Study on Cybersecurity in the energy sector of the Energy Community

Blueprint Energy Solutions GmbH
November 2019

This document has been prepared by Blueprint Energy Solutions GmbH ("Blueprint") at the request of the Energy Community Secretariat ("Client"). This study was prepared for the sole benefit and use of the Client and is based on the scope of work agreed with the Client that may not meet the interest or priorities of any third party.

The study must be construed in the context in which it was prepared including the constraints relating to availability of time and information, the quality of that information, scope of work Blueprint agreed with the Client and Blueprint assumptions and qualifications, in each case, as more fully set out in this report. Information and the opinions expressed are subject to change without notice.

The information contained in this document is supplied to any person only on the condition that Blueprint and any employee of Blueprint are not liable for any information within the document including any error, inaccuracy, whether negligently caused or otherwise, or for any loss or damage suffered by any person due to such error, omission, or inaccuracy.

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

www.energy-community.org

Consultant: Blueprint Energy Solutions GmbH, Am Gestade 3, Vienna, Austria

www.blueprintenergy.at

Date: November 2019

Document ID: FINR-CS-EC-211019

1 Executive Summary

THE STUDY AT A GLANCE – SCOPE AND RESULTS

Cybersecurity of critical infrastructure, especially in the energy sector, is becoming more important for the safety and security of energy production, distribution, transmission and storage, as well as for the stability of the European single energy market.

Information sharing and trust are key elements in cybersecurity.

For the purpose of promoting a high level of security in information systems and networks of critical infrastructure, the Procedural Act was adopted by the Energy Community with the aim of facilitating strategic cooperation and information exchange. In line with this objective, the Energy Community Secretariat has launched this study with the aim of contributing to building energy-specific cybersecurity capabilities at the national and Energy Community levels, eliminating regulatory gaps in the cybersecurity framework and harmonizing cybersecurity measures across the single energy market, including both Energy Community Contracting Parties and EU Member States.

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 with respect to cybersecurity and protection of critical infrastructure, and, at the time of publishing of the study, to reinforce the development of common methodological guidelines for risk assessment and analysis in the energy sector, by providing the owners of infrastructure and other stakeholders with access to best practices, methodologies and training on technical issues and security .

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 (Budapest Convention), which forms a basis for cybersecurity legislation by defining criminal law offences and associated provisions and thus enables prosecution of cybercrime actors. Special attention has been placed on critical infrastructure and essential services identification criteria, as well as on national strategies on the security of network and information systems applicable to both the electricity sund gas sectors.

An overview for each Contracting Party, as well as a summary overview, was prepared based on the collected and consolidated information. International standards and training programs, as well as cooperation initiatives as enablers for energy-related cybersecurity capacity building, were indicated at a country level.

In cybersecurity, one size does not fit all. What might work for the Internet and is addressed by appropriate legislation will not necessarily be adequate for the energy sector. In addition, while there are common themes in the energy-related cybersecurity space, the specific vulnerabilities of each Contracting Party were analysed. Identification of key weaknesses, risks and potential exposure to cyber threats in energy systems, as well as actors whose disruption by a cyber-incident might have a significant disruptive effect, was

performed based on the energy sector stakeholder model, including possible cyber-attack scenarios, followed by the particular aspects of the Contracting Party.

Moreover, a set of recommendations was prepared based on the assessment of gaps between the Contracting Party legislation and EU-wide energy sector cybersecurity legislation and standards. Energy Community-wide and Contracting Party-specific cybersecurity risk assessment were addressed by these recommendations.

In the final step, an impact assessment of the implementation of the proposed measures and acts as well as a roadmap of the timing of their implementation, which gives a general overview of the next steps forward, were provided.

Based on the results of this study, it can be concluded that:

- 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 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**.

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 Energy Community, which would provide a basis for **harmonising the cybersecurity approach at the Energy Community level**.

ASSESMENT OF GAPS IN CYBERSECURITY RELATED INSTITUTIONAL AND LEGAL FRAMEWORKS

An overview of the current state of development of the cybercrime legal framework of the Energy Community Contracting Parties compared to that of the EU is provided below. In summary, while national strategies on the security of network and information systems as a crucial cybersecurity building block have been developed in most (seven) Energy Community Contracting Parties and are significantly aligned with the EU

cybersecurity framework, the energy sector is referenced in only three strategies, indicating the strong need for continued effort in this domain.

All Contracting Parties except Kosovo*[1] have signed the Budapest Convention. However, it should be noted that Kosovo* has transposed all necessary provisions and harmonized the national legislation.

In comparison with critical infrastructure identification criteria, the situation is significantly more developed regarding criteria for the identification of essential services, which were already established or in preparation in practically all Contracting Parties at the time of the study. However, only one Contracting Party designated an operator of essential services, while three have started the designation process. The only observed difference between the electricity and gas sector is that the designation criteria in Albania do not include a gas subsector.

The designation of strategic and operational/tactical contact points that are important for the prevention of and efficient response to cyberattacks has been competed in seven Contracting Parties and is underway in another two. It should be noted that contact points for the energy sector are explicitly defined in only two Contracting Parties.

Cybersecurity requirements for essential energy stakeholders are aligned with EU legislation in five Contracting Parties but are legally binding for energy sector operators in only one Contracting Party.

EU-wide cybersecurity standards have been adopted by only half of the Energy Community Contracting Parties as national cybersecurity standards, while in the remaining half there has been only partial adoption.

In summary, for all Energy Community Contracting Parties, closing these gaps should be an imperative, as until this is done the overall country risks will remain at the same level.

RISK ASSESMENT RESULTS

Energy Community Contracting Parties have different levels of risks largely depending on their respective geopolitical situations.

The first group of countries consists of predominantly those from the Western Balkans – Albania, Bosnia and Herzegovina, Kosovo*, the Republic of Serbia, Montenegro and North Macedonia – all of which have small energy markets by EU standards and are coping with similar if not the same cybersecurity issues (risks, incidents). According to cybersecurity maturity level, the two most advanced countries in this group – Serbia and Montenegro – could contribute a great deal to the cybersecurity level of the overall region by actively cooperating with their neighbours and thus lowering the risk for the whole group. Once regional cooperation is established and extended with cooperating energy incident response teams with joint exercises and an early warning system, regional risks will be reduced to more acceptable levels.

---

[1] *This designation is without prejudice to positions of status, and is in line with UNSCR 1244 and the ICJ Opinion on the Kosovo* Declaration of Independence. Therefore, whenever Kosovo* is mentioned in this document, it is marked with an asterisk.*

The second group with higher risk levels consists of Georgia and Moldova, which are under the constant risk of cyber-war type incidents. These two countries require more investment in high-tech cyber defence and must engage very skilled professionals in order to achieve more significant progress in managing cyber risks.

The third group consists of Ukraine, which belongs to a separate risk category. The Ukrainian energy market is significantly larger and more complex than other Contracting Parties and of significant strategic interest not only to the EU but also to the USA and Russia. With Ukraine's cyber risks at critical levels, the country is managing them promptly and to the best of its capacity. Of course, as in the second group, Ukraine also needs further investment and to engage the best expert support in order to continue to make progress in addressing cybersecurity incidents. In addition, all neighbouring countries through collaboration and coordination must be promptly made aware of these risks and adjust their respective systems/processes to be able to handle the same level of risk.

RECOMMENDATIONS AND ROADMAP

Based on the recommendations at the Energy Community level and those developed for the Energy Community Contracting Parties, general recommendations for all Energy Community Contracting Parties are given below:

- 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.

Based on the risk analysis and impact of proposed measures, the study identified three distinctly different groups - Standard, Sensitive and High-Risk Contracting Parties - and proposed roadmaps for the implementation of the recommended measures.

2 Contents

3 Introduction

Energy infrastructures are complex systems which have physical, geographical, logical and, finally, cyber interdependencies with other critical infrastructures, e.g. transport, telecommunications, water, agriculture, health, finance, chemical industry and networks supporting the government, central and territorial entities, emergency services, as well as military- and civil defence. A disruption in the normal operation of critical energy infrastructures can have a negative cascading effect on other infrastructures, as well.

The Treaty establishing the Energy Community (EnC) provides instruments for the enhancement of the security of supply. However, cybersecurity is not explicitly recognized as an instrument for enhancing the security of supply and the NIS Directive is not part of the EnC acquis. The Permanent High Level Group (PHGL) of the EnC identified and acknowledged the necessity for building energy sector-specific cybersecurity capabilities at national and EnC level and for promoting a culture of risk management and incident reporting among electricity and gas system operators. To that end, PHGL recognized the need to explore the incorporation of the NIS Directive into the EnC acquis[2].

The legal framework and procedures for handling cybersecurity are still under development in the EnC Contracting Parties. A structured approach to regional cooperation is yet to be developed. However, there are regular meetings of the established working group (WG) which deals with cybersecurity issues in the SEE region under Regional Cooperation Council (RCC).

To promote a high level of security of network and information systems, as well as of critical infrastructures within the Energy Community, the Ministerial council of the EnC established the Energy Community Coordination Group or Cyber-Security and Critical Infrastructure ("CyberCG"). The aim of CyberCG is to facilitate the strategic cooperation and the exchange of information within the EnC, to develop trust and confidence, and to support achieving a high common level of security of network and information systems, as well as of critical infrastructures, within the EnC[3]. This Procedural Act also serves as a foundation for work conducted as part of this study and this report.

This report is based on the analysis of the collected information and the performance of a thorough risk assessment in order to provide an overview of the EU rules and regulations, legal and institutional frameworks, as well as available cybersecurity-relates standards. The analysis considered Contracting Parties, cross-border cybersecurity initiatives and mechanisms and multilateral or bilateral cybersecurity governance projects/technical assistance, education and training programs related to the cybersecurity and cyber threats and risks to which the energy sector in the Energy Community can be exposed.

---

[2] *Conclusions of the 49th PHGL, Vienna, 26.3.2018*

[3] *https://www.energy-community.org/dam/jcr:a9163c92-fb05-40c3-a74c-acca91fe94c1/PA_02_2018_MC-EnC_CSCG_112018.pdf*

3.1 Energy Community

The Energy Community is an international organisation dealing with energy policy and law. The organisation was established by an international treaty in October 2005 in Athens, Greece. The Treaty establishing the Energy Community brings together the European Union (EU), on one hand, and the Contracting Parties (CPs), namely Albania, Bosnia and Herzegovina, Georgia, Kosovo*[4], North Macedonia, Moldova, Montenegro, Serbia and Ukraine.

The activities of the Energy Community are administered by the Secretariat located in Vienna. Its tasks range from overviewing and enforcing the implementation process to implementing the Energy Community's budget – to which all Parties to the Treaty contribute – in accordance with the Work Program of the Energy Community.

Privileges and immunities of the Energy Community are laid down in the Agreement regarding the seat of the Secretariat of the Energy Community signed on 29 May 2007.

The Energy Community Treaty extends the European Union's energy policy and law to neighbouring countries. The principle objectives of the Energy Community are to create a regulatory and market framework that can attract investments for a stable and continuous energy supply. This paves the way for an integrated energy market, allowing for cross-border trade and integration with the EU market. The Energy Community also strives to enhance security of supply and competition, and to improve the environmental situation in its Contracting Parties.

3.2 Objectives of the Study

The main objective of the study is to assess and develop proposals for improving the energy-specific cybersecurity capabilities in the Energy Community at both the national and regional/pan-European levels within the interconnected power and gas systems. Key study goals based on specific objectives stipulated in the ToR[5] were identified, including:

- Identification of EU legal framework and EU-wide cybersecurity-standards for ICT products and services in the energy sector applicable at European Union level;
- Identification of cyber-security institutional frameworks, cross-border cooperation, multilateral/bilateral projects, standards, certifications and education and training programs in Contracting Parties (CP);
- Assessment of gaps between EU legal, institutional and cyber-security standards frameworks and CP legal, institutional and cyber-security standards frameworks;

---

[4] *This designation is without prejudice to positions on status, and is in line with UNSCR 1244 and the ICJ Opinion on the Kosovo* Declaration of Independence. Therefore, whenever Kosovo* is mentioned in this document, it is marked with an asterisk.*

[5] *TENDER DOCUMENTS for procurement of consultancy services for a study on Cybersecurity in the energy sector of the Energy Community, Vienna 24 July, 2018*

- Overview of cyber threats and risks to which the energy sector in the Energy Community can be exposed to;
- Propose measures, actions and organisation necessary to implement minimum common framework addressing the cybersecurity of critical energy infrastructure within the EnC; and
- Prepare recommendation and roadmap on how to align the certification schemes and procedures in the EnC with those applied in the EU and assess the impact of implementation of proposed measures.

In addition to the above objectives as per the ToR, the Study will wherever possible cover all applicable contents from the Annex to the Procedural Act6 from November 2018 and the relevant acquis indicated in the Annex – in particular in Item 5 (the tasks of the CyberCG), and Items 9 - 13 (specific activities).

3.3 Approach and methodology

The preparation of the cybersecurity readiness overviews and the identification of gaps between EU rules/standards and EnC CPs cybersecurity frameworks, is based on the consideration of the general cybersecurity aspects of the energy system. Moreover, the gap assessment criteria are based on the EU rules and standards. The application of EU rules and legal criteria serves as the basis for assessment of differentiated cybersecurity gaps (legal, regulatory, procedural, technology and resource/capacity related). Similar fit-gap assessment was completed at the EU Member States' level in 2019.

The study is carried out using a seven-step methodology (shown in Figure 1: Methodology supported by three workshops, fieldwork and four control points.

Figure 1: Methodology

---
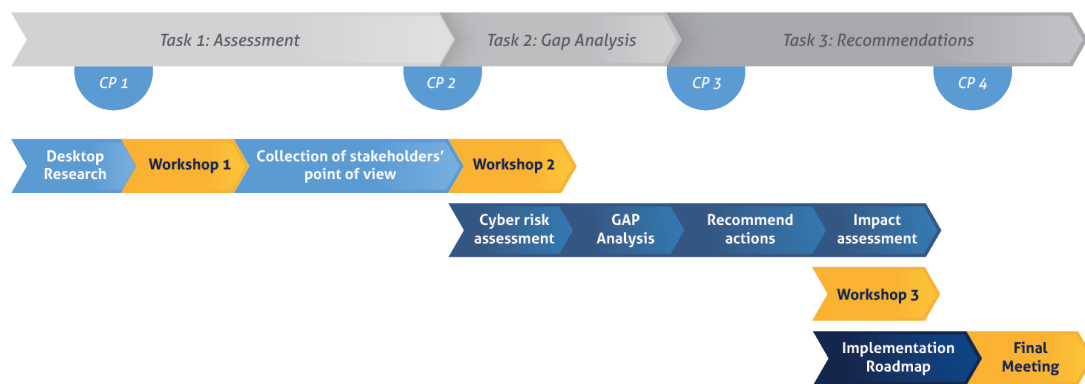
6 *Energy community cyber-security and critical infrastructure cooperation group (CyberCG), established by Procedural Act of Ministerial Council of the EnC 2018/PA/MC-EnC*

Taking into account that the architecture of energy systems, as well as that the maturity level of stakeholders could differ among the CPs, for the purpose of providing a standardized approach to the analysis, the stakeholders were categorized into three levels:

i)   national legislation and policy level encompassing competent authority for National cybersecurity strategy and implementation encompassing state wide energy sector related organisational structures (e.g. CSIRT)

ii)   national energy system physical level[7], encompassing national regulatory authorities, market operators and system transmission operators

iii)   energy system contractual level, encompassing distribution system operators.

Several methods were used for information collection in order to capture the insights and corroborate information about current status of legal and institutional cybersecurity frameworks applicable to the energy sector in the EnC. These methods include desktop research, workshops, questionnaires and interviews.

Overview per CP, as well as a summary overview presented in "Chapter 5 Overview, assessment and gaps of cybersecurity related institutional and legal frameworks in the energy sector of Contracting Parties" was prepared based on the collected and consolidated information according to the the responses on questionnaires for different stakeholders in the energy sector correlated with publicly available information.

The identification of key weaknesses, risks and potential exposure to cyber threats in the energy systems of the EnC CPs, as well as actors whose disruption by a cyber-incident might cause or have a significant disruptive effect on essential services in the energy sector was performed in two steps.

- In the first step, risks were assessed based on the energy sector stakeholder model described in the paragraphs i) to iii) above.
- In the second step, the CPs' specific risks were addressed based on the country specific information[8] and overview of energy stakeholders' cyber threats and risks Chapters from 6.2 to 6.10. Risk assessment methodology is laid out in the at the beginning of *"Chapter 6 Overview of cyber threats and risks for EnC ."*

---

[7] *Including rules and procedures applied in practice, data exchange between energy stakeholders, redundancy and backup principles, etc.*

[8] *From national risk assessment documents and strategies, amended with additional information from questionnaires.*

3.4 Abbreviations

Abbreviation	Description
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CERT	Computer Emergency Response Team
CHP	Combined Heat and Power
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CoE	Council of Europe
CIRT	Computer Incident Response Team
CP	Contracting Parties
CS	Cybersecurity
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial of Service
DSO	Distribution System Operator
EC	European Commission
ECI	European Critical Infrastructures
ECIP	European Critical Infrastructure Protection Contact Point as defined in the ECI, Article 10
EE	Energy Efficiency
EE-ISAC	European Energy - Information Sharing & Analysis Centre
E-ISAC	Electricity Information Sharing and Analysis Centre
EMP	Electromagnetic Pulse
EnCCI	Energy Community Critical Infrastructure
ENISA	European Union Agency for Network and Information Security
ENTSO-E	European Network of Transmission System Operators for Electricity
ENTSO-G	European Network of Transmission System Operators for Gas
ES	Essential services

Abbreviation	Description
ETSI	European Telecommunications Standards Institute
EU	European Union
FIRST	Forum of Incident Response and Security Teams[9]
ICS	Industrial Control Systems
ICT	Information and communications technology
IEC	International Electrotechnical Commission
III	Important Information Infrastructure[10]
IoT	Internet of Things
IP	Internet Protocol
ISACA	Information Systems Audit and Control
ISO	International Standardisation Organisation
IT	Information Technology
ITU	International Telecommunication Union
MIA	Ministry of Internal Affairs
MoD	Ministry of Defence
MoU	Memorandum of Understanding
NARUC	National Association of Regulatory Utility Commissioners
NATO	North Atlantic Treaty Organization
NCIRC	NATO Cyber Incident Response Centre
NIS	Network and Information Security
NRA	National Regulatory Authority
OECD	The Organisation for Economic Co-operation and Development
OES	Operator of Essential Services
OSCE	Organization for Security and Co-operation in Europe
OT	Operational Technology
SCADA	Supervisory control and data acquisition

---

[9] *FIRST is an international confederation of trusted computer incident response teams who cooperatively handle computer security incidents and promote incident prevention programs*

[10] *Defined in the Albanian Law No.2/2017 on Cybersecurity*

Abbreviation	Description
SEGRID	Security for Smart Electricity GRIDs
SOC	Security Operations Centre
SPoC	Single Point of Contact
SWOT	Strengths, Weaknesses, Opportunities, and Threats
TSO	Transmission System Operator
UCSI	Utility Cyber Security Initiative
UN	United Nations

4 EU legislation overview

The relevant cybersecurity legal framework in the context of the Energy Community encompasses Council of Europe conventions, EU legislation and EU-wide cybersecurity standards.

4.1 International conventions

The most important international convention in the area of cybersecurity is the Council of Europe Convention (CoE) on Cybercrime (called also the Budapest Convention). Although cybersecurity is not a key topic, CoE for the Protection of Individuals with regards to Automatic Processing of Personal Data should be mentioned especially in the relation with cross-border exchange of personal data.

4.1.1   Budapest Convention

The 2001 CoE on Cybercrime (Budapest Convention) is a legal framework of reference for combating cybercrime, including attacks against information systems. The Convention is signed by all CPs except Kosovo*[11]. The Budapest Convention requires parties: to adopt appropriate legislation against cybercrime; ensure adequate procedural tools to effectively investigate and prosecute cybercrime offenses; and to provide international co-operation to other parties engaged in such efforts.

ENISA defines any crime or criminal activity facilitated by or with the use of cyber space as cybercrime[12]. It is important to note, that cybercrime is not only limited to crimes specific to the internet (e.g. cyber-attacks), but also to online fraud and forgery as well as illegal online content, including sexual abuse material, incitement to racial hatred or terrorist acts, glorification of violence, terrorism, racism and xenophobia[13].

---

[11] *Kosovo* has not ratified the Convention on Cybercrime, but it is implemented through Law No.03/L –166 ON PREVENTION AND FIGHT OF THE CYBER CRIME.*

[12] *ENISA overview of cybersecurity and related terminology. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology*

[13] *European Commission. https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en*

4.1.2 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

The Convention is related to data protection and the legal protection of individuals with regard to the automatic processing of personal data and provides a mechanism of cooperation and sets rules in regard to the cross-border transfer of personal data.

4.2 EU Legislation

EnC Contracting Parties made legally binding commitments to adopt core EU energy legislation specifically with the adoption of the Energy Community Treaty and its »*acquis communautaire*«. In accordance with the Treaty article 25, amendments to the *acquis communautaire* can be implemented. Therefore, the Treaty and acquis can and are evolving when there is new legislation and regulation adopted on the EU level as well as when the need exists to update or replace older acts. This allows CPs to align their national legislative frameworks for energy sector with that of EU and create capabilities for optimal cooperation, participation and cross border trade on energy markets as well as data exchange.

4.2.1 NIS Directive

The directive on network and information security (NIS)[14], from August 2016, requires each Member State to establish a Computer Security Incident Response Team (CSIRT) and a competent national authority for NIS, and sets up a cross-EU cooperation group for strategic cooperation as well as a CSIRT Network for operational cooperation, among other provisions. The directive also ensures that information is shared between the private and public sectors and requires that the energy sector takes appropriate security measures and notify the relevant national authorities of serious incidents.

Based on the NIS Directive requirements the criteria for the assessment of CPs compliance as a set of queries laid out in the

have been developed. The criteria encompassed identification of essential services, definition of significant disruptive effect, adoption of relevant strategic documents, designation of competent national authorities and single point of contact for cyber security, computer security incident response teams (CSIRTs), security requirements for OES and cooperation on the national and international level.

---

[14] *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN*

Table 1: NIS Directive assessment

Identification of Operators of Essential Services (OES)

Was the identification of OES conducted? Is energy sector included? Is the list of operators available? Were the criteria for identification designated and adopted? Does it encompass all of the necessary subsectors? Have the criteria for assessment been designated based on the significance of the disruptive effect?

Significant disruptive effect

Has the identification of OES been conducted on the basis of significant disruptive effect or has the adopted criteria for identification been designated based on the significance of the disruptive effect?

Adoption of national strategy on the security of network and information systems

Did the CPs adopt national NIS strategy? Does the cyber security strategy include CI? Does the document define strategic and appropriate policies and regulatory measures for energy sector (as defined in NIS Directive Annex 2.)?

Does the strategy define governance framework, objectives and priorities? Does it define the responsible national bodies and roles? Does it list relevant actors for implementation of the strategy?

Does the Strategy define or recognize the need for public-private cooperation?

Does it define or recognize the need for education, awareness-raising and training programmes relevant for cyber security?

Does it define or recognize the need for risk assessment? Is there an established plan to conduct such activities?

National CS organisational framework

National competent authorities and single point of contact

Does the CP define national competent authority for the security of NIS covering energy sector?

Does the competent authority oversee the implementation of the strategy or legislative documents for energy sector? Is there a national single point of contact for security of NIS?

Does the single point of contact exercise cross-border liaison function and cooperate with foreign states? Does it report on the incidents regarding energy sector with other EnC members or CPs? Does it asses cross-border impact of incidents?

