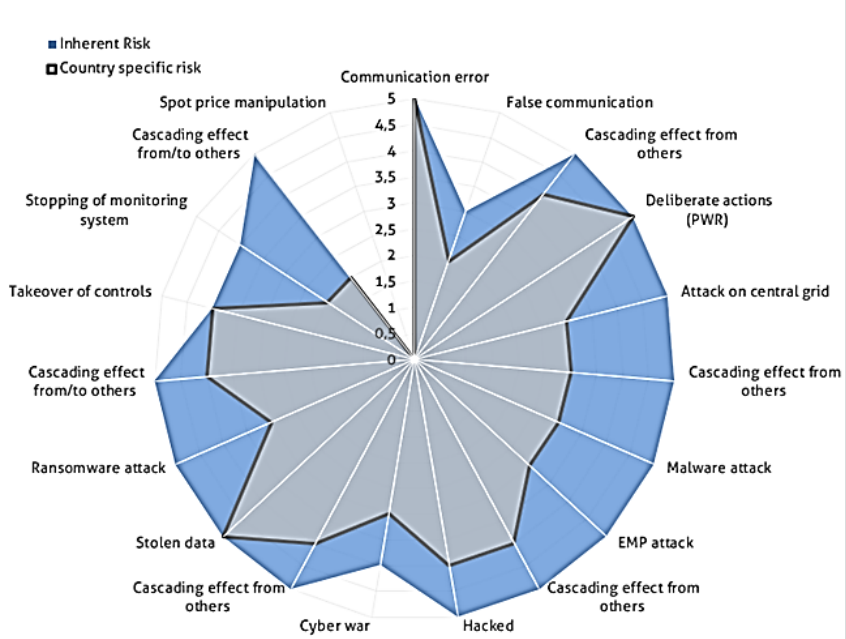
Country specific risk – North Macedonia

Sources

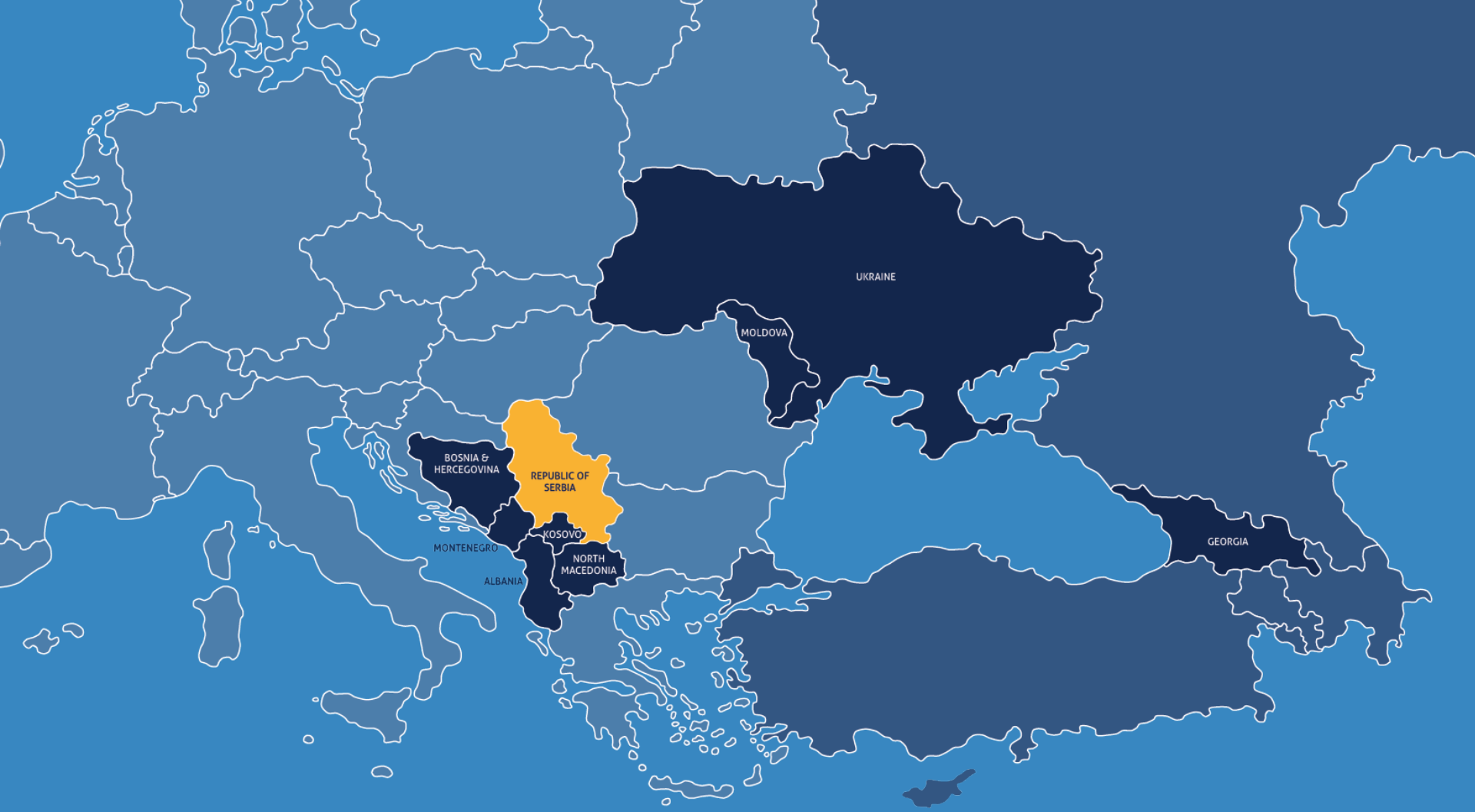
- Strategic Defence Review 2018
- National Cyber Security Strategy 2018-2022
- Public data / state of overall CS in energy

Risks

- active ENTSO-E and NATO cooperation (+)
- underdeveloped CS defence infrastructure
- organisational risks (NRA/CA)



North Macedonia risk profile



Serbia

Energy Community

BLUEPRINT energy SOLUTIONS

Serbia

Identification of EnCCI/OES					
	CI identification criteria classified ICT systems of special importance (CII/OES), sectorial list of stakeholders Disruption based identification criteria, (classified)			CI designation ongoing, ECI foreseen with the accession to EU OES designation ongoing	
NIS strategy					
	Strategy for the Development of Information Security 2017-2020 Action plan				Follows relevant NIS provisions
Contact points					
	CS authority	NIS SPoC	CI protection SPoC	CSIRT	
	Ministry of Trade, Tourism and Telecommunications		MIA	RATEL CERT	
CI operators/OES cybersecurity requirements					**EE**
	Security liaison officer for protection of CI Protection measures (regulation)			Requirements follows EU good practice	

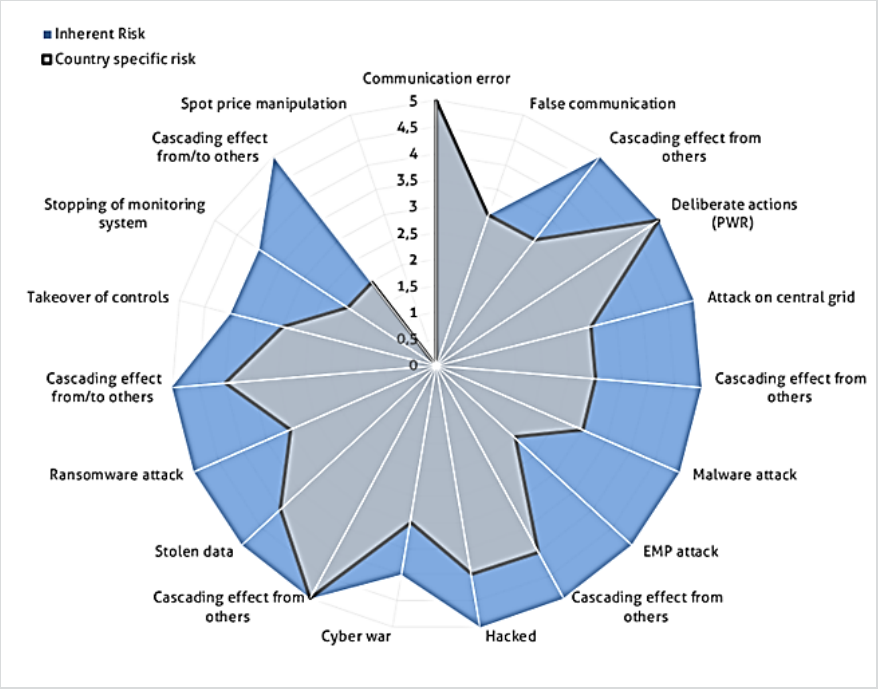
Country specific risk – Serbia

Sources

- National Security Strategy
- Strategy for Development of IS 2017-2020
- Strategy for combating high-tech crime
- Public data / state of overall CS in energy

Risks

- lack of the energy sectorial specific cyber defense architecture