CSIRT

Is there a national CSIRT established or an energy sector specific CSIRT? Does CSIRT cooperate cross-border? What are the tasks of CSIRT?

ES providers security requirements

Did CPs develop regulations or measures for OES? What kind of regulations or measures are there? Do they define technical and organizational measures? Is there an obligation for OES to report incidents to national competent authority or CSIRT?

Standardisation

Do CPs adopt international and European standards and good practices? Are national standards in line with ISO 27001, 27002 and 15408-1? Are there any other implemented standards pertaining to cyber security?

4.2.2 ECI Directive

Directive 2008/114 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection sets out approach to the protection of critical infrastructures in the EU. The directive recalls for the identification of critical infrastructures EC, the disruption or destruction of which would have significant cross-border impacts. Such critical infrastructure should be

identified and designated. The evaluation of security requirements for such infrastructures should be done under a common minimum approach.

Based on the ECI Directive requirements we set criteria for the assessment of CPs compliance as a set of queries laid out in the *"Table 2: ECI Directive assessment"*. The criteria encompassed identification and designation of EnCCI and CI, operator's security plans, Security Liaison Officers, reporting and ECI protection contact point.

Table 2: ECI Directive assessment

Identification of EnCCI and CI
Was the identification of EnCCI or CI conducted? Is the list of operators available? Does it encompass all of the necessary subsectors? Have there been any bi/multilateral agreements regarding ECI identification or designation?
Criteria for identification of CI
Were the criteria for identification of EnCCI or CI designated and adopted? Is the identification conducted on cross-cutting criteria? Is the identification conducted based on essentiality, disruption or alternatives to the service in question? Was there a bi/multilateral identification process for EnCCI with possible cross border impact?
Operators security plans
Are operators' security plans defined in the legislation or regulation? Are the CI assets identified? If there is no regulation or legislation, do operators of CI have their own security plans? Are there sector specific regulations on security plans? Do operators have security plans pertaining to cyber security?
Security Liaison Officer
Is Security Liaison Officer defined in the legislation or regulation? Do operators of EnCCI or CI have designated person responsible for security if there is no legislation? Do operators of EnCCI or CI have established communication channels or procedures? Do Security Liaison Officers report cyber incidents?
Reporting
Is there an obligation pertaining to reporting to ECI/CI protection contact point? Has there been a threat assessment conducted? Has the threat assessment been reported to ECI/CI contact point? Has there been any risks, threats or vulnerabilities reported to the ECI/CI protection contact point? Is there a sector specific contact point for reporting of incidents, risks or vulnerabilities? Do operators have to report any other information or events?
ECI protection contact point
Has ECI/CI protection contact point been designated or established? Who is responsible entity for energy sector? Is there an energy sector specific protection contact point? Are responsible entities or protection contact points cooperating cross-border? What are the tasks of protection contact points?

4.2.3 Directive 2013/40/EU of the European Parliament and of the Council "On attacks against *information systems*"

Directive 2013/40/EU introduced new rules harmonising criminalisation and penalties for a number of offences directed against information systems, and in doing so, complemented the Budapest Convention. The directive focuses mainly on ensuring that the same offences are criminalised in all EU Member States and giving law enforcement authorities the means to act and to cooperate with one another, to establish a national point of contact and use the existing network of 24/7 contact points.

4.3 Energy Community Procedural Act related to cybersecurity

Cybersecurity of critical (information) infrastructure, especially in the energy sector, is becoming more important for the safety and security of energy production, distribution, transmission and storage, as well as for the stability of the single energy market. For the purpose of promoting high level of security of information systems and networks of critical infrastructure the Procedural Act on the ministerial council of the EnC on the Establishment of an Energy Community Coordination Group for Cyber-Security and Critical Infrastructure (2018/2/MC-EnC) was adopted by EnC with the aim to facilitate strategic cooperation and exchange of information.

The Procedural act established CyberCG coordination group for the purpose of information exchange, cooperation and communication with designated CSIRTs, CI security liaison officers and other stakeholders. CyberCG is a strategic body providing guidance for activities of CPs CSIRTs, sharing of information, good practices and experience among included stakeholders, assisting in building capabilities of EnC CPs for cybersecurity and protection of EnCCI/CI, discussing as well as evaluating capabilities and preparedness of EnCCI/CIs, collecting information on incidents, incident response and mitigation, exchange of information and best practices for identification of EnCCI and CII as well as their assessments and evaluation of possible cross-border and cross-sector impacts. Among aforementioned tasks, CyberCG develops common methodological guidelines for risk assessments and analysis of EnCCI/CI in energy sector, supports owners of infrastructure and other stakeholders with providing access to best practices, methodologies and trainings on technical issues and security of critical infrastructure.

Energy Community critical infrastructure (EnCCI) means critical infrastructure located in CPs, the disruption or destruction of which would have a significant impact on at least two CPs and/or EU Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure.

Along with the operational and administrative activities, the Procedure act sets basis for implementation of provisions from NIS and ECI Directives, General protection Regulation as well as Directive On Attacks against information systems. Based on the Energy Community Treaty article 25, the NIS and ECI Directives as well as GDPR regulation could be amended to the *acquis communautaire* and contribute to the security of supply in the single regulatory space in the Energy Community.

The Procedural Act (2018/2/MC-EnC) defines requirements for Contracting Parties to:

- Designate and report national competent authorities to Energy Community Secretariat
- Designate and report a national cyber security SPoC and CI protection contact point to Energy Community Secretariat.
- Designate and report national or energy sector specific CSIRT that covers energy sector to Energy Community Secretariat
- Designate Security Liaison Officer for each EnCCI in the Contracting Party
- Report to CyberCG, CSIRT Network or EnC Secretariat on adoption of national NIS strategies and other instruments on protection of CI and on the implementation of NIS and ECI Directives
  - o Identification process and criteria for significance of disruption
  - o Identification of CI in the Contracting Party, its security measures and operator security plans implementation in accordance with ECI Directive article 5.
  - o Operators security plans and notification requirements of EnCCI
  - o Security requirements for energy trading and balancing services, digital service providers and electronic communications operators necessary for energy sector CI functionality.

4.4 Energy specific EU policies and recommendations

Cybersecurity in energy sector becoming in EC focus due to undergoing changes in the sector as well as increasing degree of digitalization what makes the new digitized energy grid vulnerable to attacks.

EC promotes information sharing at a higher-level via dedicated events, and fosters best practices among EU Member States, under a dedicated work stream on energy of the Cooperation Group established by the NIS Directive. This work stream brings together Member State Authorities from the cybersecurity and the energy side. Further, cooperation with the specialized entities such as the European Energy Information Sharing and Analysis Centre on cybersecurity (EE-ISAC) has also been enhanced in last year(s).

The EC has addressed question of cybersecurity in energy sector also through *Clean energy for all Europeans package*[15] among which the most important are:

- The new regulation on electricity on risk-preparedness in the electricity sector mandates[16] EU Member States to develop national risk preparedness plans and coordinate their preparation at regional level, including measures to cope with cyber-attacks.

- The recast of Electricity Regulation gives a mandate to the EC to develop a network code on cyber security for the electricity sector in order to increase its resilience and protect the grid.

4.4.1 Gas sector related cybersecurity legislation

Considering gas sector specific recommendations and legislation have to be noted that Security of Gas Supply Regulation: Regulation (EU) 2017/1938[17] deals also with gas supply shortages caused by a number of risk factors, among which are also cyber-attacks and events like war, terrorism and sabotage, which also encompass the cybersecurity aspects.

The legislation sets out rules for regional risk assessments and emergency planning, and introduces a mechanism for mutual assistance in the event of a severe gas supply crisis, based on the principle of solidarity which relates to the cybersecurity domain as well.

---

[15] *https://op.europa.eu/en/publication-detail/-/publication/b4e46873-7528-11e9-9f05-01aa75ed71a1/language-en?WT.mc_id=Searchresult&WT.ria_c=null&WT.ria_f=3608&WT.ria_ev=search*

[16] *https://eur-lex.europa.eu/eli/reg/2019/941/oj*

[17] *https://eur-lex.europa.eu/eli/reg/2017/1938/oj*

4.4.2 EC cybersecurity energy sector related recommendations

In April 2019 EC published *The Recommendation on Cybersecurity in the Energy Sector*[18] recently adopted by the EU Commission focused on the OES identified according to NIS directive provides an overview of the main issues related to cybersecurity in the energy sector. Key energy sector related cybersecurity recommendations are provided for three key segments:

- Real-time requirements of energy infrastructure components:

- Cascading effects - potential outage effects to other parts of the grid:

- Combination of legacy and state of art technology.

Detailed recommended actions and guidelines are given especially for network operators are given for each segment.

4.4.3 ENTSO-E and ENTSO-G cybersecurity activities and recommendations

ENTSO-E and ENTSO-G recognized the need for building capabilities to address cybersecurity issues and began developing approaches to strengthen cybersecurity of TSOs and increase safety and security of supply and transmission of energy.

ENTSOG[19] started collaborating in GIE (Gas Infrastructure Europe) Cybersecurity Taskforce to build a common understanding of key areas of importance for strengthening cybersecurity of network code for the gas sector. ENTSO-G started developing solutions for data communication harmonization which introduces cybersecurity measures for security of information and data. ENTSO-G has established the Smart Grid Task Force to evaluate the situation of cyber security in the smart grid environment. ENTSO-G programme on cybersecurity[20] includes the development and implementation of policies, controls and governance that balances the need to protect ENTSO-G and its members against cybersecurity attacks. 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, focus on Information sharing about Cyber Security incidents/threats and nominate Task Force to address the question related to operational security on SCA and smart meeting level. [21]

EnC CPs who are observers in ENTSOG[22]: Albania, Bosnia and Herzegovina, Republic of North Macedonia, Moldova, Ukraine

---

[18]

https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2 400_final.pdf

[19] *ENTSOG – Draft Plan for 2020. https://www.entsog.eu/sites/default/files/2019-08/Draft%20Annual%20Work%20Programme%20%28AWP%29%202020%20for%20public%20consultation_0.pdf*

[20] *ENTSOG – Members. https://www.entsog.eu/members*

[21] CEER Cyber Security Session 1, 21 June 2019. https://www.ceer.eu/documents/104400/-/-/2c424b85-e79a-13b4-6265-a7eb0c6dc8c1

[22] *ENTSOG – Members. https://www.entsog.eu/members*

ENTSO-E[23] recognized the need to protect TSOs' information-communication systems and networks from cyber-attacks. It has been a platform for best experience and practice sharing between TSOs' for strengthening of cybersecurity. With adoption of CGM Security Plan it addressed cybersecurity recommendations for OPDE platform which encompasses a number of EnC Contracting Parties as well, however it is not available for public. ENTSO-E is planning to address risk management and development of guidelines and recommendations for IT architecture, training and resilience building in the future. ENTSO-E is in the process of elaborating "cyber-security strategy" (publicly not available). Among other activities ENTSO-E supports operational training and organizes practical "red-blue team" exercises for TSOs' operational staff.

EnC CPs who are members of ENTSO-E[24]: Albania, Bosnia and Herzegovina, Montenegro, Republic of North Macedonia, Republic of Serbia

4.4.4 Network Code on Cybersecurity

The Smart Grids Task Force has been doing preparatory on work since 2017, and released its second interim report in July 2018[25].

The implementation of a network code on cybersecurity could aims to provide provide components designed for the cybersecurity needs of the energy sector:

- Set-up of an early warning system in Europe for the energy sector

- Cross-border and cross-organizational risk management in the EU

- Minimum Security Requirements for critical infrastructure components

- Minimum Protection Level for energy system operators

- European Energy Cybersecurity Maturity Framework for Operator of Essential Services

- Supply Chain Risk Management for Operator of Essential Services

Recommended structure of the codes can be seen on the *"Figure 2: Recommended Structure for the Network Code on Cybersecurity".*

---

[23] *ENTSO-E – Annual Work Programme 2019.* *https://consultations.entsoe.eu/entso-e-general/annual-work-programme-2019/supporting_documents/l_entsoe_AWP_2019_09.pdf*

[24] *ENTSO-E – Member Companies. https://www.entsoe.eu/about/inside-entsoe/members/*

[25] https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_2nd_interim_report_final.pdf

Figure 2: Recommended Structure for the Network Code on Cybersecurity
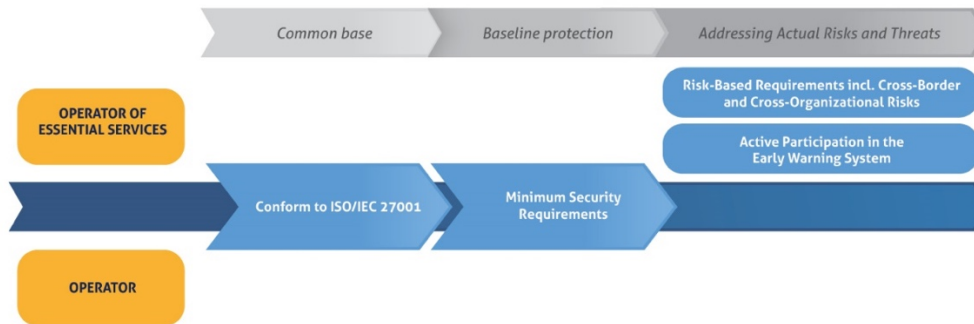
4.5 EU cybersecurity standards

There are eight (8) published European[26] cybersecurity-standards, of which "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 for the purpose of this study:

- **ISO/IEC 27001:2017 Information security management systems**[27] is one of best known ISMS standards for describing systematic approach to management of sensitive information in organizations, risk management and security aspects of people, processes and IT systems. Standards help organizations to keep their assets secure and meet legislative and organizational security requirements for certification of ISMS.
- **ISO/IEC 27002:2017 Code of practice for information security controls**[28] allows organizations to assess and prepare information security management practices including selection, implementation and management of information security controls to assess risk environment(s).

---

[26] *EU standards are developed and agreed by three officially recognized European Standardization Organizations: the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI). For a list of valid cybersecurity standards see https://standards.cen.eu/dyn/www/f?p=204:32:0::::FSP_ORG_ID,FSP_LANG_ID:2307986,25&cs=1F4A71C19873519CC81C4 B2C031CF3CF5*

[27] *ISO/IEC 27001. https://www.iso.org/isoiec-27001-information-security.html*

[28] *ISO/IEC 27002. https://www.iso.org/standard/54533.html*

4.5.1   EU cybersecurity candidate standards

Although there is no energy related specific European cybersecurity-standard, "ISO/IEC 27019:2017 Information security controls for the energy utility industry" and ISO/IEC 15408 family of standards (Information technology - Security techniques - Evaluation criteria for IT security Parts 1-3) are used as a baseline in this study as they are under drafting by the CEN/CLC/JTC 13 Work programme[29]. Voting on the adoption is forecasted for the year 2021. ISO 27019 was also identified in the ENISA study related to smart grid security measures[30] as a good practice in the energy sector applying ISO 27002 requirements to process control systems used in the energy sector for controlling and monitoring the production, generation, transmission, storage and distribution of electric power, gas and oil, and for the control of associated supporting processes.

ISO/IEC 27019 Information security controls for the energy utility[31] industry provides guidance based on the ISO/IEC 27002 security controls tailored for use in the energy utility industry for purposes of controlling and monitoring of generation, production, transmission, storage and distribution of electricity, gas, oil and heat as well as control of necessary supporting processes.

ISO/IEC 30111 Vulnerability handling processes[32] provides guidance for requirements, recommendation and mitigation process of potential vulnerabilities of critical or supporting products and services.

ISO/IEC 15408-1, 2 and 3[33] Encompass a three-part collection of **Evaluation criteria for IT security**. The standards contain set of requirements for assessment of security functions of IT products, systems and assurance measures during security evaluation.

- **15408-1** is covering introduction and **general model for assessment of IT security** with general concepts and principles for evaluation. It contains a general model for evaluation and strategic objectives for selection and definition of organizational IT security requirements for products and systems.
- **15408-2** is covering **evaluation of security functional components** with guidelines to create functional components of the target of evaluation including components, families and classes.
- **15408-3** is covering evaluation of security assurance with guidelines for assessing, defining and establishing a set of assurance components to evaluate assurance requirements of organizations and products, services and systems.

---

[29]*https://standards.cen.eu/dyn/www/f?p=204:22:0::::FSP_ORG_ID,FSP_LANG_ID:2307986,25&cs=1F4A71C19873519CC81C4B2C031CF3CF5*

[30] *ENISA: Appropriate security measures for smart grids Guidelines to assess the sophistication of security measures implementation [2012-12-06].*

[31] *ISO/IEC 27019. https://www.iso.org/standard/68091.html*

[32] *ISO/IEC 30111. https://www.iso.org/standard/69725.html*

[33] *ISO/IEC 16408-1, 2 and 3. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec-standard-15408*

5 Overview, assessment and gaps of cybersecurity related institutional and legal frameworks in the energy sector of Contracting Parties

Introduction to this chapter covers an overview and summary assessment of CPs ECI and NIS implementation and readiness of national cybersecurity related legislation and organisational structures for the inclusion of energy sector provisions foreseen in the EU legislation as well as an overview of CPs organisational structures and cybersecurity provisions in view EnC Procedural Act (2018/2/MC-EnC)

Following the introduction part, a detailed overview, assessment and description of gaps between national and EU legislation and cybersecurity standards for each CP and have the same structure:

- CP overview and assessment encompasses a brief overview and assessment of energy-specific and general cybersecurity legal and organisational framework
- SWOT analysis
- Overview of cybersecurity legislative and organisational framework and standards
- Description and assessment of national legislation, starting with cybersecurity relevant strategies and action plans legislation against cybercrime followed by energy sector cybersecurity legislation and description of cybersecurity authorities
- Cybersecurity cooperation, initiatives and overview of education and training programmes
- The last page of every CP overview contains a gap assessment against EU legislation and EU-wide standards

Overview of CPs cybersecurity organisational and legislation in view of EU legislation

EU cybercrime legal framework (Budapest convention) forms a basis for cybersecurity legislation by defining criminal law offences, connected provisions, and thus enabling prosecution of cybercrime actors. The Budapest Convention is signed by all CPs except Kosovo* however it should be noted that Kosovo* did transpose all necessary provisions and harmonized the national legislation.

Critical infrastructure[34] identification criteria foreseen in the EU legislation as a prerequisite for ECI designation are present in the national legislation only in two (2) CPs, process to develop criteria started in

---

[34] *European Critical infrastructure (ECI) and/or Energy Community Critical Infrastructure (EnCCI)*

additional three (3) CPs. Two (2) CPs already designated critical infrastructure and in two (2) the designation is under way. It should be noted that in all four (4) CPs that designated CI or started the process of designation, both electricity and gas sectors are considered. The list of designated CIs is classified in two (2) CPs.

In comparison with critical infrastructure identification criteria the situation is significantly more developed regarding the criteria for the identification of Essential Services (ES) [35], which are already established or in preparation in practically all CPs. However, only one (1) CP designated Operators of Essential Services (OES) and three (3) have started the designation process. The only observed difference between electricity and gas sector is that that CII/OES designation criteria in Albania does not include gas subsector.

National strategies on the security of network and information systems[36] as a crucial cybersecurity building block has been developed in seven (7) CPs and are mostly aligned with the EU cybersecurity framework however energy sector is referenced only in three strategies.

Designation of strategic and operational/tactical contact points that is important for prevention and efficient response to cyberattacks has been competed in seven (7) CPs and is under way in another two (2). It should be noted that contact points for energy sector are explicitly defined only in two (2) CPs.

Cybersecurity requirements for essential energy stakeholders[37] are aligned with EU legislation in five (5) CPs but in only one (1) there is legally binding for energy sector OES.

EU-wide cybersecurity standards are as National cybersecurity standards adopted by four (4) CPs and partially and partially adopted by four. The following pages contains detailed assessment and description of gaps between national and EU legislation and standards for each CP an encompassing:

- CP overview and assessment encompassing a brief overview and assessment of energy-specific and general cybersecurity legal and organisational framework
- SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis
- Overview of cybersecurity legislative and organisational framework and standards
- In-depth description and assessment of national legislation, starting with cybersecurity relevant strategies and action plans legislation against cybercrime followed by energy sector cybersecurity legislation and description of cybersecurity authorities. Cybersecurity cooperation, initiatives and overview of education and training programmes is provided at the end.
- Gap assessment against EU legislation and EU-wide standards.

---

[35] *Critical Information Infrastructure (CII) and/or Operators of Essential Services (OES).*

[36] *Study is referring to the scope strategy foreseen in NIS directive.*

[37] *CI owners/operators and operators of essential services (OES).*

Cybercrime legislation

Budapest convention is transposed to local legislation in all CPs but some of them are already in the process of planning local legislation changes for further alignment. In

Figure 3: Planned amendments of cybercrime *legislation* an overview and assessment of on-going or planned activities related to transposition of EU wide cybercrime legislation in the national legislative framework is provided.
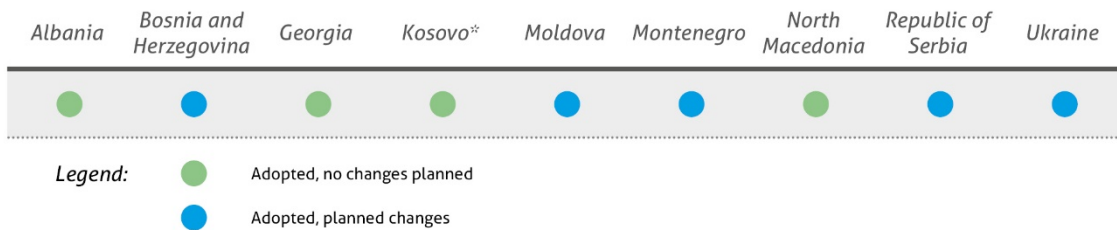
Albania	Bosnia and Herzegovina	Georgia	Kosovo*	Moldova	Montenegro	North Macedonia	Republic of Serbia	Ukraine
🟢	🔵	🟢	🟢	🔵	🔵	🟢	🔵	🔵

Legend: 🟢 Adopted, no changes planned

🔵 Adopted, planned changes

Figure 3: Planned amendments of cybercrime legislation

Identification of CI operators and OES

Starting point for the cyber protection of CI and ES is the identification process. Criteria for identification of ECI/EnCCI are present in the national legislation in only two (2) CPs with no differences related to the criteria definition between electricity and gas sectors. Per CP overview is provided in Figure 4: CI identification criteria (Electricity and Gas).

	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
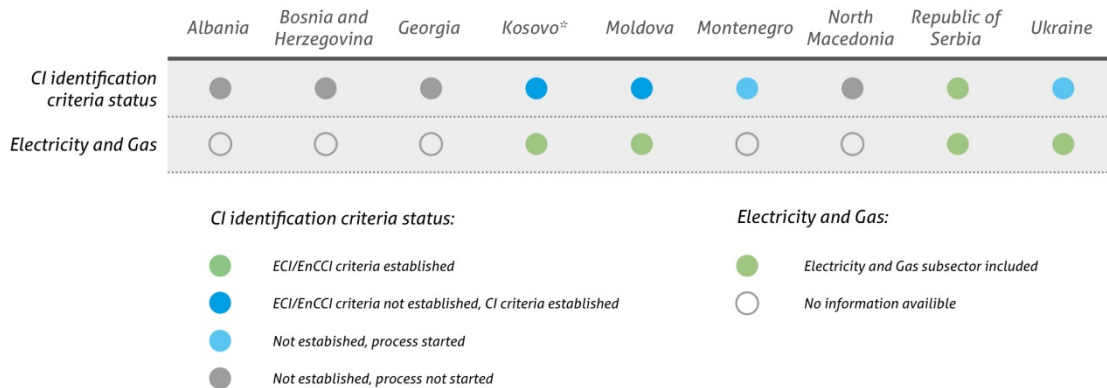
⚪ No information availible

Figure 4: CI identification criteria (Electricity and Gas)

_____

Taking into account the lack of criteria in the legislation, it is logical that CI is designated in only two (2) CPs with the designation encompassing energy sector in both cases (electricity and gas). Per CP overview is provided in Figure 5: CI designation (Electricity and Gas).

Figure 5: CI designation (Electricity and Gas)

_____

The situation is significantly better when considering the criteria for identification of ES which are already established or in preparation in more than half of the CPs. There is no difference between electricity and gas sectors with CII/ES identification criteria in CPs, except in Albania, where relevant legislation is laid out only for Electricity sector. Per CP details are represented in Figure 6: Essential services identification criteria (Electricity and Gas).
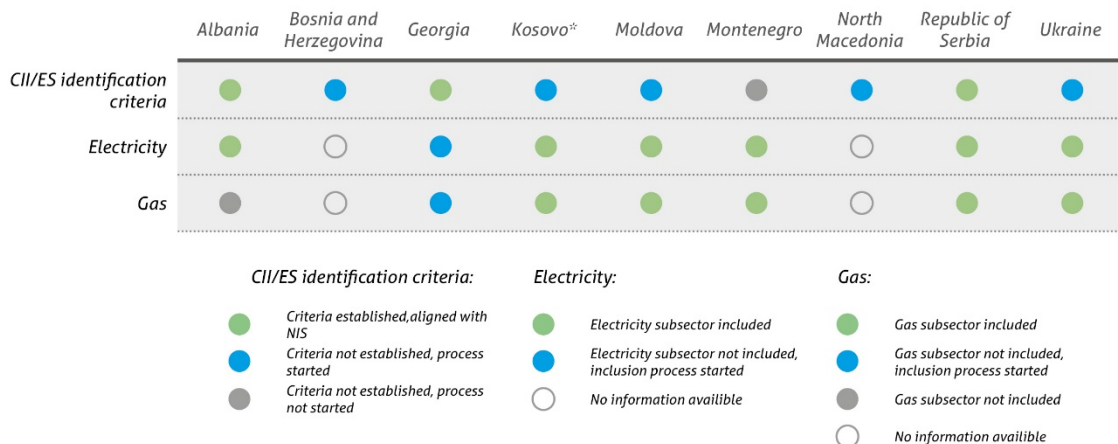

Figure 6: Essential services identification criteria (Electricity and Gas)

_____

Operators of Essential Services (OES) are designated in only one (1) CP, but even in this single case electricity or gas operators are not included.
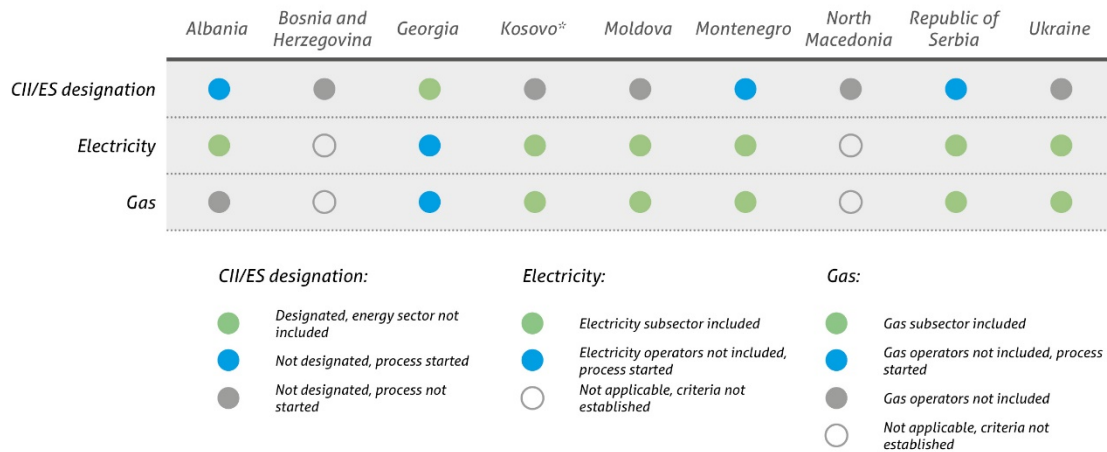

Figure 7: Designation of OESs

National NIS strategy

National strategy covering requirements of NIS directive related to national cybersecurity strategies is adopted in seven (7) Contracting parties and under development in the remaining two (2). Energy sector is considered only in the strategies of three (3) CPs. Situation per CP is represented in Figure 8: Alignment of national strategies with NIS strategy related requirements.

Figure 8: Alignment of national strategies with NIS strategy related requirements

National Cybersecurity Authorities: Contact points

Cybersecurity incidents coordination and reporting contact points are established in seven (7) Contracting Parties, two (2) CPs started process for the definition of contact points. However, contact points for energy sector are established only in two (2) CPs, Per CP status is represented in the Figure 5: CI designation (Electricity and Gas)
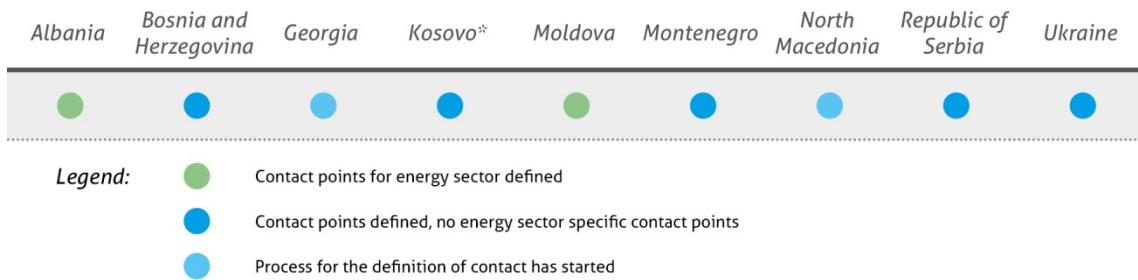
Albania	Bosnia and Herzegovina	Georgia	Kosovo*	Moldova	Montenegro	North Macedonia	Republic of Serbia	Ukraine
🟢	🔵	🔵	🔵	🟢	🔵	🔵	🔵	🔵

Legend:
🟢 Contact points for energy sector defined

🔵 Contact points defined, no energy sector specific contact points

🔵 Process for the definition of contact has started

Figure 9: Designation of a strategic and operational/tactical contact points

Security plans and requirements

Legislation provisions related to contents of OESs' security plans are in six (6) Contracting Parties aligned with NIS requirements, but only in one (1) are these provisions also applicable to energy sector. Per CP status is represented in
Figure 10: Alignment of requirements related to OES security plans with relevant NIS requirements.
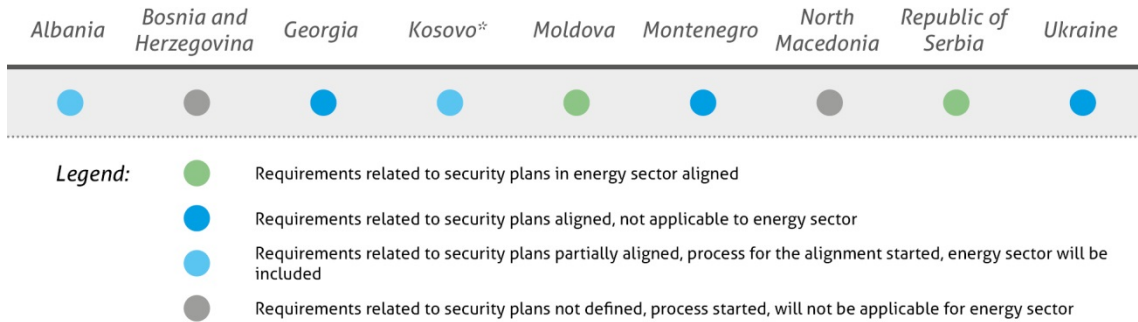
Albania	Bosnia and Herzegovina	Georgia	Kosovo*	Moldova	Montenegro	North Macedonia	Republic of Serbia	Ukraine
🔵	⚪	🔵	🔵	🟢	🔵	⚪	🟢	🔵

Legend:
🟢 Requirements related to security plans in energy sector aligned

🔵 Requirements related to security plans aligned, not applicable to energy sector

🔵 Requirements related to security plans partially aligned, process for the alignment started, energy sector will be included

⚪ Requirements related to security plans not defined, process started, will not be applicable for energy sector

Figure 10: Alignment of requirements related to OES security plans with relevant NIS requirements

_____

Standardization process

EU wide cybersecurity standards are adopted as national standards in four (4) CPs in five (5) are partially adopted or are in the process of adoption. Per CP situation is represented in Figure 11: EU cybersecurity standards adoption in Contracting Parties. More details can be found in the following pages
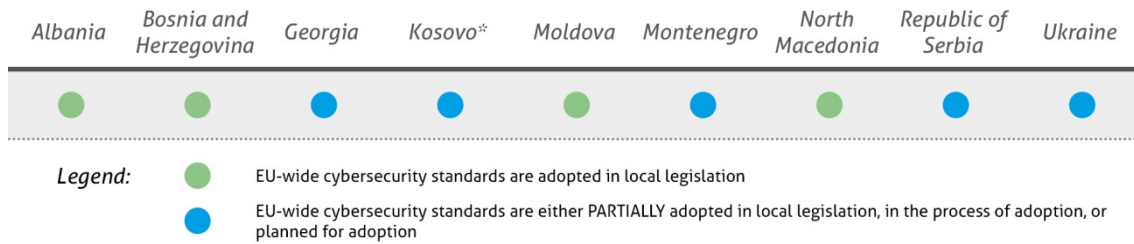
Figure 11: EU cybersecurity standards adoption in Contracting Parties

_____

Overview of CPs organisational structures and cybersecurity provisions in view of EnC Procedural Act (2018/2/MC-EnC)

In this section provides the assessment of compliance with the requirements of EnC Procedural Act. PA requirements encompass requirements related to cybersecurity structures in CPs and requirements on the reporting about adoption of national NIS strategies and other instruments on protection of CI and implementation of ECI and NIS directives. As the CPs are not obliged to implement the abovementioned ECI and NIS directives, procedural cross-border reporting has not been identified so the assessment of the current situation in the CP (NIS and ECI transposition) is given.

The current state of designation of organizational foreseen in the PA:

- National Competent Authority for Cyber Security is established in seven (7) CPs and process for designation is started in two (2).
- NIS SPoC (Cybersecurity contact points) for energy sector are designated in two (2) CPs (Albania and Moldova), while cybersecurity contact points (not energy specific) are designated in five (5) CPs and process for designation is started in the rest CPs (2).
- CI protection contact point is established in two (2) CPs (Moldova and Republic of Serbia), while process for designation is started in the rest (7).
- CSIRTs are established in eight (8) CPs while one (1) is in the process of establishment. While there is no energy specific CSIRT, all established national CSIRTs cooperate with operators of CI and OES in the energy sector.
- Security Liaison Officer
- One of the requirements set by the Procedural Act is, that CPs should designate Security Liaison Officers for cooperation with national authority. Requirements for Security Liaison Officers were legislatively defined in Moldova, Kosovo*, Serbia and Ukraine, while in other CPs such requirement was not formally established.

More detailed information on Contracting Parties' energy sector cybersecurity organisational structures alignment with the Procedural Act is represented in the "

Figure 12: Assessment of organizational structures"

| Assessment of 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

Figure 12: Assessment of organizational structures

Assessment of current state of adoption of national NIS strategies and other instruments on protection of CI (foreseen in PA):

- National NIS strategy that encompass references to energy sector is adopted in three (3) CPs, in four (4) CPs is adopted NIS strategy that does not explicitly reference energy sector while in two (2) CPs process for the development of NIS is under way. See Figure 8: Alignment of national strategies with NIS strategy related requirements
- National CI protection strategy – no strategic documents pertaining to protection of CI were identified. However, there are legislative documents setting recommendations and requirements for CI and OES. Four (4) CPs adopted relevant legislative documents (Kosovo*, Moldova, Serbia and Ukraine). See Figure 4: CI identification criteria (Electricity and Gas).
- CI and ES identification process:
    - CI is designated according to criteria aligned with ECI Directive in two (2) Contracting Parties, in two (2) is designation process under way. In five (5) CPs CI is not designated and designation process has not yet started. See Figure 5: CI designation (Electricity and Gas).
    - CII designation according to criteria aligned with NIS Directive has not been conducted in any CP, while in one (1) CP the designation has been conducted without energy sector, in

three (3) CPs the process has started, while in five (5) CPs the process has not yet started. See *"Figure 7: Designation of OESs"*.

- o CI criteria for identification is aligned with ECI Directive in one (1) Contracting Party, in two (2) only CI criteria is established, in one (1) the process has started and in four (4) the process has not started. See Figure 4: CI identification criteria (Electricity and Gas).
- o CII identification criteria aligned with NIS Directive is adopted in three (3) Contracting Parties, in five (5) the creation of criteria is underway. See Figure 6: Essential services identification criteria (Electricity and Gas)
- o CI/CII identification criteria are based on the significance of the disruption in six (6) CPs. Rest of the CPs did not develop criteria for identification of CI, CII or OES.
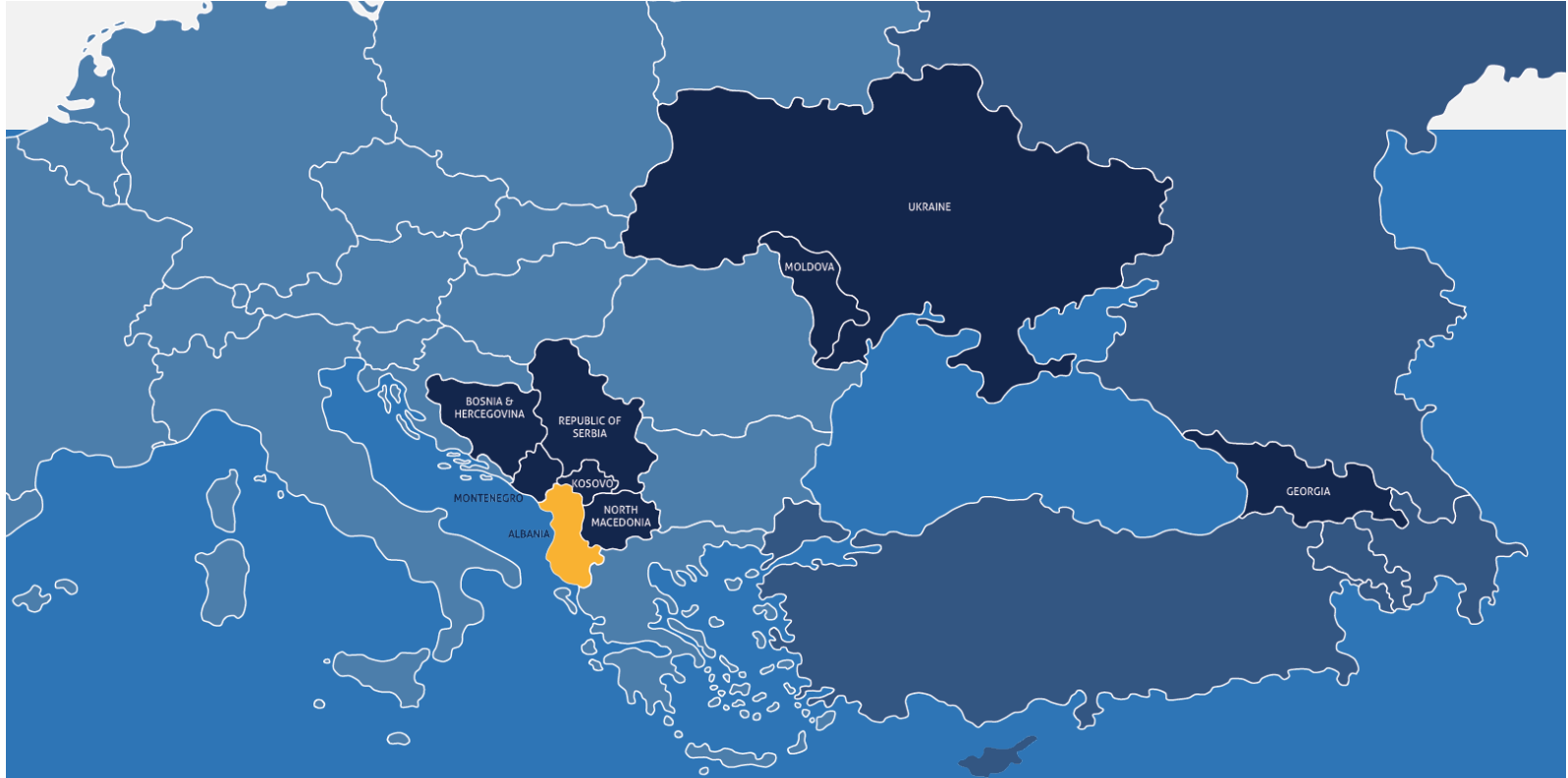
5.1 Albania

Albania made significant progress in cybersecurity in recent years. The Law on Cyber Security together with supporting regulations and decisions adopted on the basis of the "Digital Agenda of Albania 2015-2020" and "Policy paper on Cyber Security 2015–2017" provides a sound basis for further improvement of critical energy infrastructure protection.

The adopted legislation is focused on the critical information infrastructure and transposed the majority of NIS directive requirements into national legislation. Electricity TSO SCADA systems, DSO network between control centre and control points and SCADA monitoring and control systems are designated as CII. Identification of energy sector CII/ES operators that should be performed based on the adopted methodology has not been concluded. Although there is no explicit definition of criteria for the determination of a significant disruptive effect, impact-based criteria for the identification of CII can be used as an alternative.

It should be noted that existing legislation is covering only electricity critical information infrastructure while the gas sector is not mentioned in the legislation.

According to the National Authority for Electronic Certification and Cyber Security (NAECCS) Regulation on the content and method of documenting security measures CII/ES are obliged to perform risk assessment and create measures and procedures to manage incidents, risks and threats. The Energy sector operators recognised the importance of international standards (ISO 27001 standards, ENISA's recommendations) and are considering or implementing them. The Albanian TSO has started preparing internal information protection rules and adopting guidelines.

ECI directive provisions are not transposed to national legislation. Consequently, the identification of energy infrastructure the disruption or destruction of which would have a significant impact on neighbouring countries has not been conducted.

According to the Final report on the implementation of Policy Paper on Cybersecurity 2015-2017 all strategic goals and objectives pertaining to CII and energy sector have been fulfilled with the exception of /ES operators in 2019.

5.1.1 SWOT analysis

S

STRENGTHS

Proactive approach to the field of cybersecurity - it recognizes the importance of the security of information - communications technology and deems cyberattacks one of the highest risks in its National Security Strategy and already transposed the majority of NIS requirements to national legislation.

Constantly improving cybersecurity environment

W

WEAKNESSES

Existing legislation is covering only critical information infrastructure in the electricity subsector of the energy sector (gas subsector is not mentioned in the legislation), there is no legislation related to critical infrastructure and potential impacts to neighbouring countries.

Difficult access to adequate training and associated funding for these initiatives. Non-technology oriented educational system

O

OPPORTUNITIES

Although CII operators in the energy sector are not yet designated as foreseen by the regulation, electricity operators of CII are in the process of the implementing the ISO 27001 standard as well as following ENISA recommendations. These initiatives could be reinforced with EnC coordination. The business community recognises the importance of cybersecurity

T

THREATS

NAECCS, as designated National authority for CS, SPOC and as national CSIRT may face resourcing issues. Without adequate resources, this could lead to the risk that NAECCS would not be able to effectively separate operational and strategic tasks. Lack of cooperation between public and private sector. Upgrade of infrastructure and control systems at energy operator premises is not progressing in pace with state-of-the-art cybersecurity requirements

5.1.2 European Critical Infrastructure and Essential Services legislation requirements

Identification of EnCCI and ES

The Law on Cybersecurity does come with certain drawbacks, as it does not go into detail about the criteria set for critical or important infrastructure. It does designate NAECCS to carry out preparation of criteria. NAECCS has developed methodology criteria for identification of operators of CII, however gas sector is not included. The responsible Ministries designate critical or important infrastructure in their respective sector and amended the list. Decision no. 222 defined all CII and III by sectors and not specifically for the subject except in certain cases. For electrical energy sector TSO and DSO SCADA monitoring and control systems are listed as critical infrastructure but the list of operators is under development and not publicly available.

| *Decision no. 222, 26.4.2018* | *Lead: Council of Ministers* |

Criteria for CI designation and criteria for significant disruptive effect

Criteria for the identification of CII in the Electricity subsector of Energy sector (TSO/DSO) are defined based on the significant disruptive effect (one or more criteria met):
- 39,000 individuals are influenced,
- incident causes disconnection for intervals longer than 24 hours,
- financial impact is more than 3.3 million Lek (27,300 €)

| *Methodology for the identification and classification of CI* | *Lead: NAECCS[38]* |

National NIS strategy

Policy Paper on Cyber Security 2015-2017 defines the need for identification of CII, public-private partnership, reporting obligations and implementation of measures.

| *Policy Paper on Cyber Security 2015-2017* | *Lead: NAECCS* |

New strategy is in the process of adoption for timeframe 2019-2022.

| *For period: 2019-2025* | *Lead: NAECCS* |

National CS organisational framework

Energy sector contact point for the coordination of CII protection with other states is not established. Law on Cybersecurity defines NAECCS as National authority for CS, SPoC and as national CSIRT. NAECCS is responsible for definition of cybersecurity measures and to cooperate with energy sector operators. NAECCS has also jurisdiction for cross border CS cooperation including reporting of incidents.

| *Law on Cybersecurity, 2017* | *Lead: Ministry of Infrastructure and Energy[39]* |

CI operators shall assign personnel to the roles of Information Security Manager and Cyber Security Specialist. Regulation also defines their responsibilities related to ISMS and reporting of incidents.

| *Law on Cybersecurity, Regulation (no. 22) on the content and method of documenting security measures, 26.4.2018.* | *Lead: NAECCS* |

---

38 NAECCS, Papa Gjon Pali II Street, No. 3, Tirana, Albania.

39 Ministry for Infrastructure and Energy, Rr. Abdi Toptani 1, Tirana.

CI operators and ES providers security requirements

Law on Cybersecurity oblige energy sector CI/ES operators to implement technical and organizational security measures and establish incident reporting procedures. NAECCS has according to the Law defined the content of operators' security plans in more detail encompassing technical and organizational measures and asset management procedures. Requirements for operators' security plans are following EU and international standards and good practice.

Law on Cybersecurity. Regulation (no. 22) on the content and method of documenting security measures, 26.4.2018.   *Lead: NAECCS*

Standardisation

Albania adopted international ISO 27001, 27002 and 15408-1 standards as local standards (SSH).
CII in the energy sector are not obliged to follow them, however requirements set forth in Regulation 22 follows ISO 27002 guidance. According to the information provided by NRA the electricity TSO is implementing ISMS based on the ISO 27001 requirements.

Lead: General Directorate of Standardization; NAECCS

Besides the interconnections to CPs Kosovo* and Montenegro, Albania has interconnections of electricity energy system to EU Member States with possible cascading effects to Greece. The existing major entities of bulk power systems are in process of being upgraded with IP-based communication infrastructure over the past decades. These interconnected entities have a profound impact by cyber manipulation, either locally, regionally, or continent-wide. The manipulation using a compromised local control system can impair system operation due to the potential impacts on the physical system. The transmission line with Greece accounts for large share of Albania's electricity imports and in case of its severing from the rest of the grid, other substations and power connections with Kosovo* and Montenegro, in the north of the country, would shut down as well.