- cascading effects from neighbours
- control gaps (NRA)



Serbia risk profile

Ukraine

Energy Community

BLUEPRINT energy SOLUTIONS

Ukraine

Identification of EnCCI/OES		
	"Important facilities" and operators designated (criteria not publically available) OES identification no performed	Process of CI identification potentially not aligned with ECI OES not identified

NIS strategy		
	Cyber Security Strategy of Ukraine, yearly Action Plans	Follows relevant NIS requir.

Contact points					
	CS authority	NIS SPoC	CI protection SPoC	CSIRT	
	State Service on Special Communication and Information Protection	CERT-UA	Not established	CERT-UA	

CI operators/OES cybersecurity requirements		EG-O
	Complex System of Information Protection (KSZI) General Requirements for Cybersecurity in Critical Infrastructure objects	Not aligned with EU good practice Requirements follows EU good practice (applicability?)
	Ministry of Energy and Environmental Protection is developing energy sector specific cybersecurity strategies, regulations and incident response capabilities.	

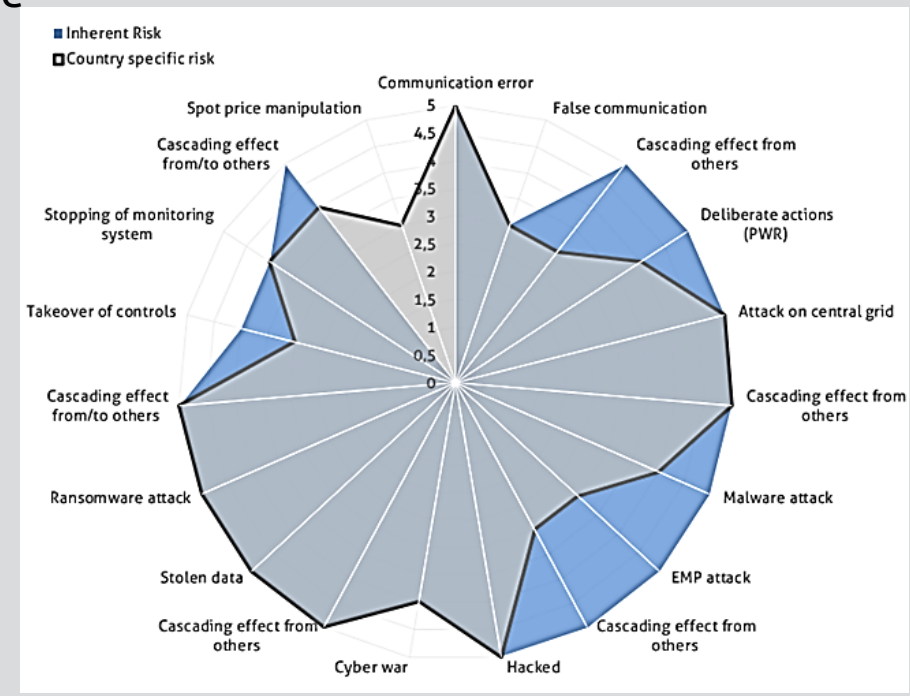
Country specific risk – Ukraine

Sources

- Strategy of National Security of Ukraine
- Doctrine of Information Security of Ukraine
- Public data / state of overall CS in energy