Considering gas, Albania will host transit of Trans Adriatic Pipeline (TAP) with compressor stations being deployed during the development of this study. The cybersecurity aspects of the management of the TAP critical business systems have potential impact and associated cyber risk to Italy and Europe as a whole.

5.1.3 Legislation at the national Level

Strategy and action plans

The adoption of the Cross-cutting strategy "Digital Agenda of Albania 2015-2020" allowed the country to set strategic goals in the field of digitalization, modernization of processes as well as development of information society. The Strategy is recognizing the importance of cross-sectorial and international approach to cybersecurity and understands that cybercrime presents a danger, which is a good starting point.

The National Policy paper on Cyber Security 2015–2017 set priorities, goals and plans for the development of organizations, ICT infrastructure, legislative documents and decisions in the field of cybersecurity. The policy paper defines strategic policies in the field of cybersecurity of CII and the need for identification of operators of CII/ES. The energy sector is not explicitly defined in the policy paper, but Decision 222 of the Council of Ministers defines electricity subsector TSO and DSO operators as CII. However, the identification of operators of CII/ES in electricity subsector is yet to be conducted and should be prioritized.

Along with the identification of OES, Policy paper establishes strategic objectives to strengthen cooperation between public and private sector for protection of CII, implementation of security measures as well as outlines the need for regulatory changes pertaining to reporting of serious cyber incidents. Considering NAECCS and Government of Albania are in the process of creation of a new National Cybersecurity Strategy 2019-2025, such initiative should be coordinated at both national level and leveraging EnC cybersecurity activities.

Legislation against cybercrime

The Republic of Albania has shown commitment to international cooperation by ratifying the Budapest Convention in 2004 and amended necessary articles and provisions to harmonize its legislative system.

Budapest Convention is implemented in: Law no. 8888 "On Ratification of the Convention on Cyber Crime", Criminal code, Criminal Procedure Code, Law on Criminal Liability for Legal Entities, Law on Copyright, Law on Electronic Communications.

Energy sector relevant cybersecurity legislation

Following the National Policy Paper on Cybersecurity the Law on Cybersecurity[40] was adopted with the goal to achieve a high level of cybersecurity by defining security measures, rights, obligations and mutual cooperation between the entities operating in the field of cybersecurity.

On the basis of the Law on Cybersecurity the Council of Ministers adopted decision no. 222[41] encompassing the list of CII and important information infrastructure (III). It listed electricity TSO SCADA systems and DSOs network between control centre and control points and DSOs SCADA monitoring and control technology as a part of CII or III. However, the identification of specific operators of CII and III in the energy sector has not yet been performed at the time of writing. According to the Law on Cybersecurity, operators of CII in electricity energy subsector (but not gas, which is important to highlight) are responsible to implement security measures foreseen in the chapter III of the law.

The Law on Cybersecurity designates the Ministry for Infrastructure and Energy as the responsible entity for energy sector and responsible for identifying CII in the energy sector and for proposal of addition of the operator of energy CII to the list of CIIs. The aforementioned law designates the National Authority for Electronic Certification and Cyber Security (NAECCS) as the Responsible authority in the field of Cybersecurity and is responsible among others to define minimum technical standards for the CII and serves as a national CSIRT and separately provides the list of critical information infrastructures and list of important information infrastructures. The list identifies electrical energy sector and administrative operators, with TSO SCADA systems and DSOs network between control centre and control points and DSOs SCADA monitoring and control technology in the electrical subsector as part of CII. However, the identification of specific operators of CII and III in the energy sector has not yet been finished at the time of writing and the list of operators is not available, which should be on the future agenda for the responsible ministry.

---

[40] *The Assembly of The Republic of Albania adopted in January 2017 the Law No.2/2017 on Cybersecurity*

41 *Decision no. 222 On approval of the list of critical information infrastructures and list of important information infrastructures.*

The Law on Cybersecurity defines obligation for operators of electrical energy subsector CII to follow technical and organizational provision as well as provisions for asset management which are further elaborated in the Regulation 22 On the content and method of documenting security measures

Organizational provisions demand from electrical energy sector organizations to implement information security and risk management systems, develop security policies, develop organizational security measures, assess and implement measures dealing with safety requirements of third parties, asset management, human resource and access management systems, develop system of security event and incident management measures, develop measures for work continuity as well as control and audit measures and capabilities. Technical measures defined in the Law on Cyber security demand implementation of measures of physical security, measures to protect integrity of communications network, measures to identify user identity and manage their access through authorization, develop security measures for users and administrators as well as implement systems for detection of cybersecurity events. Along with technical and organizational, the above mentioned Law describes the need to implement asset management measures for tracking and evaluating cybersecurity incidents, application security, use of cryptographic equipment and create measures to secure industrial systems. With the regulation of NAECCS no. 22 organizations in the energy sector among other CI, must document implementation of 20 security objectives and measures defined by the Law on Information Security that are based on international standards used by electronic communications providers in the EU (ESI – Electronic Signature and Infrastructures standards) and follow ISO 27001 and 27002 standards. According to the information received by the Albanian Energy Regulatory Authority, the national TSO (OST) started preparing internal information protection rules, adopting guidelines and international laws. As the process is in the initial stages of development no specific law or standards have been named. Along with the creation of such guidelines and provisions it is also an in-depth audit undergoing.

Albania adopted international ISO 27001, 27002 and 15408-1 standards as local standards (SSH)[42].

The list of operators of CII and III must be audited and updated at least once every two years. Current state of affairs is periodically reported through the mechanism of evaluation and publication of a final report on Policy paper on Cyber Security.

5.1.4   National Cybersecurity Authorities

The Republic of Albania has a cross-sector approach to cybersecurity. It encompasses multiple state agencies but the National Authority on Electronic Certification and Cyber Security (NAECCS) is the Competent National Cybersecurity Authority for cybersecurity. It is a single point of contact for cyber incidents as well as responsible organization for defining standards and issuing regulation in the field of cybersecurity for electrical energy CII operators, serves as a CSIRT and cooperates with electrical energy subsector CII. The Albanian Energy Regulatory Authority does not have any responsibilities when it comes to cybersecurity. Albania does not have an ECIP contact point designated but the Ministry of Infrastructure and Energy is the responsible Ministry for the energy sector and identifies and proposes addition of identified operator of CII/ES in the energy sector to the list of CIIs to Council of Ministers.

NAECCS is defined as the National Responsible Authority for Cybersecurity in the Law on Cybersecurity and serves as a single point of contact in matters of cybersecurity. Being the official national coordinating body for handling reporting and management of cybersecurity incidents it cooperates and communicates with

---

42

http://www.dps.gov.al/standard/?ics_id=&national_committee_id=&directive_id=&standard_code=27001&title=&Submit=Search

national TSO and DSO operators in the energy sector as their SCADA systems are included in the list of CIIs and IIIs as well as prescribes regulations, responsibilities and monitors the implementation of information and cybersecurity measures in the energy sector.

NAECCS is responsible organization for definition of minimum technical security standards for energy sector CII operators, as a contact point for reporting of incidents, provides help and support in operations in the sector of cybersecurity, analyses weaknesses of ICT, conducts awareness campaigns and education programmes, helps with drafting relevant legislation and serves as a national CSIRT with a team for emergency monitoring and response.

NAECCS is in the process of joining the FIRST – Forum of Incident Response and Security Teams for purpose of international cooperation and coordination in the field of cybersecurity as well as protection of critical infrastructure including energy sector.

Beside NAECCS there are two other entities working in the field of cybersecurity. The Ministry of Defence is responsible for building and developing national defence capabilities in the cyber domain as well as reducing risks through education, awareness training and introduction of good practices and standards. Its main objective is security and defence of MoD's, Military and Air Forces critical infrastructure as well as handling cybercrime incidents.

The Albanian State Police and the prosecutor's office Cybercrime Investigation Unit[43] is responsible for investigation, research and procedural matters connected with cybercrime and prosecution as well as international cooperation in judicial matters. Cybercrime Investigation Unit is designated as a 24/7 single point of contact under the Budapest Convention.

The National Regulatory Authority for the energy sector[44] does not exercise any rights or obligation pertaining to cybersecurity nor does it monitor or assess implementation of Cyber security strategy. NRA does not communicate with operators in the energy sector regarding cybersecurity incidents nor does it cooperate with NAECCS CERT, and this fact should be highlighted as a risk.

The Ministry of Infrastructure and Energy is the responsible Ministry for the field of energy. It is responsible for identification and proposal for addition of identified operator of energy CII to the list of CIIs and cooperates in Council of Ministers to approve the list of CIIs. The Council of Ministers adopted decision 22 on approval of the list of critical information infrastructures and list of important information infrastructures, identifying electrical energy sector as CII, but the identification of operators in the energy sector has not yet been concluded. Albania does not have a legislatively designated ECIP contact point for the protection of critical energy infrastructure.

5.1.5 Cooperation and initiatives

The Republic of Albania defined international cooperation as one of the strategic objectives in its National Policy Paper on Cybersecurity (2015-2017) as it recognizes that cyberspace has no borders. Therefore, it needs to cooperate and coordinate actions between the public and private sectors, as well as with other states to ensure cybersecurity. As a NATO member and in the accession process towards EU membership it understands the need to actively cooperate in the initiatives on cybersecurity as well as introduce itself as an active and reliable partner by fulfilling commitments towards its allies.

---

[43] *Sector for Investigating Computer Crimes, Criminal Police Department, Bulevardi "Bajram Curri", Tirana. National Office of Interpol Tirana, Bulevardi "Bajram Curri", Tirana*

[44] *ERE (Energy Regulatory Authority)*

Cooperation within Energy Community Parties
TSO participates with the ENTSO-E for information sharing and implementation as well as harmonisation with electricity market rules. As a contracting party, Albania cooperates in the Cyber Security and Critical Infrastructure coordination group (CyberCG) of EnC for the purpose of promotion of high level of security of network and information systems and CI through strategic cooperation and exchange of information.
Cooperation with EU Member States
The Council of Europe and other specialist entities, both private and public, have provided NAECCS with relevant response training. A Memorandum of Understanding (MoU) has been signed with Romania for exchange of incident information and cooperation in matters of cybersecurity. The Republic of Albania is also in the process of signing a MoU with Cyprus and Slovenian CSIRTs.
Cooperation with other parties
Albania cooperates with USEA and its UCSI through workshops with Albanian TSO for the purpose of achieving greater capabilities of detection and management of incidents, strengthen protective measures and enhance infrastructure resilience as well as improve cross-border communication and experience sharing. Programs within USAID Albania Cyber-Security Program contributed to creation of NAECCSs CSIRT. The Program was established for the purpose of providing training through workshops for government and non-government sectors alike. Workshops were carried out by the Carnegie Mellon University Software Engineering Institute and focused on building capabilities for the development of process for managing cyber-incidents as well as safeguarding operational capabilities and defence against threats. A MoU was signed with North Macedonia and Kosovo*/UBT-CERT and is in the process signing a MoU with the Serbian and Montenegrin CSIRTs. OSCE organized national table-top simulation exercise in Albania, that brought together all relevant parties responsible for cybersecurity and protection of critical energy infrastructure from terrorist cyber-attack.
Public-private partnership
Albania took a proactive approach to the field of cybersecurity, including the energy sector, by creating legislative and institutional cooperation for the purpose of addressing cybersecurity as well as creating a mechanism for identification of CII and III as the approach encompasses all Ministries and their responsible sectors, that play a key role in sustaining security, health and economic wellbeing of citizens and effective functioning of the country's economy. The cooperation among stakeholders in the energy sector does not vary from public or private sector, as the Law on Cybersecurity or the Decision no. 222 does not differentiate between public and private sector nor does it go in detail which organizations are actually included.

Table 3: Overview of energy related cybersecurity cooperation initiatives

Overview of education and training programmes

The Republic of Albania understands the importance of creating a security culture surrounding cyberspace and has developed multiple education and training programmes. The NAECCS is the legal Agency responsible for the organization of awareness campaigns and trainings, publication of important material for private or public sector as well as guidelines and regulations on the minimal requirements for the operators of CII and III. The NAECCS organizes incident response awareness training for the purpose of sharing good practices and experience. There is no official training or educational programmes for security specialists, even though the law demands a responsible person for cybersecurity with every operator of CII and III, as well as the definition of criteria for employment of such personnel is in the domain of responsible Ministry.

The private sector is starting to develop its own cybersecurity awareness campaigns for organizations to strengthen its security culture pertaining to cyber-domain including in the energy sector, but it is still in the early stages.

The education system of Albania recognizes the potential and importance of the field of information security and therefore brings together government, industry and academia to offer different courses from information or network security to cryptography. The University of Tirana developed Master's degree in Information security covering the topic of cybersecurity at the Faculty of Economics. NAECCS, NAIS, and UBT CERT from Kosovo* organized Albanian Cyber Academy with sponsorship from the US Embassy in Albania. The Albanian Cyber Academy offered students from different Albanian universities and faculties to participate in workshops to increase knowledge, skills about cybersecurity as well as get understanding of cybersecurity protection practices. NAECCS also conducted multiple educational lectures on different universities for awareness raising on cybersecurity.

The NAECCS and the government institutions as well as non-governmental organizations did receive training through workshops supported by the USAID Albania Cyber Security Program. The workshops were provided by Carnegie Mellon Universities Software Engineering Institute for purpose of building skills to deal with operational threats and develop processes for managing incidents. USAID provided help and training for entities in the energy sector through USEA and NARUC organized workshops. Besides the USAIDs programme similar cybersecurity and incident response trainings were provided by other specialist entities and Council of Europe, but those activities were only for IT public administration, State Police, Bank of Albania and others, but were not conducted in the energy sector.

Albania participated in two workshops organized by Slovenia and Croatia named Balkans Regional Cyber Defence Workshop for the purpose of cooperation on cyber defence issues through workshops, seminars and other regional activities.

5.1.6   Gaps against EU legislation and standards

Cybercrime legislation
Legislation against Cybercrime is implemented in the legislative system and allows investigation and prosecution of offences pertaining to cybercrime.

Identification of CI operators and OES
CI is not identified nor is identification foreseen in the current legislation. Decision no. 222 of the Council of Ministers lists Electricity TSO SCADA systems and DSOs network between control centre and control points and DSOs SCADA monitoring and control as energy CII but the list of CII operators foreseen in the legislation is not yet available nor is available identification timeframe. Gas sector is not mentioned in the legislation related to critical information infrastructure nor is represented in the assessment methodologies foreseen in the legislation.

National NIS strategy
No major gaps were identified regarding transposition of NIS directive. The National Policy Paper on Cybersecurity (2015-2017) and the Cross-cutting Strategy "Digital Agenda of Albania 2015-2020" have set strategic goals, priorities and policies for the digitalization and information domain as well as cybersecurity field. The Policy paper goes well in detail about identification of CII and III as well as setting of guidelines for minimum security requirements which was implemented through adoption of the Law on Cybersecurity. It is important to note that new cybersecurity strategy is in the preparation.

National Cybersecurity Authorities: Contact points

CI and ECI protection contact point is not established.

NAECCS serves as a National Cybersecurity Authority, SPoC and CSIRT. NAECCS serves as a central authority for communication with other sectors and other state institutions or foreign entities and is designated as a single point of contact.

However, there is no formally established channel for sharing of energy sector cybersecurity incidents with EnC CPs.

Security plans and requirements

Cybersecurity measures foreseen in the legislation for CII/ES operators are aligned with EU and international good practice.

In addition, the Law on Cyber Security demands from operators of CII and III to communicate any implemented measures and incidents to the NAECCS.

Standardization

No gaps were identified as Albanian national standards (SSH)[45] encompass cybersecurity ISO 27001, 27002, 15408-1, 2, 3 standards.

Operators level

The Energy sector recognised the importance of international standards (ISO 27001 standards, ENISA's recommendations) and are considering or implementing them. CII and III are obliged by NAECCS's regulation on minimum standards to perform risk assessment and create measures and procedures to manage incidents, risks and threats. Nation-wide risk or threat assessment in the energy sector has not been carried out.

The Albanian Transmission System Operator has started preparing some internal information protection rules and adopting guidelines as well as international laws requirements, however no specific standard or law has been mentioned as this initiative is at an initial stage of development.

Cooperation

The National Energy Regulatory Authority does not cooperate across different sectors inside the country nor does it cooperate across borders. The TSO on the other hand does participate internationally as well as internally through different initiatives under NATO CCD CoE, United States Energy Association Utility Cyber Security Initiative and ENTSO-E.

---

[45] Albanian national Standards. https://www.wto.org/english/thewto_e/acc_e/alb_e/WTACCALB38_LEG_3.pdf

5.2 Bosnia and Herzegovina

Bosnia and Herzegovina (BiH) is with the help of OSCE developing Strategic Framework for Cyber Security that will be based on the ENISA guidelines with no information about adoption date. Based on the information provided by Ministry Foreign Trade and Economic Relations the new Strategic framework will address CI and OES in the energy sector and will be aligned with NIS directive requremetns. Lack of strategic documents in the field of cybersecurity is reflected in the lack of legislation regulating identification of CI and CII/ES operators as well as related cybersecurity provisions.

It should be noted that the political system demands consensus and all decisions have to be coordinated and agreed upon, creating a challenge for amendments to the legislative system, acceptance of strategic documents, as well as institutional organization and cooperation among entities and state level introducing additional complexity to the implementation of cyber-security in BiH.

BiH has multiple gaps regarding NIS and ECI directives. There is no country level legislation pertaining designation of CI, CII/ES and cybersecurity measures in the energy sector. The only cybersecurity requirements that energy sector operators must implement are those of international organizations as in the case of NOSBIH (Electricity TSO) that is in the process of implementation of ISO 27001 and OPDE/ATOM[46].

In BiH there is no country level energy specific or general legislation pertaining to cybersecurity. National CS Authority, cybersecurity SPoC and national CERT are not established or designated, however IT security department in the Sector for Protection of Classified Information of Ministry of Internal Affairs is a designated SPoC for public institutions

Republic of Srpska adopted the general Law on Information security pertaining to public institutions but not for organisations in the energy sector. Federation of Bosnia and Herzegovina and District Brčko are in initial stages of developing general cyber/information security laws.

---

46 Guidance OPDE/ATOM for the preparation of security plan and Agreement on Minimal Viable Solutions issued by by ENTSO-E are not publicly available.

5.2.1   SWOT analysis

S

STRENGTHS

Strengthening of capabilities for fight against cybercrime in BiH was developed through European Union and Council of Europe devised project CyberCrime@IPA. Project helped with raising awareness, enhancing cooperation between public and private sector as well as with international entities, organizations and foreign states paving the way for good practice in energy sector as well.

W

WEAKNESSES

In BiH there is no national level energy specific or general legislation pertaining to cybersecurity, and consequently there is no national CS Authority, cybersecurity SPoC nor national CERT established or designated.

O

OPPORTUNITIES

BiH is in the process of creation of Strategic Framework for Cyber Security in BiH with the help of OSCE and based on ENISAs guidelines, giving it an opportunity to use latest published recommendations issued in March by EC.

T

THREATS

Lack of legislation on a country level and associated risk assessment is further made more complex by the political system demanding consensus on these matters.

5.2.2 European Critical Infrastructure and Essential Services legislation requirements

Identification of EnCCI and ES

There are no legislative provisions related to identification of critical infrastructure and OES. Process for identification of CI/ES has not yet started. Complex nature of the political system causes obstacles pertaining to jurisdiction relating to cybersecurity and territorial CI/ES identification.

/	Lead: Council of Ministers

Criteria for CI designation and criteria for significant disruptive effect

There are no legislative criteria established pertaining to disruptions or criteria for significant disruptive effect assessment.

/	Lead: No designated national/entity body

National NIS strategy

There is no cybersecurity strategy on national level or entity level. Strategic Framework for Cyber Security is in the development in collaboration with international organizations (OSCE) and taking into account ENISAs guidelines. Based on the approach taken it is reasonable to assume that Framework will be aligned with NIS directive but the draft is not publicly available. Republic of Srpska started development of its own strategy but it is yet to be adopted, while BiH Federation and District Brčko did not start with development.

No time period available	Lead: Council of Ministers, Entity responsible Ministry

National CS organisational framework

State wide energy sector CI protection contact point is not established. Ministry of Foreign Trade and Economic Relations is responsible for energy sector on national level.

/	Ministry of Foreign Trade and Economic Relations[47]

As there are no legislative provisions pertaining to cybersecurity on the national level, national SPoC for cybersecurity, national CERT and CS authority have not been designated. On the entity level only Republic of Srpska designated SPoC as well as entity CERT as SPoC for cyber incidents, but they are not responsible for energy sector.

Ministry for Scientific and Technological Development[48]; DB: none	

Energy sector operators are not obliged to designate person responsible for cybersecurity.

/	Lead: /

CI operators and ES providers security requirements

As there is no legislation or other provisions pertaining to cybersecurity requirements, there are no obligations for operators of infrastructure/services in the energy sector.

Standardisation

BiH national standards encompass cybersecurity ISO 27001, 27002 and 15408-1, 2, 3 standards.

---

[47] Ministry of Foreign Trade and Economic Relations, Musala 9, Sarajevo

[48] Ministry for Scientific and Technological Development, department for Higher Education and Information society

Energy sector stakeholders are not obliged by the legislation to follow national or international cybersecurity standards.

ENTSO-E recommended implementation of ISO 27001 standards for national TSO (NOSBIH) and set recommendations to follow EU Commission regulation 2017/1485 and Council Directive 2008/114/EC. ENTSO-E prescribed OPDE/ATOM guidelines and provisions pertaining to Minimal Viable Solutions and Security plan.

Lead: General Directorate of Standardization; NAECCS

Considering gas BiH is situated at the end of supply route with interconnection point with Srbijagas and ambitious plans to increase internal transmission network and new connections towards Croatia. When building new interconnections or internal transmission capacities, cybersecurity shall be take into consideration as well. Considering electricity interconnections, BiH has besides CPs possible cascading effects to Croatia.

5.2.3   Legislation at the national Level

Complex nature of political system in BiH replicates itself in the complexity of the legislative system and cybersecurity strategy adoption. Multiple autonomous entities comprising of Federation of Bosnia and Herzegovina (FBiH), Republic of Srpska (RS) and District Brčko (DB) each have their own legislative system with provisions relating to cybercrime and cybersecurity incidents. With the state legislative system dealing with offences representing clear danger to the values protected by the state it does allow BiH to coordinate prosecution of cybersecurity incidents in special cases.

The Strategy for Establishment of CERT in BiH 2011 under Ministry of Security can be used as an example for complexity of strategy and legislation adoption procedures. Although the successful adoption of the strategy for creation of CERT by Council of Ministers and following Expert working group an action plan for the creation of BiH CERT and CERTs of entities was devised it was not put in action because of procedural and jurisdictional issues.

Strategy and action plans

Strategy for the Establishment of CERT in BiH has been adopted by the Council of Ministers but it was not implemented because of disagreements about jurisdiction (state/entities).

BiH is in the process of creation of Strategic Framework for Cyber Security in Bosnia and Herzegovina with the help of OSCE and based on ENISAs guidelines. The energy sector will presumably be addressed in the upcoming strategy. One of the main objectives in the upcoming Strategic Framework for Cyber Security will be definition and identification of CI and its protection, establishment and strengthening of incident response capacity as well as creation of incident reporting mechanisms.

Strategic documents that include energy sector are Strategy for Prevention and Combating of Terrorism 2015-2020 and Strategy for Combating of Organized Crime (2014-2016, new 2017-2020) which address cybersecurity issues.

Strategy for Prevention and Combating of Terrorism BiH sets strategic goals for protection of CI. The strategy puts emphasis on the need to protect critical cyber infrastructure, but it is not clear whether energy sector is included.

Same can be said for Strategy for Combating of Organized Crime, where general strategic goals pertaining to cybersecurity are set but applicability to energy sector is not clear. Strategy addresses strategic goals for implementation of necessary cybersecurity related legislative provisions and laws, strengthen cooperation between public and private sector, educate and spread awareness for safe use of technology, educate necessary law enforcement and persecutors as well as allows improvement of their technology, improvement, equipment and development of technologies used for cybersecurity of the state and its affairs, implements necessary legislative regulations and provisions of international treaties as well as detects and prevents copyright violations and infringement. It is not clear how this strategy effects energy sector as it is not explicitly defined in the strategy and the development of legislative provisions are in the initial stages.

Republic of Srpska (RS) started developing Cyber Security Strategy but the process has not yet been concluded.

Legislation against cybercrime

With the state legislative system dealing with offences representing clear danger to the values protected by the state it does allow BiH to coordinate prosecution of cybersecurity incidents in special cases.

BiH ratified Budapest convention in 2006 and the provisions were later amended or implemented in the respective criminal and criminal procedure codes of entities as well as on the state level. Cybersecurity remains in the domain of each of the three entities and their respective legislative codes under their jurisdiction but it is important to note that in certain cases of conflict of jurisdiction and cross-entity-border incidents, the state can take charge in the matters of cybersecurity. It is important to note that although BiH ratified Budapest Convention, the legislative system is only partially harmonized with Conventions provisions.

Addition of definitions of "service provider" and "traffic data" must be added, as well as amendments to the substantive and procedural law by all entities for full compliance with the Budapest Convention. BiH also ratified the additional protocol on Convention on Cybercrime Concerning the Criminalization of Acts a Racist and Xenophobic Nature Committed through Computers Systems.

Provisions pertaining to fight against cybercrime, based on the Budapest Convention are only partially transposed in the criminal and criminal procedure code in Federation of Bosnia and Herzegovina. Adoption of legislation pertaining for fight against cybercrime based is only partially implemented in criminal and criminal procedure code in Republic of Srpska. District Brčko partially harmonized its criminal and criminal procedure code with Budapest Convention.

Budapest Convention is implemented in:

Bosnia and Herzegovina: Criminal Procedure Code, of BiH, Criminal Code of BiH, Law on mutual legal assistance in criminal matter.

Republika Srpska: Criminal Procedure Code of RS, Criminal Code of RS.

Federacija BiH: Criminal Procedure Code FBiH, Criminal Code FBiH.

District Brčko: Criminal Procedure Code DB, Criminal code DB.

Energy sector relevant cybersecurity legislation

BiH and state entities are at the moment not developing any energy sector ECI/NIS or cybersecurity specific legislative provisions. There is also no initiatives or strategic documents pertaining to cybersecurity in the energy sector in development or initial stages that could be used for basis of future development of regulatory or legislation in the area of cybersecurity for energy sector.

For national TSO there are ENTSO-E recommendations for implementation of ISO 27001 standard and recommendations for following EU Commission regulation 2017/1485 and Council Directive 2008/114/EC. Along with above-mentioned recommendations, ENTSO-E prescribes implementation of OPDE/ATOM security plan and agreement on Minimal Viable Solutions. Also national gas TSO should start the implementation of ISO 27.000 and as observer in ENTSO-G follow the cybersecurity related activities.

Other general cybersecurity related legislation

There is no general cybersecurity legislation that would regulate information and cybersecurity on a national level.

Federation of Bosnia and Herzegovina did not develop or adopt any general cybersecurity legislative or regulatory documents and is not in the process of doing so.

Republic of Srpska developed Law on Information Security that serves as a general law on cybersecurity for institutions in the public sector and organizations or individuals working, analysing and processing information of public institutions of Republic of Srpska. The law does not go in detail about the standards (either international or domestic) but it designates the Government of RS for regulation of protection measures on the proposal of Competent authority – in this case Ministry for Scientific and Technological Development, Higher Education and Information Society of RS along with specialized institution under Agency for the Information Society - CERT. It is important to note that Republic of Srpska appointed interdepartmental working group for drafting and development of Cyber Security Strategy and Strategy for Fight against Cybercrime, but it has not yet been adopted.

District Brčko did not develop or adopt any general cybersecurity legislative or regulatory documents and is not in the process of doing so.

BiH national standards[49] encompass cybersecurity ISO 27001, 27002 and 15408 standards.

5.2.4 National Cybersecurity Authorities

On state level Ministry of Foreign Trade and Economic Relations of BiH is designated Competent National Authority for energy sector and as a coordinative institution for cooperation among entities. Due to lack of legislation it does not have responsibilities pertaining to energy sector cybersecurity or protection of CI. As a part Council of Ministers of BiH it represents executive branch of the state dealing with definitions of policies

---

[49] *Institute for Standardization of Bosnia and Herzegovina.*
http://www.bas.gov.ba/standard/?ics_id=&classification_id=&national_committee_id=&directive_id=&status_natstd_id=0&standard_code=15048&title=&ics_text=&directive_text=&national_committee_text=&from_date=&to_date=&Submit=Tra%C5%BEi

and basic principles, coordination of activities as well as consolidation of entity plans with those of international institutions. Authority is designated as a single point of contact in the matters of Energy Community Cyber Coordination Group for Cybersecurity and Critical Infrastructure (EnC CyberCG).

Ministry of Internal Affairs was designated as SPoC for institutions of Bosnia and Herzegovina with its specialized IT security department in Sector for Protection of Classified Information. It defines physical, organizational and technical provisions and standards for protection of classified information but it does not exercise any responsibility over energy sector. Incident-response and activities connected to communication are not well coordinated across organisations but are more often created ad hoc. Directorate for Coordination of Police Bodies can be used as an example as it mediates and coordinates the efforts of entities and forwards the necessary information obtained through international channels to the respective entity or agency as the operational capabilities are in domain of the entity. It is a 24/7 SPoC under Budapest Convention[50].

National Regulatory Authority for energy sector[51] does not exercise any rights or obligation pertaining to cybersecurity nor does it monitor or assess implementation of Cyber security strategy. There are agreements between NRA and TSO's for the purpose of communication of major transmission network events (also cyber related) but TSO does not need to inform other institutions about cyber-incidents. NRA does not cooperate with CERT on the national level as such body has not been established.

As there are no legislative provisions there is also no state designated SPoC for cybersecurity or CERT. With exception of Republic of Srpska, entities have not designated their cybersecurity authorities. Entities did not provision responsibilities for cybersecurity of CI/ES operators or established CERT.

It is important to note that the Republic of Srpska adopted the law on Information security and started developing the Cyber Security Strategy and Strategy for Fight against Cybercrime. Although last 2 strategic documents have not been adopted yet, Republic of Srpska did develop its own structures for purpose of cybersecurity. CERT of RS which operates under Agency for Information Society under oversight of Competent Authority: Ministry for Scientific and Technological Development, Higher Education and Information Society of RS. CERT serves as a coordinating and operative body for the Authority and its primary mission is coordination of ICT security, incident prevention and response as well as spreading awareness for protection of cyber space of Republic of Srpska. It serves as a point of contact for cyber incidents, while the Competent Authority is designated as the point of contact for cyber incidents. As there is no responsibility of CERT regarding operators of energy CI or ES, operators do not have any obligations for reporting.

For the purpose of investigation of cybercrimes committed in the jurisdiction of Republic of Srpska there is a specialized police Unit for Prevention of High-tech Crime under Ministry of Interior of Republic of Srpska. It works closely with the Department for Information Security within Agency for Information Society.

Federation of BiH has a very similar procedure for handling and investigating cyber-security incidents. Incidents are reported to the Crime Police Department of Federal Police Administration. There is no specialized cybercrime unit as the cantonal level and Federal Ministry of Interior report incidents to the Crime Police Department as well as organizations from other sectors. There are cases where incidents are not reported because there is no obligation to do so and organizations therefore manage incidents by themselves according to internal policies. On the entity level there are representatives of the Government of Federation of BiH participating in the Ministry of Security for the purpose of coordination of activities and developing capabilities in the field of cybersecurity.

---

[50] *International Police Cooperation Sector – INTERPOL Sarajevo, Direction for Cooperation of Police Bodies of Bosnia and Herzegovina, Ministry of Security of Bosnia and Herzegovina, Aleja Bosne Srebrene, Sarajevo*

[51] *State Electricity Regulatory Commission*

5.2.5   Cooperation and initiatives

BiH recognizes the importance of cooperation between public and private sector as well as internationally. Through multiple different laws, strategies and international organizations set strategic goals and objectives and is working towards strengthening of international cooperation as well as creation of public-private partnership and cooperation for cybersecurity protection of CI, although not explicitly defined the effect and role of energy sector as the identification of sectors has not yet been conducted.

Cooperation within Energy Community Parties
As an EnC contracting party BiH cooperates in the Cyber Security and Critical Infrastructure coordination group (CyberCG) of EnC for the purpose of promotion of high level of security of network and information systems and CI through strategic cooperation and exchange of information.
Cooperation with EU Member States
European Union with support of Council of Europe devised project CyberCrime@IPA for strengthening of capabilities for fight against cybercrime in BiH. Project helped with raising awareness, enhancing cooperation between public and private sector as well as with international entities, organizations and foreign states. Along with CyberCrime@IPA there was also iPROCEEDS project created between EU, CoE and BiH for purpose of establishing search, seizure and confiscation of data and funds obtained by cyber criminals.
Cooperation with other parties
National Regulatory Authority participated in multiple international programmes organized with emphasis on technical aspects of cybersecurity. The programme for Effective Regulation of Cybersecurity has been organized by U.S. Agency for International Development (USAID) and National Association of Regulatory Utility Commissioners (NARUC). Above mentioned organizations have also organized workshops with the intention of creating guides for regulators in the Black Sea and Southeast Europe regions to reinforce knowledge and practical understanding of cybersecurity solutions. TSO Elektroprenos-Elektroprijenos BiH cooperates cross governmentally and with international organizations as well. There have been multiple exercises, conferences, trainings, workgroups and others organized for strengthening of cybersecurity, cooperation, assessment of capabilities and experience sharing. Independent system operator NOSBIH cooperates internationally through ENTSO-E organization for the purpose of establishing high security standards for the protection of critical transmission systems infrastructure and in the field of cybersecurity also through different workshops, regulations and experience sharing initiatives. Organization for Security and Cooperation in Europe has organized informal working groups for creation of Strategic Framework for Cyber Security in Bosnia and Herzegovina, carried out training on the role of ICT in the context of regional and international security and organized exercises for risk assessment and crisis situation management based on recommendations of the Good Practice Guide on Non-Nuclear CI protection. In collaboration with United Nations it organized Annual Review Conference on Compliance with OSCE and UN Security Commitments of BiH – Cyber Security Panel. OSCE has organized discussion on the topic of enhancing multi-stakeholder Cybersecurity Governance in collaboration with The Geneva Centre for Democratic Control of Armed Forces and supported by the UK Governments Foreign and Commonwealth Office.
Public-private
BiH is in the process of developing public-private partnership and sharing of information. At the time of writing, there was no legislative provision that would obligate or facilitate public-private partnership. The Strategy for Combating of Organized Crime sets goals on strengthening of public-private partnership although not directly defined for the purpose of addressing cybercrime or protection of CI in the energy sector.

Table 4: Overview of energy related cybersecurity cooperation initiatives

5.2.6 Overview of education and training programmes

BiH developed multiple awareness-raising programmes, courses, seminars, online resources, educational opportunities in the universities dealing with cybersecurity. However, there are no special energy sector specific campaigns, trainings or education programmes. ENTSO-E has organized special training workshops for strengthening the awareness for cybersecurity and for fostering the compliance with OPDE/ATOM standards, as well promoting the provisions for national electrical TSO and the development of security plans.

Education and training programmes are important for creating a security culture and help develop necessary skills, mindset and knowledge for managing incidents as well as for creating a safe cyberspace. Despite the fact that BiH has a number of different awareness-raising programmes, courses, seminars and online resources, it is lacking a coordination plan on a state level to efficiently promote its strategy.

Education system in BiH is not centraklly managed and therefore there are no systematic qualification programs for educators and teachers. But However, there are a number of cybersecurity courses available as a part of the Faculty of Engineering at the undergraduate, masters and PhD levels.

BiH hosts the American University in Bosnia and Herzegovina, with its multiple college courses on different levels, ranging from masters to doctoral degree, that cover aspects related to cybersecurity. With its research and development unit of South-East Europe Cyber Security Centre (SEECSC) offer to young officials and professionals the possibility to increase knowledge, skills and capacities in the field of cybersecurity. The Centre is aiming to improve cybersecurity capacities for public institutions and private sector. The centre and university cooperate and they are supported by DiploFoundation, Geneva Centre for Democratic Control of Armed Forces, as well as by the Federal Department of Foreign Affairs of Switzerland.

However, it is important to note that there is no official training, programme or any other course for achieving certification with either internal or internationally recognized standards in the field of cybersecurity in BiH. There are possibilities to acquire certification by Microsoft, Cisco or Neseco, but empirical knowledge in dealing with incidents is inadequate and organizations do not consider important to hire accredited specialists. Education and training in either public or private sectors are carried out only upon the approval of managers that recognize the importance of cybersecurity for their companies.

There are multiple international workshops that help operators or experts in energy sector to acquire new experience, share good practices or cooperate and build confidence with foreign countries, internal and external entities and organizations as well as international organizations. One of such workshop is OSCE's workshop that focuses on the role of ICT in international security, where participants from multiple countries and agencies exchange views on how to mitigate the impact of major cyber incident and on how to create more resilient national ICT system.

5.2.7 Gaps against EU legislation and standards

Cybercrime legislation
The legislative system of state and entities (Federation of BiH, Republic of Srpska and Brčko District) should be amended with the missing provisions from Budapest Convention.
Identification of CI operators OES
Bosnia and Herzegovina on national level as well as entity level do not have any legislative or regulatory provisions related to identification of CI/OES operators. Consequently, neither energy sector Critical infrastructure, their dependency on key information systems and information technology nor OES for energy sector are identified.

National NIS strategy

There is no cybersecurity strategy adopted. The Strategic Framework for Cyber Security is in preparation with the help of OSCE. It is foreseen that it will address objectives, development, needs, potential threats and international obligations and standards. The Strategic Framework is being developed following ENISAs guidelines for designing and implementing of National Cyber Security Strategy and with ENISAs regulation in mind (NIS Directive).

National Cybersecurity Authorities: Contact points

The Ministry of Foreign Trade and Economic Relations of Bosnia and Herzegovina is designated as responsible Ministry for energy sector, but ECIP contact point is not established as there is no underlying legislative provision pertaining to CI/ES operators.

National level Cybersecurity Authority, SPoC and CSIRT are not designated.

Legislative system does not foresee communication with other EnC contracting parties in case of incidents, nor is there any legislative provisions regarding reporting, cybersecurity measures and reporting of incidents domestically or internationally in general or specifically for energy sector. There is an agreement between NRA and TSO in electricity sector to report major transmission events; reporting of cyber incidents that do not result in major transmission event is not obligatory.

Security plans and requirements

There is no legislation that would oblige CI, CII and OES operators to establish cybersecurity plans and measures.

There are also no established or foreseen reporting communication channels or procedures with relevant authorities. However, there are international standards recommended by the international organizations (e.g.: ENTSO-E) as well as recommendation to follow EU provisions pertaining to cybersecurity and security of CI.

Standardization

There are no gaps in regards to standardization as Bosnia and Herzegovina national standards encompass cybersecurity ISO 27001, 27002 and 15408-1, -2, -3 standard.

Operators level

There are no cybersecurity international standards or good practices obligatory for energy sector operators by law. Organizations and institutions in energy sector do implement standards and good practices based on recommendations of international organizations or recognize the need to implement them by themselves. As there is no official law, strategy or any other strategic document pertaining to implementation of internal or international standards on the state level for energy sector, there are standards recommended for TSO by ENTSO-E for implementation of ISO 27001 and recommendations to follow EU Commission regulation 2017/1485 and Council Directive 2008/114/EC. ENTSO-E prescribes OPDE/ATOM Security plan and agreement on Minimal Viable Solutions for NOSBIH TSO.

Cooperation

Absence of central cybersecurity authority and limited cooperation between ministries, entities and organizations create communication and jurisdiction issues in the cybersecurity incident prevention and mitigation. Cybersecurity incident information sharing and communication channels are not prescribed in the legislative system and are usually done on ad hoc basis. Prosecution of offences remains in the jurisdiction of entities and cooperation begins only if an offence crosses borders of entities or state.

There is no determined agency or ministry for organization of exercises in the field of cybersecurity on the state level although cybersecurity exercises in the energy sector were carried out under OSCE mission to Bosnia and Herzegovina.

Organizations in the energy sector cooperate internationally with other countries and international organizations (USAID, NARUC), but the majority of communication is done through direct contact with foreign participants with little coordination with BiH stakeholders.

5.3 Georgia

With creation of National Cyber Security Strategies (2012-2015 and 2017-2018) Georgia created a sound base for development and strengthening of cybersecurity. Based on past experience Georgia recognizes the importance of cybersecurity and is working towards legislative and organizational regulation of CII/ES operators.

Georgian legislation pertaining to CII/ES is highly aligned with the NIS directive requirements but it is currently not applicable to the energy sector. Nevertheless, energy sector operators and National Cyber Security Authority (DEA) cooperate and communicate and some organizations in the energy sector voluntarily implement cybersecurity standards (e.g. ISO 27001).

A year ago NRA established working group to address cybersecurity in the energy sector. Working group is cooperating with National Cyber Security Authority to identify critical information infrastructure in the electricity, gas and water. It is planned that CII/ES energy sector operators will be identified in Q4 of 2019. Identification will be followed by legislative procedure to designate energy sector CII/ES operators and encompass related cybersecurity requirements into the legislation.

DEA was designated as National authority for CS, SPOC and as national CSIRT in the Law on Information Security. It is important to note that without adequate resources, this could lead to the risk that DEA would not be able to effectively separate operational and strategic tasks.

Currently there is no legislation regarding the identification of CI, their security plans and contact points for cross-border energy sector cybersecurity incident communication and coordination.

New National Cyber Security Strategy for timeframe 2019-2022 is in preparation for timeframe 2019-2022 is in the development and will incorporate strategic goals pertaining to CII/ES operators.

5.3.1 SWOT analysis

S

STRENGTHS

Georgian legislative system demands from operators of essential services to provide information about cyber-related incidents to the DEA. CERT as well as obligates them to assign personnel to the roles of Information Security Manager and Cyber Security Specialist energy sector organisations do not have to comply with provisions set in related regulations, but they are voluntarily implementing related law provisions.

W

WEAKNESSES

Responsible ministry for energy sector is Ministry of Energy however no ECIP or CI contact point has been designated. Due to no legislation related to critical infrastructure there is no assessment of potential impacts to neighbouring countries.

O

OPPORTUNITIES

Identification process for energy sector CII is well in progress and it is foreseen that it will be finished until the end of the 2019. Update of cybersecurity legislation is planned to incorporate CII (it is foreseen that the vast majority of CII will be in energy sector)

T

THREATS

Georgia is in a very exposed state to possible cyber-attacks in energy as well as other critical infrastructure domains and as such needs more agile mechanism for coordinating energy sector with general legislation. Upgrade of infrastructure and control systems at energy operator premises is not progressing in pace with state-of-the-art cybersecurity requirements

5.3.2   European Critical Infrastructure and Essential Services legislation requirements

Identification of EnCCI and ES
Critical information systems are identified but do not include energy sector CI/ES operators or NRA. CI/ES operators in energy sector will be designated on the basis of multi-agency approach of DEA, MoD, MIA, Intelligence agencies in 2019 and passed to legislative procedure.

Issued: 11.3.2013	*Lead: Government of Georgia*

Criteria for CI designation and criteria for significant disruptive effect
Criteria for the identification of CII is defined in the Law on Information Security and encompasses following criteria: gravity, scale of potential consequences and expected economic loss, necessity of services delivered for normal functioning of society, number of users, amount of estimated penalties incurred as result of liabilities. Criteria for significant disruptive effect are not defined.

Law on Information Security, issued 5.6.2012	*Lead: DEA*

National NIS strategy
National Cyber Security Strategy (2012-2015, 2017-2018) has set strategic goals, principles and plans and set basis for development of legislative acts, competent agencies, CERTs and strengthening of cybersecurity and ICT infrastructure resilience. One of strategic goals is the identification of operators of CI/ES, but energy sector is not explicitly mentioned.

For time period 2012-2015, 2017-2018	*Lead: DEA*

New strategy is in the process of adoption for timeframe 2019-2022.

For period: 2019-2022	*Lead: DEA*

National CS organisational framework
Energy sector contact point for the coordination of CI protection with other states is not established. The Ministry of Energy is responsible for energy sector

Law on Information Security	*Lead: Ministry of Energy[52], Government of Georgia*

DEA is National authority for CS, SPoC and is responsible for definition of cybersecurity measures. Although DEA CERT was established as public administration CSIRT it also serves other organizations. As there is no legislation pertaining to operators in energy sector, there is no obligation for them to cooperate with DEA, but they developed voluntary communication channels and cooperation initiatives with DEA. CI operators shall assign personnel to the roles of Information Security Manager and Cyber Security Specialist with responsibilities to implement ISMS and report administrative/organizational activities and incidents to DEA and CERT. Aforementioned requirements are not mandatory for energy sector operators as they have not yet been designated as CI/ES operators.

Law on Information Security	*Lead: DEA*

CI operators and ES providers security requirements
Because energy sector organisations has not yet been identified/designated as CI or OES operators they do not have to comply with provisions set in related regulations, but organizations in energy sector are voluntarily implementing legislative provisions.

---

[52] *Ministry of Energy, Sanapiro str. N2, Tbilisi.*

Operators Security plans are foreseen in the DEA Order on Approval of Minimum Information Security Requirements and Minimum Standards for the Information Security Manager of the CI System subject. The legislative provisions pertaining to implementation of cybersecurity measures follow ISO 27001 standard.

Order on Approval of Minimum Information Security Requirements and Minimum Standards for the Information Security Manager of the CI System subject	*Lead: DEA*

Standardisation
Georgia adopted international standards ISO through GeoSTM and therefore ISO 27001, 27002 and 15408-1 are national standards.
Operators in the energy sector are not obliged to follow provisions set by DEA, however some are voluntarily implementing necessary provisions as well as international standards (e.g. 27001).
Lead: GeoSTM, Energy organizations, DEA

Georgia is largely dependent on imports of energy, especially during the winter. The electricity system of Georgia is interconnected with the systems of all neighbouring countries with, possible cascading effects besides CPs, to/from Russia, Turkey, Armenia and Azerbaijan. All of these interconnections have high requirements for implementation of cybersecurity measures in all control systems. One of the most serious security issues is the location of certain facilities of the largest hydroelectric power plant is in the occupied territory of Abkhazia. Considering gas, Georgia has well-developed cross-border connections with all neighbouring gas systems. It is very important gas transit country since provides the only onshore route for transit of Azeri and Russian gas to Turkey and Armenia. This strategic role of Georgia demands special also in the segment of cybersecurity in gas sector.

5.3.3   Legislation at the national Level

Strategy and action plans

The creation of Cyber Security Strategy[53] paved the way for strategic goals, principles and plans and set basis for development of legislative acts, competent agencies, CERTs and strengthening of its cybersecurity and ICT infrastructure resilience as well as recognized the need for identification of CII. Strategy takes into the account NIS directive provisions pertaining to national network and information security strategies.