Risks

- under constant cyberattack
- geopolitical conflict
- cybersecurity measures on op. level
- cooperation with EU and NATO (+)
- control gaps (NRA)



Ukraine risk profile

Recommendations

- Proposed measures on national level
- Proposed measures on regional level, cooperation mechanisms
- Roadmap for implementation

Contracting Parties General Recommendations

- CA, together with the NRAs should develop and prescribe requirements certification scheme for CISO position in energy sector
  (ISO 27019 lead auditor IRCA certification, CISA, CISM and CISSP)
- CPs should establish bilateral cooperation's through country energy CSIRT and ISAC with neighbouring countries to address cascading risks
- Energy sector companies should completely and successfully finish the unbounding process and the segregation of unnecessary interconnected IT/OT systems
- The TSOs (both electricity and gas) implementing EU wide and international cybersecurity good practices (ISO27000 framework, especially ISO 27019) and to establish a continuous risk management process

Competent Authorities general recommendations

- During implementation of the legal framework / providing budgetary resources
- **Organizing a sector specific energy CSIRT**
- CA to e**stablish an online communication channel with the responsible Ministry and** NRA
- Overall sector specific risk assessment for the country
- CA should organize an energy ISAC as a source of information for SMBs

National Energy Regulatory Authorities general recommendations

- Developing NRA CS capability (central hub in exchange of information)
- NRA cyber liaison officer (CISA, CISM, CISSP. ISO27LA) – focal point for EnC CG
- CA to e**stablish an online communication channel with the responsible Ministry and** NRA
- Capability in EU CIP and NIS Directive issues (power to enforce)
- Power to audit/monitor licencees in CS issues

Electricity sector general recommendations

- Handling new type of vulnerabilities (vendors/service providers as source)
- Limiting remote access (especially from public infrastructure)
- Information security audit / forming expert SOC
- Taking active role in forming the e-ISAC
- Capability for smart metering, SCADA, IoT (SOC)
- For critical projects/processes implementation of standards (ISO27k, ISO31000)
- For TSOs active cooperation in ENTSO-E

Gas sector general recommendations

- Recognizing vulnerabilities and mitigating risks in legacy IT and OT systems
- Yearly security tests of pumps and metering infrastructure (smart features)
- Disconnect all critical networks from public access infrastructure
- Assessing CMI impact on CI
- Fully IT/ITSEC segregation of DSO from TSO (if it is not done yet)
- For critical projects/processes implementation of standards (ISO27k, ISO31000)
- For TSOs active cooperation in ENTSO-G

Albania country recommendations

1. Implementation of cybersecurity standards during development of an action plan for joint power exchange by the Kosovo* and the Albania Working Groups.

2. All the cybersecurity risks when developing infrastructure for AGS must be addressed in a timely manner and managed to prevent cascading incidents.

3. Creation of a SOC and coordination of its activities with gas TSOs in Greece and Italy.

Bosnia and Herzegovina country recommendations

1. Organization of a unified cybersecurity protection system for the energy sector with well-defined communication and reporting channels.

2. Establishment of bilateral agreements regarding entities and district legislative aligning with regards to recommendations in energy sector.

3. Enforcement of implementation of security standards to measure and manage risks, as well as to define and maintain processes

Georgia country recommendations

1. NRA must develop its own cyber security expertise in energy sector to successfully cooperate with DEA.
2. Development of a risk assessment study for the energy sector.
3. Following the completion of Georgia's Improved Power Transmission (GIPT) Project, a targeted security risk assessment especially about the possible impacts of cascading risks in smart grid components and transformer gas monitoring system should be performed by the TSO.