National Cyber Security Strategy 2012-2015 addressed multiple strategic goals, created a strategic assessment of cyber threats and challenges, set basic principles of cybersecurity policy and adopted an action plan for the implementation. Strategic goals were conducting of research and analysis of cybersecurity field, creation of new regulatory and legislative framework, among which was also framework for identification of CII, goals for strengthening of institutional cooperation and building of CERT, public awareness campaigns and education activities and strengthening of international cooperation. One of the plans for creation of regulatory framework for identification of CII was set, although energy sector was not explicitly incorporated.

---

[53] *Cybersecurity Strategy of Georgia 2012-2015, and latter Cyber Security Strategy 2017-2018*

Cyber Security Strategy for the timeframe of 2017-2018 set strategic goals pertaining to identification of CII and recognized the need to adopt necessary legislative provisions for CII and establish criteria and standards for assessment and identification of CII and ES, however the energy sector was not explicitly mentioned in the strategy and no risks or threats were assessed for energy sector. Among other strategic goals Georgia defined: improvement of legislation, building of capabilities for prevention and response to cyber incidents, educating and spreading awareness about cybersecurity and the need to strengthen international cooperation.

Based on the information received from interviews new Cyber Security Strategy for the timeframe of 2019-2022 is in the making and its release is scheduled in the coming months.

Legislation against cybercrime

Georgia is a ratifying party of the Budapest Convention and through the changes in legislative system managed to incorporate and implement all necessary provisions. The definitions demanded by the Budapest Convention have been implemented and accepted in the Criminal procedure code as well as Criminal code, allowing Georgia to incorporate necessary definitions into national legislation. Procedural provisions of Budapest convention have been implemented through Constitution, Criminal Procedure Code, Electronic Communications Law and Operative-Investigative Activities Law. Jurisdiction provisions are defined under Criminal Code. Georgian law on Cooperation in Criminal Matters and international (either bi-, multi-lateral or ad-hoc) treaties and agreements allow Georgia to cooperate with foreign entities and states, as long as there is no legislative act that would prohibit such actions. The legislative system of Georgia is therefore in compliance with the Budapest Convention.

Budapest Convention is implemented in: Criminal Procedure Code, Criminal Code, Law on Electronic communication, Law on Operative-Investigative activities, On International Cooperation in Criminal Matters.

Energy sector relevant cybersecurity legislation

Law on Information Security is the main law pertaining to regulating cybersecurity measures for operators of CI and ES. The law is provisioning operators of CI and OES implementation of minimum measures defined by the National Cybersecurity Authority – DEA.

The NRA and organizations in energy sector are currently not identified as OES, but they did develop informal communication practices and share knowledge, information and experience through such means with the DEA.

At present time, the process of critical infrastructure identification and OES in is underway in Georgia encompassing energy sector operators. It is expected that the list of CII operators will contain few dozens with the majority in the energy sector. The law is planned be done in 2019 and passed in the legislative procedure.

In addition, operators in energy sector and the DEA are currently in discussions for the implementation of regulations, provisions and standards from CIIP, NIS and ECI directive. One of discussed approaches is that implementation timeframe will vary from the operator to operator of energy CI based on their capabilities and importance. Operators and organizations in the energy sector comprehend the importance of implementing standards and are obtaining the ISO 27001 certification although they are not obliged by law to do so.

The Law on Information Security is the main act pertaining to essential services and critical infrastructure as well as prescribes minimum requirements for information security and establishing Data Exchange Agency as responsible agency for definition of technical and organizational provisions as well as implementation monitoring. At present time, the process of critical infrastructure identification and OES in private and public-

private sector is underway in Georgia with expected finalization by the end of 2019 and energy sector is expected to be included in the identification.

Georgian legislative system demands from OES to provide information about cyber-related incidents to the DEA[54] CERT as well as obligates them to assign personnel to the roles of Information Security Manager and Cyber Security Specialist under Law on Information Security. First is responsible for implementation of ISMS, based on ISO 27001, and reporting of administrative/organizational activities as well as incidents, while Cyber Security Specialist is responsible for assessment, analysis and identification of incidents, and coordination with CERT. The NRA and organizations in energy sector currently do not fall under the above-mentioned criteria and law, as they are not identified as OES. But they did develop informal communication practices and share knowledge, information and experience through such means with the DEA.

Georgia adopted international standards ISO through GeoSTM and therefore ISO 27001, 27002 and 15408-1 are national standards.

5.3.4 National Cybersecurity Authorities

Georgian Law on Information Security set basis for the work of Data Exchange Agency (DEA) as the Competent National Cybersecurity Authority. It is a legal entity of public law of Georgia, governed by Ministry of Justice. It's the central agency in the field of Information Security and is established as a Single Point of Contact for matters of information and cybersecurity.

Part of DEA is its CERT (Computer Emergency Response Team) responsible for handling of critical incidents. Although intended for governmental networks and critical infrastructure it handles all critical incidents that occur in Georgia, as National CERT currently does not operate. Its area of work comprises warnings and alerts issuing, incident handling, security audits and assessments, workshops and training as well as intrusion detection services.

Georgia has alongside with DEA CERT also the Georgian Research and Educational Networking Association – CERT and Cyber Security Bureau – Computer incidents assistance department with responsibility for critical infrastructure in the defence sector.

National Regulatory Authority for energy sector[55] neither exercise any rights pertaining to cybersecurity nor monitor or assess implementation of Cyber security strategy, but cooperates in work groups on cybersecurity with organizations from energy sector and national cybersecurity authority – DEA.

A specialized unit of Central Criminal Police Department named Division for the Fight Against Cybercrime[56] operates also in Georgia. It is a 24/7 Single Point of Contact for matters of investigation and cybercrime prevention as it is the only investigative organization in the field of cyber incidents.

The process of planning, implementing of cybersecurity policies, designation and identification of CI and essential services is done through cooperation between state agencies of DEA, MoD, Ministry of Internal affairs

---

54 Data Exchange Agency of the Ministry of Justice of Georgia

55 Georgian National Energy and Water Supply Regulatory Commission

56 Cybercrime Division, Ministry of Internal Affairs of Georgia, Central Criminal Police Department, 10 G. Gulua str., Tbilisi 0114, Georgia.

and intelligence agencies with the Governments approval of operator and addition to the list of subjects of CI.

5.3.5   Cooperation and initiatives

Georgia developed initiatives for domestic cooperation between public and private sector through multi-stakeholder approach as well as international cooperation on basis of international treaties (either bi-/multi-lateral or ad hoc) with foreign entities and states as long as there is no domestic law that would prohibit such activities. Georgia reaffirms international cooperation as one of the main strategic principles for greater cybersecurity in the Cyber Security Strategy.

Cooperation within Energy Community Parties
As a contracting party, Georgia cooperates in the Cyber Security and Critical Infrastructure coordination group (CyberCG) of EnC for the purpose of promotion of high level of security of network and information systems and CI through strategic cooperation and exchange of information.
Cooperation with EU Member States
Georgia is cooperating with United Kingdom through the British Embassy in Georgia with experts and knowledge as well as experience sharing for support in establishment of criteria for definition and identification of critical infrastructure.
Partnership and cooperation between Estonia and Georgia began in 2013 as a part of working group of Ministry of defence with Estonian experts and support of NATO Liaison office in Georgia. It analysed situation related to cybersecurity and through training, awareness raising, sponsorship, sharing of information, experience, knowledge and experts it set the base for creation of strategic documents, CSB and facilitated building process of capabilities to prevent and respond to cyber threats, reduce vulnerabilities, minimize damage from cyber incidents and to protect information systems of Defence sector, by creating compliance with standards and critical infrastructure protection guidelines.
Partnership with Lithuania began in 2016 as a Bilateral Cooperation Plan between MoDs of Georgia and Lithuania. Representatives of the CSB participated within Lithuanian team in cyber exercise "Locked Shields 2017". Locked Shields is meant for training of security experts protecting national critical information systems, networks and services, and allowed Georgian representatives to check their capabilities and work with partner countries.
Cooperation with other parties
Close partnership and cooperation between United States of America and Georgia started in 2015 in context of Foreign Military Funding (FMF). Its goal was provision of necessary technology for cybersecurity in defence field. Cooperation continues with Memorandum on deepening of defence and security partnership from 2016 and was set for 5-year plan, to improve effectiveness of Cyber Security Program through Military to Military (M2M) activities. Georgian National Energy and Water Supply Regulatory Commission as the National Energy Regulator Authority cooperates internationally in the field of cybersecurity in the energy sector through different international bi- or multilateral programmes as well as support and aid programmes like USAID, NARUC and Utility Cyber Security Initiative for the Black Sea Region among others. Georgia is active in international cooperation with other countries as Georgia along with Ukraine, Moldova and Azerbaijan, developed GUAM[57] – regional organization that tackles issues in the cyber-domain among others. Through working groups on cybersecurity above mentioned parties discuss wide range of issues pertaining to combating and prevention of cybercrime,

---

[57] GUAM. *https://guam-organization.org/en/1st-meeting-of-guam-working-group-on-cyber-security/*

national legislation, procedures and operative situation as well as exchange information and good practices.

Public-private partnership

Companies in the energy sector cooperate with state agencies in different working groups with stakeholders from the energy sector, National Cybersecurity Authority and NRA for purpose of development of cybersecurity policy, cybersecurity standards defining process and identification of critical infrastructure.

Georgia also developed a volunteer collaborative platform to facilitate good practices and information sharing named "Incidents portal" under DEA.

5.3.6 Overview of education and training programmes

Education and training programmes are organized under DEA as educational activities are determined as DEA responsibility under the Law of Information Security[58]. At current time, there is only certification scheme and accreditation for Authorised auditors under the Law on Information Security. DEA also organizes training programmes on ISO standards (27001, 19011 and 31000).

Under the Law on Information Security organisations managing CI or providing essential services must appoint a "Cybersecurity specialist". At current time there is no officially recognised training or programme for a "Cybersecurity specialist" as well as no official training, college or university degree which could serve for acquisition of said title.

There are also educational and training campaigns with the aim to educate, spread awareness and introduce good practices of cybersecurity among general public like Information Security Awareness Raising Campaign of DEA.

5.3.7 Gaps against EU legislation and standards

Cybercrime legislation

Legislation against Cybercrime is well implemented in the legislative system and allows investigation and prosecution of offences pertaining to cybercrime.

Identification of CI operators and OES

To our knowledge, there is no legislation related to critical infrastructure and potential impacts on neighbouring countries.

Energy sector CII/ES operators have not yet been identified. The process of identification of energy sector critical information infrastructure operators is underway and is expected to be finished in 2019 and later encompassed in the legislation. Twenty-five organisations in the energy sector are identified in the working list of energy CI operators.

National NIS strategy

---

[58] *Law of Georgia on Information Security: https://matsne.gov.ge/en/document/view/1679424?publication=3*

Georgia cybersecurity strategies (2012-2015 and 2017-2018) have addressed cybersecurity challenges, risks and threats as well as identification of CII, however critical infrastructure of energy sector and specific risks and threats were not directly assessed or addressed. Strategies were in compliance with NIS directive provisions pertaining to national NIS strategies.

With the expiration of current Strategy 2017-2018, new National Cyber Security Strategy is in preparation with adoption foreseen in 2019. It is foreseen that energy sector cybersecurity requirements, strategic goals, risk and threat assessment will be addressed in the strategy.

National Cybersecurity Authorities: *Contact points*

To our knowledge there is no ECI protection contact point established. Ministry of Energy serves as a responsible Ministry for energy sector.

DEA serves as a National Cybersecurity Authority, SPoC and CSIRT. DEA and organizations in energy sector have an agreement on reporting of incidents and cooperation in the cybersecurity field.

Legislative system does not foresee communication with other EnC contracting parties in case of incidents.

Security plans and requirements

At the time being there is no ECI/NIS related legislation applicable to energy sector. Guidelines and obligations for the OES[59] encompass technical and organizational measures and are following ISO 27001 and ISACA recommendations. Provisions are in compliance with NIS directive provisions pertaining to cybersecurity requirements and will become mandatory for energy sector CII after the identification of operators.

Standardization

Georgia adopted international standards ISO through GeoSTM and therefore ISO 27001, 27002 and 15408-1 are national standards. Implementation of standards is currently not obligatory for energy sector.

Operators level

Energy sector stakeholders comprehend the importance of cybersecurity and are currently discussing the implementation of CIIP regulations, NIS and ECI directives. Some energy sector companies (electricity and gas) have started implementation or are considering the implementation of cybersecurity standards (e.g. ISO 27001). Energy sector operators are cooperating in a workgroup with other stakeholders (DEA, NRA, etc.) in the field of cybersecurity to prepare legislation and regulation for operators in energy sector in regards to cybersecurity measures and reporting provisions.

Cooperation

Although DEA has legislative possibility to coordinate and communicate cybersecurity incidents, there are currently no officially established communication channels with EnC CPs.

Private energy sector operators are active in international cooperation sharing cybersecurity related good practice.

DEA is the most important civil agency in the field of cybersecurity appointed to organise cybersecurity exercises, but no public, nor energy sector exercises took place in the last 5 years.

---

[59] *According to current legislation ES are government and public administration, however national energy regulator is not included in the list.*
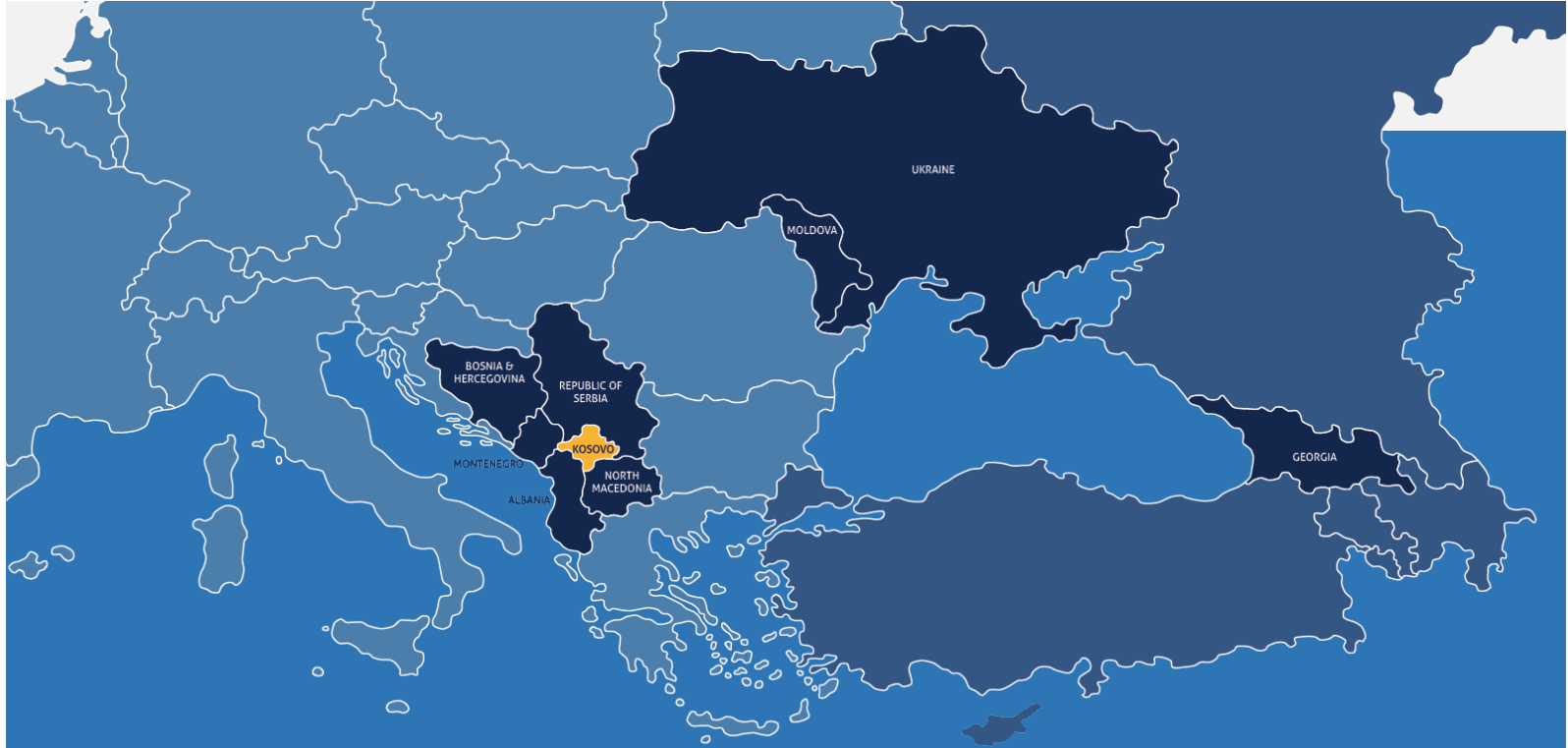
5.4 Kosovo*

As a part of Government Programme for 2015-2018 Kosovo* adopted National Cyber Security Strategy 2016-2019 for purpose of developing and strengthening the cybersecurity capabilities in accordance with international guidelines and practices as well as expressed the willingness to cooperate with other countries to contribute to higher level of cybersecurity on global scale. One of strategic goals is identification of CII operators as well as tighter regulation in the field of cybersecurity for those operators.

Kosovo* transposed the majority of ECI directive provisions into the national legislation while the NIS transposition is ongoing. CI operators must comply only with broad regulations defined in the Law on Critical Infrastructure pertaining to creation of operators' security plan for ICT systems.

Energy sector CI operators were identified on the basis of the Law on Critical Infrastructure taking into the account criteria that encompass impact of disruption but the detailed criteria as well as list of CI operators are classified.

Kosovo* is developing CII/ES cybersecurity through cross-sectorial approach for developing and strengthening of capabilities. The identification of CII/ES operators has not yet started and therefore they are not yet identified. Considering that the CI has been identified on the basis of Law on Critical Infrastructure, one should reasonably expect that energy sector CI operators will also be identified as CII/ES. At the time of the study there were no cybersecurity specific provisions related to CII/ES in the legislation. In some cases, energy sector stakeholders decided to follow ISO 27001/27002 guidance.

Based on the information received from Cybersecurity Authority is Kosovo* in the process of drafting new legislation on cybersecurity and it that will incorporate CII, but the adoption date is not yet known.

5.4.1 SWOT analysis

STRENGTHS

Law on Critical Infrastructure defines energy production, transmission, distribution and storage as CI sector as well as potential ECI with developed cross-sectoral criteria for risk analysis.

WEAKNESSES

Kosovo* is not a ratifying party of the Budapest Convention

Operators must comply only with broad regulation defined in the Law on Critical Infrastructure

NIS directive is only partially covered as identification of operators and legislative harmonization is underway.

OPPORTUNITIES

Kosovo* participates in many international initiatives and network platforms for development, experience sharing, trend analysis, mutual growth and development of global cybersecurity.

CI law requires from operators of CI to create "Operator security plan" based on the identification of key assets and resources, risks analysis encompassing relevant dependencies and interdependencies, and establish incident prevention, protection and mitigation systems. Operator security plan need to encompass key systems and there is opportunity to expand these.

THREATS

Kosovo* is in the process of drafting new legislation on cybersecurity and it will incorporate CII, but the adoption or end date is not yet known and it is not progressing in pace with state-of-the-art cybersecurity requirements.

International cooperation for implementation and execution of international and cross border initiatives is still largely dependent on external help of international organizations and donors.

5.4.2   European Critical Infrastructure and Essential Services legislation requirements

Identification of EnCCI and ES

Law on Critical Infrastructure transposes EU ECI Directive and defines energy production, transmission, distribution and storage as CI as well as potential ECI. Identification process followed approach laid out in the ECI directive and was led by Ministry of Internal Affairs. The List of CI operators as well as criteria for their identification is classified.

At the time of writing there has been no legislative or regulative document pertaining to identification of CII or OES in the energy sector or in general.

Law on Critical Infrastructure, 27.4.2018	*Lead: Ministry of Internal Affairs*

Criteria for CI designation and criteria for significant disruptive effect

Criteria for designation of CI, defined in the Law on Critical Infrastructure, encompass geographical reach, severity, public, economic, environmental and psychological impact, political influence, effect on public-health, intelligence-based threats and effect on other relevant dependencies and interdependencies. Detailed cross-cutting criteria for identification and impact assessment are defined but are classified. Identification of CII/ES is identified as a strategic objective in the Cyber Security Strategy. Although the identification of CI is based on the significance of the disruption, at the time of writing no specific criteria for the assessment of significant disruptive effect in the energy sector or in general CII/ES is laid out in the legislation. Considering that the identification of CI has been conducted based on the consequences of a disruption, same criteria can be potentially used for assessment and definition of significant disruptive effect.

Law on Critical Infrastructure, 27.4.2018	*Lead: Ministry of Internal Affairs*

National NIS strategy

National Cyber Security Strategy and Action Plan 2016–2019 was developed on the basis of ENISAs methodology and the content is in compliance with NIS directive provisions. The Strategy defines the need for identification and protection of CII/ES as well as strategic goals for harmonization of legislation with ECI and NIS directives. Additional strategic goals encompass institutional development and capabilities building, public-private cooperation, strengthening the incident response and international cooperation as well as development of educational and awareness raising campaigns.

For time period 2016-2019	*Lead: Ministry of Internal Affairs*

National CS organisational framework

Energy sector contact point for the coordination of CI protection with other states is not established and is in the development. Ministry of Internal Affairs is responsible for coordination activities pertaining to protection of CI, while Ministry of Economic Development, the Department of Energy and Mining is responsible for energy sector.

Law on Critical Infrastructure, 27.4.2018	*Lead: Ministry of Internal Affairs, Ministry of Economic Development[60]*

National CERT (KOS-CERT) was established in scope of Regulatory Authority of Electronic and Postal Communications (ARKEP). KOS-CERT is designated as National Cybersecurity Authority, NIS and CSIRT contact point.

---

[60] *Ministry of Economic Development, Square "Zahir Pajaziti", No.36, 10000 Prishtina, Republic of Kosovo**

Law on Electronic Communications, 9.11.2012	Lead: Regulatory Authority of Electronic and Postal Communications – KOS-CERT[61]

Energy sector CI operators are obliged to designate Security Liaison Officer for purposes of communication between the operator of CI and relevant government authority.

Law on Critical Infrastructure	Lead: Energy sector CI and OES

CI operators and ES providers security requirements

Operators' Security plans are foreseen in the Law on Critical Infrastructure. Operators of CI in the energy sector shall comply with provisions and define appropriate security solutions, conduct assessments of risks, threats and vulnerabilities and implementation of protection activities to assess, mitigate and neutralize identified threats and vulnerabilities. Organizations must implement organizational and technical measures for protection, control and communication systems, as well as information security systems.

At the time of writing, there was no specific cybersecurity legislative document pertaining to CII/ES in Energy sector. Under the Law on Critical Infrastructure, CI energy operators shall include essential ICT systems in the security plan. It is planned that the new Law on Cybersecurity which is in the drafting process will provide more specific and detailed cybersecurity requirements for CII/OES.

Law on Critical Infrastructure, 27.4.2018	Lead: Energy sector organizations; MIA oversight

Standardisation

Kosovo* adopted ISO 27001 standard, while old version of ISO 27002 standard has been withdrawn. Standards ISO 15408-1, 2, 3 are not adopted as national standards.

CII in the energy sector are not obliged to follow international standards as there are no technical provision that would regulate and obligate implementation of standards for cybersecurity. In some cases, energy sector stakeholders decided to use ISO 27001/27002 standards guidance even if by law they are not obliged to do so.

Lead: Kosovo Standardization Agency

Kosovo* is geographically positioned between other CPs with possible cascading effects. North Macedonia and Kosovo*, signed in 2019 a Memorandum of Understanding on the Energy Sector under which they plan to revitalize electricity interconnection lines and potentially build a new gas interconnection, which would bring gas from nearby Skopje to Kosovo* thereby extending security of supply and the need for coordination at cybersecurity level too.

5.4.3   Legislation at the national Level

Strategy and action plans

Kosovo* has adopted National Cyber Security Strategy and Action Plan 2016 – 2019[62] in December of 2015 with the objective of addressing issues in the field of cybersecurity. With strategic goals set for strengthening

---

[61] *KOS-CERT, st. Bedri Pejani, nr. 23., 10000 Prishtina, Republic of Kosovo**

[62] *National Cyber Security Strategy and Action Plan 2016–2019*

the protection of critical information infrastructure, institutional development and building of capabilities and public-private partnership, developing and strengthening capabilities for incident response and international cooperation.

One of Strategy's goals is building of capabilities and strengthening the protection of critical infrastructure, including both electricity and gas. Strategy aims to create safe and secure environment by setting measures and actions for protection of CII disruption or destruction of which would have serious consequences to essential and vital services of state and society functions. Kosovo* recognizes protection of CII as the main priority in cybersecurity. Strategy also recognizes the need for legislative and rule level harmonization with international legislative documents and directives for the purpose of maintaining and securing CI during everyday operations as well as during crises.

Republic of Kosovo* recognizes the need to identify critical information infrastructure and to manage sectors with best possible measures for their protection. The process of identification will follow, according to Strategy, ENISA's "Methodologies for the identification of Critical Information Infrastructure assets and services"[63]. There will be multiple steps for CII designation from determine critical sectors and services, identification of infrastructure that is needed for operations, introduce protection level criteria and measures needed as well as establish monitoring and exercises, to train and educate operators about possible incidents, disruptions and counter measures.

Legislation against cybercrime

Republic of Kosovo* is not a ratifying party of the Budapest Convention, but even so Kosovo* did transpose all necessary provisions defined in the Convention and harmonized the national legislation.

Budapest Convention is implemented in: Law on Prevention and Fight of the Cyber Crime, Criminal Code, Constitution of the Republic of Kosovo*, Law On Electronic Communications, Law on International legal cooperation in criminal matters.

Energy sector relevant cybersecurity legislation

The Law on Critical Infrastructure[64] regulates cybersecurity in the energy sector but encompasses only high-level requirements and needs further development in order to ensure strategic goals implementation based on the Strategy. The Law defines energy production, transmission, distribution and storage as CI sector as well as potential ECI.

At the time of writing, there was no cybersecurity specific legislation pertaining to energy sector defining more detailed and specific requirements.

In addition, cross-sectorial criteria for risk analysis resulting in CI designation encompass severity, geographical scope, public, economic, environmental and psychological impact, political influence, public health effect, intelligence-based threats and effects on other relevant dependencies and interdependencies. Detailed criteria for identification of CI are classified.

---

[63] *ENISA: Methodologies for the identification of Critical Information Infrastructure assets and services.* *https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis/at_download/fullReport*

[64] *Law on Critical Infrastructure. https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=16313*

Although broad, criteria used for the identification of CI can be also used for assessment and definition of significant disruptive effect.

The above-mentioned law does not go into detail about cyber dimension but it requires from CI operators to create "Operator security plan" based on the identification of key assets and resources, risks analysis encompassing relevant dependencies and interdependencies, and establish incident prevention, protection and mitigation systems. Operator's security plan shall encompass key ICT systems.

The process of identification of stakeholders and institutions was performed by the Ministry of Internal Affairs but the list of operators and institutions is classified.

New Law on Cybersecurity is in the drafting process with unknown adoption date. Therefore, there are no recommendations or prescriptions of minimum standards for operators.

Kosovo* adopted ISO 27001 standard, while ISO 27002 standard has been withdrawn.

Other cybersecurity related legislation

Kosovo* adopted Law on Electronic Communications for the purpose of defining competent authorities in the field of electronic communications and postal services. Designated entity is Regulatory Authority for Electronic and Postal Communications. The law establishes the responsibilities and work area of the regulatory Authority as well as regulate public electronic communication providers, services and networks.

Kosovo* adopted Regulation on technical and organizational standards on the safety and integrity of networks and/or services for electronic communication as underlying infrastructure for provision of electricity and gas services. It defines rights and obligations of operators of networks and/or services of public electronic communications and defines technical standards for security, integrity and operation of networks and services.

5.4.4   National Cybersecurity Authorities

National Cyber Security Strategy and Action Plan for 2016-2019 designates the stakeholders in the process of establishing and implementing the strategy for strengthening the cybersecurity. The Strategy designates Ministry of Internal Affairs (MIA) as the National Coordinator for Cyber Security. MIA is responsible for coordination with other stakeholders, monitoring progress and reporting on the implementation process in addition to drafting periodic reports.

MIA, along with the coordination activities, has a functional role in the implementation of the Strategy with its law enforcement agency – Kosovo* Police. Kosovo* Police has a specialized unit under Department for Cyber Crime[65] with responsibilities for combating all forms of cybercrime and supporting other structures of Kosovo* Police with technical capabilities. Above mentioned strategy states that the Kosovo* Police will serve as a single point of contact 24/7 for international cooperation in the field of cybercrime.

Strategy foresees creation of National Cyber Security Council (Council) for the purpose of strengthening the governmental as well as private sector cooperation. The purpose of cooperation under the Council umbrella

---

[65] *Sector for Cybercrime Investigation, Directorate for Organised Crime Investigation65., Kosovo Police, Luan Haradinaj street – Rexhep Luci, 10000 Prishtina, Republic of Kosovo.*

would be to coordinate recommendations and implement preventive measures at the strategic level. The Council would be comprised of MIA, Police, Forensics Agency, Security Forces, Intelligence Agency, and Agency for Information Society, Security Council, Ministry of Finance, Customs, Ministry of Education, Science and Technology, Ministry of Foreign Affairs, Regulatory Authority for Electronic and Postal Communications as well as Central Bank of Kosovo. Among these, the representatives of private and academic sector would be included on the technical level. At the time of writing, it is unclear whether such cooperation body is functional.

Regulatory Authority for Electronic and Postal Communications (ARKEP)[66] is national regulatory authority for the field of electronic communications. ARKEP hosts national CERT: KOS-CERT. KOS-CERT as national and governmental CERT can cooperate with other organizations including those in the energy sector however there is no legislative regulation obliging them to do so. KOS-CERT is intended as awareness raising and incident response coordinating body within Kosovo. Its incident response coordination efforts are set as a bridge between affected parties, establishing communication channels, gathering information, notifying involved and collecting statistics about incidents in the country. KOS-CERT conducts obligations relating to the Law on Electronic Communications, National Strategy for Cyber Security and Regulation on Technical Standards and Security Networks and Services. KOS-CERT cooperates with law enforcement agencies of Kosovo* and other CERTs, for the purpose of networks, services and users protection. KOS-CERT developed and online platform for reporting of cybersecurity incidents.

Along with KOS-CERT there are other national CERTS developed in Kosovo. CERT for Kosovo Police (CERT-KP-RKS) is developed for coordination and managing of cyber incidents to protect the Police systems and services. Security Forces of Kosovo developed their own CERT for the purpose of Kosovo Security Forces systems/services protection as well as addressing incidents in scope of mission assurance process. Ministry of Internal Affairs developed CERT for purposes of protecting sensitive registers and systems of MIA as well as incidents response and coordination. UBT-CERT was developed for the University of Business and Technology for the purpose of cybersecurity incident management and response to protect the University infrastructure and systems as well as personal and sensitive data.

National Regulatory Authority[67] for energy sector neither exercise any rights or obligation pertaining to cybersecurity nor monitor or assess implementation of Cybersecurity strategy.

5.4.5 Cooperation and initiatives

Kosovo* defined a strategic goal in the to play an active role in the cybercrime field by fostering European and global cooperation, exchange of information, development of voluntary schemes and legally binding regulations, holding of transnational exercises and cooperation projects as well as by prosecuting criminal offences. Representatives of international organisations and domestic private sector were a part of the Working Group established for the creation of national strategy.

It is important to note that international cooperation for implementation and execution of international and cross border initiatives is still largely dependent on external assistance of international organizations and donors[68].

---

[66] *Regulatory Authority for Electronic and Postal Communications. http://www.arkep-rks.org*

[67] *Energy Regulatory Office*

[68] *Diplo. Cyber Security in the Western Balkans: Policy Gaps and Cooperation Opportunities. https://www.diplomacy.edu/sites/default/files/Cybersecurity%20in%20Western%20Balkans.pdf*

Cooperation within Energy Community Parties

As a CP, Kosovo* participates in the EnC's Cyber Security and Critical Infrastructure coordination group (CyberCG) for the purpose of achieving high level of security of network and information systems and CI promotion through strategic cooperation and exchange of information.

Cooperation with EU Member States

Kosovo* participated in the EU-funded project ENCYSEC[69] for the cooperation, strengthening and enhancement of cybersecurity. One of the initiatives was the establishment of the KOS-CER and the creation of small but skilled team of cybersecurity professionals responsible for incident response, reporting and coordination, as well as dissemination of information. One of tasks assigned to KOS-CERT was the national coordination of awareness-raising campaigns related to cybersecurity. ENCYSEC also supported Kosovo* with regards to development of cybersecurity strategies as well as fostering the cooperation in the field of government, private and academic sector, dissemination of information and capacity building.

The European Union with the support of the Council of Europe launched the project CyberCrime@IPA[70] to promote and support the fight against cybercrime in Kosovo. The project helped raising the awareness of the involved stakeholders, as well as enhanced the cooperation between the public and the private sector, along with the support and collaboration from international entities and foreign states.

The iPROCEEDS[71] project between EU, CoE and Kosovo* focused on the establishment of the necessary measures and remedies situations related to incidents involving unauthorised data access and possession, as well as incidents of financial nature.

The strategic goal of Kosovo* is to join European Union and therefore, according to its strategic plan, it targets close collaboration with ENISA, for the purpose of protection of CI, dissemination of information, as well as international cooperation.

KOS-CERT has signed a Memorandum of Understanding with the National Emergency Response Centre (MKD-CIRT) of Republic of North Macedonia and National Agency for Computer Security of the Republic of Albania (ALCIRT).

Cooperation with other parties

A cooperation program with the United States International Criminal Investigative Training Assistance Program (ICITAP) for education and training of law enforcement units and prosecutors in the field of cybersecurity was carried out. Kosovo* cooperates with the organization for Cybersecurity Alliance for Mutual Progress[72] (CAMP) for the purpose of capacity building increasing the awareness level related to cybersecurity. It also involves, dissemination of information, trend analysis, and mutual growth and development of global cybersecurity standards and countermeasures.

Kosovo* participates in a number of international initiatives and programmes, such as the programme for Effective Regulation of Cybersecurity, which has been organized by U.S. Agency for International Development (USAID) and National Association of Regulatory Utility Commissioners (NARUC).

Kosovo* cooperates also with OSCE[73] in the field of Cyber/ICT security for strengthening cybersecurity of institutions. It assists development and monitoring of the National Cyber Security Strategy implementation, as well as plays an active role in the working group on cybersecurity of Kosovo*. OSCE with local law enforcement bodies organizes workshops and conferences for addressing the cybercrime, international or domestic cyber threats, towards strengthening cybersecurity in Kosovo*.

---

[69] Enhancing Cyber Security. http://www.encysec.eu/web/

[70] CyberCrime@IPA. https://www.coe.int/en/web/cybercrime/cybercrime-ipa

[71] iPROCEEDS Kosovo. https://www.coe.int/en/web/cybercrime/iproceeds

[72] Cybersecurity Alliance for Mutual Progress (CAMP). https://www.cybersec-alliance.org/

[73] Cyber/ICT Security of Mission to Kosovo*. https://www.osce.org/mission-in-kosovo/cyber-ict-security

United Nations Development Program[74] also assists Kosovo* in creation of strategic, legislative and regulatory framework for the field of cybersecurity.

<div style="background:#2e75b6;color:white;font-style:italic;font-weight:bold;padding:4px">Public-private partnership</div>

Kosovo* started developing a public-private partnership through a working group for the preparation of the National Cyber Security Strategy. The working group involves multiple stakeholders, ranging from governmental and public institutions as well as professional associations, private sector organizations, civil society and international partners. The working group envisaged the creation of a specialized body for cybersecurity. One of the achieved goals in the National Cyber Security Strategy and Action Plan for 2016-2019 is the development of the cooperation between the public and the private sector in the field of cybersecurity for exchange of information and implementation of good practices in the energy sector, as most of the institutions providing and managing energy infrastructure are private.

Kosovo* recognizes the need to establish information exchange and implementation of good practices as described in the above-mentioned Strategy and also to create an organizational strategic basis for cooperation and coordination in the implementation phase of the measures. National Cyber Security Council would be the appointed agency for coordination of such actions with the private sector, academia and other stakeholders, but it is not clear whether National Cyber Security Council is operational.

Overview of education and training programmes

Training initiatives and programmes in information security at the current time do not take place or are organized ad hoc within institutions of public or private sector including energy sector. Organizations receive trainings organized by law enforcement, Universities of Kosovo* and by accredited international or private organizations. Currently there is neither official education or training for Cyber Security Specialists in the energy sector nor any requirement for energy or CI organizations defined under legislative system to have Cyber Security Specialists employed in the organization exists.

Kosovo* has developed an educational system that creates opportunity as well as educates specialists from information and cybersecurity. Through courses in the Universities in Kosovo*, there is a lot of options for enrolling in bachelor or master's degree study on topics of IT and data security, information assurance and security, cryptography, forensics etc.

There are multiple awareness raising campaigns organized in Kosovo* and are being conducted by KOS-CERT. KOS-CERT organizes awareness raisings for target demographic for safe use of internet as well as publishes weekly notifications on cybersecurity news and threats. Kosovo* recognizes the need to create joint activities between public and private sector for the purpose of education in the National Cyber Security Strategy 2016-2019. Such cooperation would allow private and public sector to exchange advices and set basis for cybersecurity curriculum for the purpose of certification of information security experts.

---

[74] *United Nations Development Program: Kosovo* Safety and Security Project.*
https://reliefweb.int/sites/reliefweb.int/files/resources/KSSP%2520Brochure_Final%2520ENG%2520sz.pdf

5.4.6 Gaps against EU legislation and standards

Cybercrime legislation

Even though Kosovo* did not ratify the Budapest convention, it has developed Law on Prevention and Fight against Cyber Crime with assistance of Council of Europe. All provisions of Budapest convention are incorporated into legislative system and allow investigation and prosecution of offences pertaining to cybercrime.

Identification of CI operators and OES

The identification of CI has been conducted based on the Law on Critical Infrastructure, list of CI operators is classified. Criteria for significant disruptive effect are not defined in the legislation.

CII/ES operators have not been identified yet as there is no legislative base. One can reasonably expect that the energy sector CI will be also designated as CII/OES operators.

At the time of writing no specific criteria for the assessment of CII/OES significant disruptive effect is laid out in the legislation.

National NIS strategy

The National Cyber Security Strategy of Republic of Kosovo 2016-2019 was developed in accordance with ENISA guidelines and addresses cybersecurity challenges, risks and threats, education and awareness raising, institutional, legal and regulatory mechanisms, implementation and monitoring process. Action plan for implementation of the Strategy was created.

One of the strategic goals identified in the above-mentioned Strategy is the identification of CI and OES, but the strategy neither directly address the energy sector, nor energy specific risks and threats to infrastructure.

National Cybersecurity Authorities: Contact points

Legislative system on protection of CI is defined with Law on Critical Infrastructure and sets obligations for reporting of CI to Ministry of Internal Affairs, while reporting of cybersecurity specific incidents and issues in the energy sector are not mandatory. ECI Protection contact point SPoC for ECI directive is in development.

KOS-CERT is designated as the national cybersecurity authority and SPoC for incident reporting and coordination. Ministry of Economic Development is the responsible Ministry for the energy sector, Ministry of Internal Affairs serves as coordinating party for identification and protection of CI as well as coordination of cybersecurity.

Security plans and requirements

CI operators in energy sector are obliged by the Law on Critical Infrastructure to develop an operator security plan encompassing incident prevention. Personnel, facility, physical infrastructure and ICT protection and mitigation measures should be also covered in the plan.

Standardization

Kosovo* adopted ISO 27001 standard, while obsolete ISO 27002 standard has been withdrawn. ISO 15408-1, 2, 3 has not been adopted as national standards.

Technical cybersecurity guidelines and obligations pertaining to standardization for the OES and CI are not defined in legislative system. Operators of CI/ES are not obliged to incorporate international standards or good practices nor is there any standardization relating to ICT products or services. Institutions of energy sector have started implementing ISO 27000 series standards even if there is no law obligating them to do so.

Operators level

CI operators in the energy sector must prepare security plan as foreseen in the Law on Critical Infrastructure. However, legislation requirements are high-level, which could lead to different levels and maturity of implementations. Public and private operators in the energy sector comprehend the importance of cybersecurity and are starting implementation of standards and international good practices (e.g. ISO 27001/27002 standards).

Cooperation

Organizational structures to communicate or liaison with owner/operator of the EnCCI and the relevant Contracting Party authority are currently not set in practice nor are they foreseen in the legislation.

Although the National Cyber Security Strategy 2016-2019 does foresee development of stronger cooperation between a public, private and academic sector a public-private cooperation platform is currently not set in practice.

Companies in the energy sector do not cooperate cross-border. There is no appointed institution for organization of cybersecurity exercises and therefore there were no organized for energy sector in last 5 years.

Kosovo* cooperates internationally with different international organizations in the field of cybersecurity (EnC, OSCE, EU, CoE, ICITAP, USAID, NARUC etc.).

5.5 Moldova

"National Cybersecurity Program 2016-2020" that provides a sound basis for the development of cybersecurity was established based on the needs recognized in the strategic document "Digital Moldova 2020".

ECI provisions are mainly transposed to the local legislation with the exception of cross border CI protection contact point establishment. Moldova adopted Anti-Terrorist Critical Infrastructure Protection Regulation for the purpose of identifying operators of CI in the energy sector, with electricity, gas and oil subsectors. The list of energy CI operators is classified and not publicly available. Identification of energy sector operators was performed on the basis of disruption severity, same criteria could be used for significant disruptive effect assessment.

Public energy sector CI operators are obliged to comply with the Government decision on Minimal Requirements in Cyber Security defining cybersecurity measures that are following ISO 27002 standard. However, privately-owned CI operators are not obliged to comply with before mentioned Decision requirements and there is also no general or CI/energy sector specific legislation that would regulate cybersecurity in the private sector.

Although NIS directive provisions are not directly transposed into the national legislation the majority of NIS requirements including CSIRT, SPoC and national cybersecurity authority are covered in the CI and related cybersecurity legislation.

Identification of CII/ES operators has not been performed but the identification is one of goals of the new Information Security Strategy. It is reasonable to expect that major energy sector operators will be identified as CI/ES operators thus the impact of this shortcoming to major energy sector operators is limited.

A new Information Security Strategy 2019-2024 which foresees identification and designation of CII[75] and information systems of vital importance (ES) is in the adoption process. One of strategic goals is to adopt legislation pertaining to elaboration of cyberdefence measures for the protection of CII/ES operators.

---

[75] *Cybersecurity related strategies use term CI for CII, while Anti-terrorist CI Protection Regulation identifies only the CI.*

5.5.1 SWOT analysis

STRENGTHS (S)

New Information Security Strategy for 2019-2024 has been developed in 2018 along with the Action plan for implementation and is in the adoption process. One of the strategic goals is elaboration of cyber defence measures for protection of national CI. While the strategy does not explicitly mention energy sector, based on the Anti-terrorist CI protection regulation, energy sector is identified as CI and therefore the Strategy is applicable to the energy sector CI protection.

WEAKNESSES (W)

NIS directive security provisions for CII and ES are implemented in the Moldova CI legislation but the identification of CII and operators of ES is currently not covered. Although Anti-terrorist Center is designated as a coordinating and point of contact for matters of CI protection Moldova did not designate an ECI contact point.

The list of energy CI operators is classified and not publicly available. The identification of CI and operators of ES has not yet started and therefore energy sector operators of CII and ES are not yet identified – though expected to be classified as CI

OPPORTUNITIES (O)

Moldova is very active in cooperation initiatives, it organized Regional Cyberweek in 2018 which was supported by EU and ENISA as well as Embassy of United States of America. Its purpose was to share experience and good practices in the field of cybersecurity, solutions, trends, strategies and to establish partnerships with emphasis on international cooperation.

THREATS (T)

Private owned energy sector operators of CI do not need to comply with the related legislation but the impact cannot be assessed because the list of (energy sector) CI operators is classified.

5.5.2 European Critical Infrastructure and Essential Services legislation requirements

Identification of EnCCI and ES	
Identification of CI has been conducted under Anti-terrorist Critical Infrastructure Protection Regulation and identifies energy sector as CI. The list of CI operators is classified and not publicly available. The identification of CII/ES has not yet been conducted, but the need to do so is identified in the draft of the Information Security Strategy 2019-2024.	
Critical Infrastructure Protection Regulation, 26.4.2018	*Lead: Information Security and Cyber Security Service (STISC)*

Criteria for CI designation and criteria for significant disruptive effect	
Criteria for the identification of CI are defined based on the significance of disruption on multiple levels. Criteria for Severe disruption: More than 10,000 individuals are affected, Disruption and recovery activity lasting more than 6 months, Economic impact is more than 100 million Leu (5.07 million €). Criteria for significant disruptive effect are not established, but the identification criteria for CI can be potentially used for this purpose as it encompasses disruption categories and thresholds.	
Anti-terrorist Critical Infrastructure Protection Regulation, 11.7.2019	*Lead: Antiterrorist Center of the Information and Security Service of the Republic of Moldova*

National NIS strategy	
National Cybersecurity Programme 2016-2020 addresses NIS directive provisions.	
For time period 2016-2020	*Lead: Ministry of Information Technology and Communications*
New Information Security Strategy 2019-2024 is in the adoption process.	
For period: 2019-2024	*Lead: Responsible Institutions*

National CS organisational framework	
Contact point for protection, identification coordination and implementation of measures laid out in the Anti-terrorist Critical Infrastructure Protection Regulation is Anti-terrorist Center of the Information and Security Service. Responsible Ministry for energy sector is Ministry of Economy and Infrastructure.	
Anti-terrorist CI Protection Regulation	*Lead: Ministry of Economy and Infrastructure, Anti-terrorist Center of IS and Security Service.*
Governmental Decision on Minimum Requirements in Cyber Security defines Ministry of Economy and Infrastructure with its Information and Communication Technology sector as national authority for cybersecurity as well as NIS contact point[76]. CERT-GOV-MD[77] is designated as national CERT.	
Governmental Decision on Minimum Requirements in Cyber Security, 28.3.2017	*Lead: Ministry of Economy and Infrastructure*
Governmental Decision on Minimum Requirements in Cyber Security sets obligation for public CI operators to: designate person responsible for cybersecurity and to report cybersecurity incidents, risk assessments, action plans and established measures to national authority (CERT-GOV-MD).	
Governmental Decision on Minimum Requirements in Cyber Security, 28.3.2017	*Lead: Ministry of Economy and Infrastructure*

---

[76] *Ministry of Economy and Infrastructure, Piata Marii Adunari Nationale, nr.1, Chisinau.*

[77] *CERT-GOV-MD, Piata Marii Adunari Nationale, nr.1, Chisinau.*

CI operators and ES providers security requirements	
Regulation on protection of CI requires from CI energy sector operators to perform risk assessment, implement protection measures, designate responsible person for protection of CI, annually report any security plan changes and ensure that information reported to the Anti-terrorist Center is complete and valid. It also requires that CI operators participate in the training, planning and consulting activities coordinated by the Anti-terrorist Center.	
Anti-terrorist CI Protection Regulation	*Lead: Energy sector operators; Anti-terrorist Center of IS and Security Service*
Governmental Decision on Minimum Requirements in Cyber Security sets obligation for public energy sector CI operators to implement cybersecurity measures. Measures encompass action plans, development of cybersecurity policy, definition of responsibilities for personnel, development of internal regulations and recovery procedures, establishment of communication channels with national authority and other relevant stakeholders and document technical controls. CI operators should regularly report activities pertaining to documentation, incidents, measures and assessments conducted to the Ministry of Energy and Infrastructure.	
Regulation (no. 22) on the content and method of documenting security measures.	*Lead: Energy sector operators; Ministry of Economy and Infrastructure*

Standardisation	
Moldova adopted SM EN ISO/IEC 27000, 27001, 27002, 27011 and 15408-1-2-3[78] standards. In addition, 15 ETSI standards in the "Cyber Security" category were approved as Moldovan standards. Standards are not directly referenced in the legislation nor are mandatory for energy sector CI operators.	
	Lead: National Institute of Standardization; Ministry of Economy and Infrastructure

Moldova is gas transit country for Russian gas to Turkey and the Western Balkans (via the Trans Balkan pipeline). Natural gas is the major fuel in Moldova, providing more than half of the total primary energy supply therefore gas operators needs to focus on best practices in cybersecurity design and operation. Moldova has an imbalanced distribution of electricity generation and insufficient capacity of the interconnection lines with Europe (both South-East and Western), limiting cascading effects to CP Ukraine and EU Member State Romania. National risk of country-wide blackout in case of cyber-attack in high due to the same reason.