Kosovo* country recommendations

1. Provision of legal framework and sufficient budgetary resources for implementing laws, legal documents and strategies for the cybersecurity protection in energy sector.

2. Establishment of an early warning and an exchange of information system for cyber threats.

3. Electricity TSO (KOSTT) and KEK 142 to provide joint continuous cyber risk assessment and management of cyber assets for KOSOVA A and B power plants.

Moldova country recommendations

1. Identify and operators of CI/ES in the energy sector.
2. Mandatory implementation of ISO 31000 and ISO 27001 during the planning and developing the Ungheni-Chisinau project.
3. Risk management for legacy system for TSOs and DSOs the provision of the needed security level of supplies.

Montenegro country recommendations

1. CA should take into consideration an energy specific cooperation network and must be aware of responsible parties in neighbouring countries in the handling of energy specific cyber incidents in the context of the Memorandum of Understanding with Albania.

2. Implementation of cybersecurity standards for the power exchange company of Montenegro (BELEN)

3. Risk assessment related to the Adriatic Pipeline and the Ionian-Adriatic Pipeline to prevent cascading effects.

North Macedonia country recommendations

1. Implementation of cybersecurity standards for the day-ahead market, as well as for Bulgaria and North Macedonia market coupling.
2. Implementation of cybersecurity standards during planning, implementation and commissioning of the Nea Mesimvria – Skopje gas pipeline project.
3. Electricity DSOs to form their own cyber security protection environment covering the aspects of smart metering and large scale IoT systems.

Republic of Serbia country recommendations

1. Implementation of cybersecurity standards for the day-ahead market on SEEPEX, as well for the coupling of the SEEPEX and HUPX exchanges in Serbia and Hungary, respectively.
2. Implementation of cybersecurity standards for TurkStream pipeline development.
3. Implementation of cybersecurity standards during planning, implementation and commissioning for the Banatski Dvor gas storage facility expansion project.

Ukraine country recommendations

1. As Ukraine owns Europe's most powerful network of underground gas storage facilities (UGS)150 it is highly recommended to implement high security standards.

2. Implementation of cybersecurity standards for the electricity and day-ahead markets by Ukrenergo.

3. Implementation of cybersecurity standards during separation of business processes and IT systems between the GTS Operator of Ukraine and service departments of JSC Ukrtransgas.

Recommendations for EnC framework

- Forming of Cyber CG Action Group (leadership involvement, arbitrary issues)
- Forming Cyber CG secretariat (coordination, e-CSIRT, certification scheme issues), NRA coordination group (monitoring, legal framework, EU bodies communication) – segregation of sensitive data
- Cyber CG TSO working stream (exchange of information, ENTSO-E, ENTSO-G)
- Establishing EnC e-CSIRT (ENISA contacts, cyber awareness, cyber exercises, trainings)
- Establishing EnC e-ISAC (DSOs, SMBs etc.) and early warning communication system

Recommendations for regional cooperation mechanism on EnC level

- Trust is a key component
- Only few energy sector specialist have in-depth understanding
- Issues are often addressed on CP level – this need to change
- The legal and policy context is complex and fragmented
- The given information need to have applicable taxonomy
- Need to create PPP (ISACs)
- Focus is today more on physical infrastructure, cyber is „newbie“

Recommendations for certification schemes

- ISO27k family of standards, especially ISO27019 for ISMS
- ISO31000 for risk management
- Standardised audit for the stakeholders based on ISO
- To be modified if ENISA release it's own schemes
- Personal certification of key personnel (CISA, CISM, CISSP, vendor-based)

Recommendations for awareness and training

The goal is to develop an EnC CS education program to raise capability:

- In transposition of EnC acquis cybersecurity requirements into local legislation
- In making unified criteria for the identification of CI, ESP and significant disruptive effect
- Gaining knowledge on CS EU wide standards and good practice
- Have information about CS aspects of new and emerging technologies

Impact assessment of proposed measures

Legislative measures: *High impact for legal framework/ CI and ES identification*

Organizational measures: *High impact for forming e-CSIRT / medium for NRA capability program*

Cooperation improvement: High impact for cross-border crisis management, medium for cross-border cooperation and data exchange, low impact on PPP cooperation

Cybersecurity education: Low impact on implementing energy specific cybersecurity educational/awareness schemes

Cybersecurity certification: Medium impact on process certification schemes and low impact CS expert certification schemes

Roadmap with timing – EnC roadmap

Proposed provisions and measures	*Expected results*	*Timing*
Adapt and encompass EU cybersecurity legislation into the EnC acquis	EnC acquis aligned with EU cybersecurity legislation and good practice	*6 months*
Further development of EnC cybersecurity organisational structure	Establishment of: • Cyber CG NRA Working Stream • E-CSIRT working group • Cyber CG TSO/DSO Working Stream	*6 months*
Establish Cyber CG activities monitoring improvements process	Develop and implement monitoring and improvement process	*6 months*
	Regular progress reporting	*Quarterly*
Support to CPs in the implementation of legislative requirements	Organisation of awareness campaigns, capacity building and training activities	*24 months*
Sharing and coordination of essential cybersecurity information and activities between CPs	EnC CSIRT	*24 moths*
	EnC ISAC	*12 months*
	Cybersecurity incidents early warning communication system	*12 months*
Harmonisation of Contracting Parties' cyber security standards with EU wide standards and good practice	Providing technical assistance on: • Methodologies and standards • Certification schemes • Mutual recognition of accredited certification bodies	*24 months*

Roadmap with timing – Standard CP roadmap

Proposed provisions and measures	*Expected results*	*Fulfilment End date*	*Project sponsor*
Addressing gaps between national and EU legislation and standards	National legislation aligned with amended EnC acquis	24 months	CA
Designation of EnCCI and ES and implementation of OSP	CPs energy sector cyber risk analysis (CI and ES overall risk based, with cross-border and cross-sectorial risks taken in account).	within 12 months	CA
	CI and ES designation	24 months	CA
	OSP plans developed for EnCCI and OES	36 months	CA/TSO/DSO
Organisational changes for NRA (internal knowledge of cybersecurity issues, information security audit capability in energy sector)	NRA cybersecurity/security of supplies function NRA reporting cyber security status in energy sector to CA	within 12 months	NRA
Energy specific CERT/CSIRT	Operational national energy CSIRT	within 18 months	CA
	Early warning cooperation program regarding energy in national CSIRT	within 18 months	CA

Roadmap with timing – Standard CP roadmap cont.

Proposed provisions and measures	Expected results	Fulfilment End date	Project sponsor
Cross-border cooperation and data exchange	Cooperation MoUs with neighbouring countries regarding cybersecurity matters in energy sector, data exchange, incident cooperation	within 18 months	CA
Cross-border crisis management	Cooperation MoUs with neighbouring countries regarding incident cooperation, forming a joint task force	within 24 months	CA
Proposals for implementing energy specific cybersecurity educational/awareness schemes	National energy sector related cybersecurity education schemes in alignment with EU same program, 3-year cybersecurity awareness program in energy sector, joining ENISA/EnC exercises regarding energy	within 12 months	CA
Proposals for energy systems/process certification schemes	IT/OT and process certification schemes in energy sector	within 12 months	CA/CP Accreditation Authority
	ISMS certification of TSOs and DSOs, IT and OT assets (vendor) security certified, Large scale project IS risk management certified	within 24 months	TSO/DSO/ Vendor
Proposal for PPP cooperation	Operational national energy e-ISAC	within 24 months	CA and NRA

Energy Community

BLUEPRINT energy SOLUTIONS

Discussion?