5.5.3   Legislation at the national level

Strategy and action plans

Strategy Digital Moldova 2020 defines the need to strengthen CI cybersecurity and adopt legislation in the field of cybersecurity and protection of CI.

National Cybersecurity Program 2016-2020 for strengthening and building cybersecurity capabilities strategic goals encompass elaboration and approval of the legal framework for the identification and designation of national CI and information systems of vital importance as well as assessment and reporting on the status and level of security of national CI.

---

[78] *http://estandard.md/Standard/SearchResult*

Program Action plan has been developed for the implementation of strategic goals, encompassing legislative framework, development of defence and military capabilities to protect CI and services for national defence. Moldova recognized the need to conduct and organize educational activities for personnel in public and private sector as well as operators of CI. Strategic goals encompass strengthening of capabilities of National Response Centre for incident response, cybersecurity analysis, coordination and response capabilities as well as development of training initiatives for qualified specialists.

New Information Security Strategy for 2019-2024 has been developed in 2018 along with the Action plan for implementation and is in the adoption process[79]. One of the strategic goals is elaboration of cyber defence measures for protection of national CI. While the strategy does not explicitly mention energy sector, based on the Anti-terrorist CI protection regulation, energy sector is identified as CI and therefore the Strategy is applicable to the energy sector CI protection.

Legislation against cybercrime

Republic of Moldova has started to create a better internal political and legislative system by ratifying the Budapest Convention in 2009, and implementing all necessary provisions from it into national legislation. Moldova adopted and ratified the additional protocol to the Budapest Convention. It is important to note that Republic of Moldova identified shortcomings of the legal system pertaining to cybercrime in its Information Security Strategy 2019-2024 and is working towards implementing needed changes.

Budapest Convention is implemented in: Criminal Procedure Code, Criminal Code, Law on Preventing and Combating Cybercrime.

Legislation targeting OESs

Based on the Anti-Terrorist Critical Infrastructure Protection Regulation energy sector is designated as critical and operators of CI are identified. Energy sector CI encompasses oil and gas storage activities and pipelines, transport and distribution of electricity, heating, gas and oil. The list of CI operators is classified and not publicly available. Same Regulation and CI identification is used as a basis for other strategic documents and legislative provisions including ones pertaining to cybersecurity and security of information and network systems (see section on Strategy and action plans above).

Table 5: Criteria for designation of CI - Moldova could be also used for the definition of significant disruptive effect in connection to cybersecurity, as there is no other yet adopted.

---

[79] *Information Security Strategy has been developed for timeframe 2018-2023, but with adoption delayed, the implementation is planned to begin in 2019-2024 timeframe.*

Criteria	Severe	High	Medium	Low
Security (deaths/injuries)	10,000 people	1,000-10,000	100-1,000	< 100
Economic	>100 million Leu (20,936,020€)	10-100 million Leu (2,093,602€-20,936,020€)	1-10 million Leu (209,360€-2,093,602€)	< 1 million Leu (209,360€)
Geographical	Regional	10-100 km^2	1-10 km^2	< 1 km^2
Social	Disruption lasting more than 6 months	1 week – 6 months	1 day – 1 week	< 1 day

Table 5: Criteria for designation of CI - Moldova

Public operators of CI in the energy sector are obliged by the Governmental decision to implement Minimum Requirements in Cyber Security[80]. The decision mandates reporting activities pertaining to documentation, incidents, measures and assessments conducted to the Ministry of Energy and Infrastructure. The decision follows ISO 27002 standards, but it should be emphasized that private owned energy sector operators of CI do not need to comply with the above-mentioned decision, neither are obliged to follow any other energy sector specific or general cybersecurity legislation.

Although the standards are not directly defined in the Governmental decision, Moldova among other adopted 15 ETSI standards in the field of cybersecurity. Along with ETSI, Moldova also adopted 22 ISO standards and overall 214 other international standards in the field of processing, storing, securing access, securing of information systems and others in the field of ICT and cybersecurity. Among them SM EN ISO/IEC 27000, 27001, 27002, 27011 and 15408-1-2-3[81]. E-Governance centre is designated as the responsible authority for auditing of compliance with information security standards of organizations and institutions of Moldova.

Other general cybersecurity related legislation

Governmental decision No. 201 from 2017 brought the Minimum Requirements in Cyber Security for public organizations and institutions, setting the base for obligation to follow such standards and requirements. Among others it defines access controls, physical and operational security and secure data exchange on two levels – basic and advanced cybersecurity level but it is not relevant for energy sector.

---

[80] *Encompassing: physical and technical security, designation of a responsible person for cyber security, establish cyber security policies, develop training initiatives and raise awareness, cooperation in exercises, preparation of cyber security action plan and policy, create internal cyber security policies pertaining to continuity of work, recovery and disaster management plan, set access controls and responsibilities, documentation of measures, audits, penetration tests and assets, use of encryption, implementation and upgrading of ICT, use of specialized software and hardware, restriction of technologies and application.*

[81] *http://estandard.md/Standard*

5.5.4   National Cybersecurity Authorities

A multi-institutional approach between ministries has been developed in Moldova to address cybersecurity. Ministry of Economy and Infrastructure[82] is designated as public central competent authority for the field of cybersecurity and NIS SPoC. It coordinates activities and creation of capabilities for cybersecurity with other Ministries, agencies and institutions.

Anti-terrorist Center of the Information and Security Service of Republic Moldova is the responsible authority for the coordination of designation and analysis of CI with all stakeholders and ministries. Information and Security Service develops proposals for ensuring information security, protection of state secrets, strategy and implementing policies and providing, creating and ensuring communications, technology and cryptography for the ICT of national importance.

Information Security and Cyber Security Service (STISC) CERT named CERT-GOV-MD[83] is also responsible for energy sector, one of main priorities is establishment of strategic relationships to improve cybersecurity of national CI. CERT-GOV-MD is the main contact point for reporting, coordination and assisting in response to incidents, facilitates exchange of information and good practices, disseminates information and organizes awareness campaigns. It helps organizations with implementation of active and reactive cybersecurity measures to reduce risks.

Besides CERT-GOV-MD there are two other CERTS which are not related to energy sector CI. CERT Orange Moldova[84] is a team developed under Moldovan ISP provider Orange and responsible for company's and cybersecurity. CERT-md[85] is developed under national research and educational network infrastructure for the purpose of gathering, registering and analysing incidents in academic and education field.

National Energy Regulatory Agency (NRA) does not exercise any rights or obligation pertaining to cybersecurity nor does it monitor or assess implementation of Cyber security strategy.

Moldovan main 24/7 contact point in investigative field of cybercrime and international cooperation is established under the General Prosecutor's office Section for Information Technology and for Fighting Cybercrime[86]. Specialized police unit is developed under Moldovan MIA – General Police Inspectorate named Center for Combating Cyber Crime[87] of National Inspectorate for Investigations is designated for police-to-police cooperation as well as provisions of technical assistance and advice, and would need exercise to demonstrate efficiency of measures in case of energy system cyber-attack.

---

[82] *Governmental Decision on Minimum Requirements for Cyber Security designates Ministry of Economy and Infrastructure (former Ministry for Information Technology and Communication) as the responsible authority: For execution of the Decision and overseeing the implementation of minimum requirements in all sectors; Central point for reporting of incidents of public sector institutions as well as reporting of results of audits and penetration tests, discovered risks and threats and implemented countermeasures; National Authority for energy sector and responsible for implementation of the mandatory cyber security requirements that are coordinated by the Information and communication technology sector of the same Ministry.*

[83] *Information Security and Cyber Security Service: CERT-GOV-MD. https://stisc.gov.md/ro/content/servicii-cert*

[84] *ORANGE Moldova – CERT. https://cert.orange.md/ro/about*

[85] *National research and educational network infrastructure – CERT. https://cert.md/about-us/*

[86] *Section for Information Technology and for Fighting Cybercrime, General Prosecutor's Office, 26 Banulescu Bodoni st., Chisinau*

[87] *Center for Combating Cyber Crime, National Inspectorate for Investigations of the General Inspectorate of Police, Chisinau*

5.5.5 Cooperation and initiatives

Moldova recognizes international and domestic cooperation, in the Cyber Security Program 2016-2020 and Information Security Strategy 2019-2024, as one of the facilitators for greater cybersecurity on national, regional and international level as well as understands the importance of addressing issues of information and hybrid warfare through international cooperation and prohibition of such actions.

Cooperation within Energy Community Parties
As an EnC contracting party Moldova cooperates in the EnC's Cyber Security and Critical Infrastructure coordination group (CyberCG) for the purpose of promoting higher level of network, information systems and CI security through strategic cooperation and exchange of information.

Cooperation with EU Member States
Moldova is cooperating with European Union in the programme EU4Digital: Improving Cyber Resilience in the Eastern Partnership Countries[88]. Purpose of the programme is to strengthen Moldovan cyber-resilience and criminal justice capabilities through individual, regional and multi-national approach as well as EU best practices and rule of law. Main objectives described are strengthening the international cooperation, implementation of legal framework and compliance with NIS directive, awareness raising, increased participation between public and private sector, strengthening of protection of CI, increase operational capacities of national CSIRTs and incident management among others.
Moldova organized Regional Cyberweek in 2018 which was supported by EU and ENISA as well as theEmbassy of United States of America. Its purpose was to share experience and good practices in the field of cybersecurity, solutions, trends, strategies and to establish partnerships with emphasis on international cooperation[89].

Cooperation with other parties
Republic of Moldova is active in international cooperation with other countries as Moldova along with Ukraine, Georgia and Azerbaijan, developed GUAM[90] – regional organization which tackles issues in the cyber-domain among others. Through working groups on cybersecurity above mentioned parties discuss wide range of issues pertaining to combating and prevention of cybercrime, national legislation, procedures and operative situation as well as information and good practices exchange.
Moldova cooperates within organization for Cybersecurity Alliance for Mutual Progress[91] (short: CAMP) for purpose of building its capabilities and level of cybersecurity. It is developed as a network platform

---

[88] *EU4Digital: Improving Cyber Resilience in the Eastern Partnership Countries.* https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/c_2018_8184_f1_annex_en_v1_p1_1000418.pdf

[89] *Moldova Cyber Week 2018.* https://moldovacyberweek.md/

[90] *GUAM.* https://guam-organization.org/en/1st-meeting-of-guam-working-group-on-cyber-security/

[91] *Cybersecurity Alliance for Mutual Progress (CAMP).* https://www.cybersec-alliance.org/

for development, experience sharing, trend analysis, mutual growth and development of global cybersecurity.

Cooperation of national gas and electricity operators (especially electricity TSO Moldolectrica) with international organizations and initiatives is underway with Moldovan participation in the United States Energy Association in the field of the Utility Cyber Security Initiative through multiple workshops, lectures, trainings, exercises and experience as well as good practice sharing. The purpose of the initiative is to address and create high level cybersecurity strategy, assess, identify, prioritize and address risks and develop regional information sharing and analysis.

Along with above mentioned cooperation Moldova cooperates in NARUC and USAID initiatives for Black Sea Region[92]. Regulator in the energy sector is offered help, technical support and tools for creation of strategies for prevention, mitigation and improve safeguards.

Moldova is cooperating with NATO[93] through different multi-year initiatives under the Science for Peace programme. Initiatives are designed to improve cyber-defence and create cyber-incidents response capabilities as well as creation of cyber defence laboratory for purpose of educating and training Moldovan public sector.

There are multiple trainings, exercises and cooperation's covering law enforcement under Budapest Convention and bilateral cooperation with foreign institutions such as the FBI from United States of America, Federal Criminal Police Office of Germany and others[94].

Public-private partnership

CERT-GOV-MD serves as a forum for public-private partnership and experience sharing among all stakeholders in the country. It is also designated institution for organization of Cyber Drills aimed at increasing skills of all participants from all sectors of public and private sector as well as foreign experts. Alongside above-mentioned CERT there is Security and Intelligence Service[95] as governmental agency designated for cooperation and cybersecurity exercises for operators of critical infrastructure including energy sector.

5.5.6   Overview of education and training programmes

The Government Decision on the approval of Minimum Requirements in Cyber Security defines that institutions defined in the Decision, have to nominate Cyber Security Specialist(s) or department responsible for implementation of the cybersecurity management system. Official training for Cyber Security Specialists is available and encompasses different positions and specializations like in the case of incident managers and restoration managers. Beside training initiatives there are multiple courses on Cyber Security Education and Awareness, Digital Security and Mobile Espionage organized by MoD. Security and Intelligence Service organizes annual trainings and courses for Moldovan TSO Cyber Security Specialists with the goal to strengthen cybersecurity and build cyber defence capabilities.

CERT-GOV-MD organizes awareness raising and education campaigns for different demographic groups. It organizes Cyber Week during European Cyber Security Month and other cybersecurity events and activities. It organizes and implements modules for children and students for online safety and awareness raising in

---

[92] *Black Sea Region Initiative for Cyber Security. https://www.naruc.org/international/news/black-sea-regulators-on-path-to-effective-cybersecurity-strategies/*

[93] *NATO-Moldova Science for Peace Initiative. https://www.nato.int/cps/en/natohq/news_152364.htm?selectedLocale=en*

[94] *Cybercrime and cybersecurity strategies in the Eastern Partnership region. https://rm.coe.int/eap-cybercrime-and-cybersecurity-strategies/168093b89c*

[95] *Security and Intelligence Service of Republic of Moldova. https://sis.md*

curriculum of schools. Educational system allows attainment of Bachelor's degree from Technical University of Moldova in Information Security and Security of Computer and Telecommunication Systems.

USEA within its Utility Cyber Security Initiative organizes multiple trainings through workgroups for TSO personnel and leadership for creation of cybersecurity strategies, identification and prioritization and addressing of risks and threats. There have been also multiple trainings organized through bilateral cooperation with United States of America with the Federal Bureau of Investigation (FBI) for cooperation in addressing cybersecurity incidents, investigation and prosecution of cybercrime and sharing of good practices and information.

5.5.7   Gaps against EU legislation and standards

Cybercrime legislation

Legislation against Cybercrime is implemented in the legislative system and allows investigation and prosecution of offences pertaining to cybercrime. In its Information Security Strategy 2019-2024 the Republic of Moldova identified gaps of the legal system and is working towards implementing needed changes.

Identification of CI operators and OES

Identification of operators of CI has been conducted, the list is not publicly available. Criteria for identification of CI are established in the Anti-terrorist Critical Infrastructure Protection Plan and are based on the severity of consequences in case of disruption, malfunction or destruction of CI.

Identification of CII and OES has not been conducted as there is currently no legislative or regulatory base for identification.

The criteria for significant disruptive effect are not yet established, however the criteria for identification of CI can potentially be used as they are based on the impact of disruption, malfunction or destruction of CI.

National NIS strategy

The content of the Cyber Strategy Program 2016-2020 is in compliance with NIS directive provisions pertaining to national cybersecurity strategy.

There are multiple strategies pertaining to information and network systems adopted in Republic of Moldova. The Digital Moldova 2020, Cyber Security Program for 2016-2020 and Information Security Strategy 2018-2023 (2019-2024) are complementary and set strategic needs, goals and objectives for the purpose of achieving greater cybersecurity. Energy sector is mentioned only in the Digital Moldova 2020, although indirectly can be found in other strategies as well. The strategic goals for the CI are identified under Government Decision on Antiterrorist Critical Infrastructure Protection Plan, but none of the strategies address cyber risks or threats specific to energy infrastructure.

National Cybersecurity Authorities: Contact points

Ministry of Economy and Infrastructure is designated public Cybersecurity Authority and NIS SPoC. National CERT of Moldova is CERT-GOV-MD. Cross-border communication of cybersecurity incidents to other CPs is not foreseen in the legislation.

Anti-terrorist Center of the Information and Security Service of Republic is national contact point for CI operators and is responsible for CI identification and designation coordination as well as CI protection analysis and cooperation with other stakeholders and ministries.

Legislative system foresees the communication between the CI operators and CERT-GOV-MD as well as reporting to National Cybersecurity Authority.

Security plans and requirements

Regulation on anti-terrorist CI Protection complies with ECI directive.

Government Decision on Minimum requirements follows ISO 27002 standard and complies with the NIS directive pertaining to the security requirements.

It should be noted that the Decision is mandatory only for public CI operators while there is no cybersecurity legislative provision for private sector CI operators.

Standardization

Moldova adopted SM EN ISO/IEC 27000, 27001, 27002, 27011 and 15408-1-2-3 standards.

Moldova also adopted other cybersecurity standards, e.g. ETSI standards for the field of cybersecurity.

Operators level

Public operators in the energy sector are obliged to develop cybersecurity plans encompassing protective measures, incident response and communication, business continuity and ISMS auditing. Requirements for public CI operators laid out in the legislation complies with the NIS directive pertaining to the cybersecurity requirements. Private operators of CI are not subjected to any obligations however they are in some cases implementing provisions voluntary.

Cooperation

Moldova is very active in international cooperation with other countries in the field of cybersecurity in general as well as in the energy sector. Through workshops, trainings and international organizations (USEA, CAMP, GUAM, USAID, NARUC...) it cooperates with other organizations to protect the CI, experience and information sharing and capability building.

Although not officially designated, CERT-GOV-MD serves as a public-private cooperation forum in the field of training, awareness and communication campaigns, exercises and experience sharing. CERT-GOV and Security and Intelligence Service are organizing cybersecurity exercises, no energy sector specific cybersecurity exercise have been organized in the past. However, energy specific exercise was organized by UCSI a few years ago.

5.6 Montenegro

Montenegro has advanced fast in the cybersecurity area since 2010 when the Law on Information security was adopted along with regulation on Information Security Measures.

ECI directive is not transposed in the national legislation as well as there are no legislative provisions pertaining to CI. Identification of CI has not been conducted and there is also no CI or ECIP contact point established for matters of CI protection. New legislation for critical infrastructure is in the development and is expected to be finished in Q3 2019.

Montenegro partially transposed NIS directive as adoption of Cyber Security Strategy 2018-2021 set strategic goals for assessing challenges, risks and threats, established objectives pertaining to organizational capabilities and cooperation, developing defence capabilities as well as definition and identification of CII among which energy sector is explicitly mentioned. Considering the information obtained from the Strategy, the identification of CII/ES sectors has been conducted based on set criteria and an initial list of CII/ES sectors encompassing energy sector has been created. Designation of operators of CII/ES is on-going but current status is not publically available. It should be stressed that SCADA systems are identified as CII without connection to specific (i.e. energy) sector.

Legislation pertaining to CII cybersecurity has been incorporated into the Law on Information Security with CII specific amendments, but the Law is not applicable to the energy sector operators because CII operators in energy sector are not yet designated. The same is true for regulation on Information Security Measures as it was adopted based on the aforementioned law.

5.6.1   SWOT analysis

S

STRENGTHS

Methodology for identification of CII defines energy sector with its electricity, oil and oil derivatives and gas subsectors as CII and distribution of electricity, gas, oil and oil derivatives as ES.

SCADA systems are identified as CII without connection to specific (i.e. energy) sector, making it easier to implement cybersecurity standardization, certification regardless of jurisdiction

W

WEAKNESSES

Law on CI is in development - approximate adoption date is not yet known.

Ministry of Economy is the responsible Ministry for the energy sector, but energy sector ECIP contact point is not established.

O

OPPORTUNITIES

Although CII operators in the energy sector are not yet designated as foreseen by the regulation, electricity operators of CII are in the process of the implementation of ISO 27001 standard as well as following ENISA recommendations and these initiatives could be reinforced with EnC coordination. The business community recognises the importance of cybersecurity

T

THREATS

NAECCS, as designated National authority for CS, SPOC and as national CSIRT may face resourcing issues. Without adequate resources, this could lead to the risk that NAECCS would not be able to effectively separate operational and strategic tasks. Lack of cooperation between public and private sector. Upgrade of infrastructure and control systems at energy operator premises is not progressing in pace with state-of-the-art cybersecurity requirements

5.6.2 European Critical Infrastructure and Essential Services legislation requirements

Identification of EnCCI and ES

Based on the information obtained from the Cyber Security Strategy 2018-2021 identification of CII/ES has taken place and an initial list of operators of CII has been created with designation still ongoing. According to the Strategy, energy sector is included. List of sector CII is identified in the Methodology for identification of Critical Information Infrastructure.

Identification of CI has not been conducted as there is no legislative provision or strategic document pertaining to protection of CI. There is a Law on Critical Infrastructure in the adoption process and is expected to be finished in Q3 2019 that would set grounds for identification of operators of CI.

Cyber Security Strategy 2018-2021; Law on Information Security; Methodology for identification of Critical Information Infrastructure	*Lead: Ministry for Information Society and Telecommunications; Responsible Ministry: Ministry of Economy*

Criteria for CI designation and criteria for significant disruptive effect

No criteria have been developed for identification of CI as there is no legislative provision or strategy adopted. Based on the Methodology for identification of CII, among designated CI sectors there is also energy sector.

Criteria for the identification of CII/ES in the energy sector are based on the significance of disruptive effect:

- Human loss
- Economic loss
- Importance of the infrastructure and its criticality for public.

However, the detailed criteria are not publicly available.

Methodology for identification of Critical Information Infrastructure	*Lead: Ministry for Information Society and Telecommunications; Responsible Ministry: Ministry of Economy*

National NIS strategy

Cyber Security Strategy of Montenegro 2019-2021 set strategic goals for assessing challenges, risks and threats, established objectives pertaining to organizational capabilities and cooperation, developing defence capabilities as well as definition and identification of CII/ES among which energy sector is explicitly mentioned. The strategy is following NIS directive provisions pertaining to national strategy

For time period 2019-2021	*Lead: Ministry for Information Society and Telecommunications*

National CS organisational framework

Energy sector contact point for the coordination of CI protection with other states is not established, as there is no legislation pertaining to CI. Ministry of Economy is responsible for energy sector.

Methodology for identification of Critical Information Infrastructure	*Lead: Ministry of Economy*

Law on Information Security designates CIRT-ME as national authority, CERT and SPoC for NIS.

Law on Information Security; Methodology for identification of Critical Information Infrastructure	*Lead: CIRT-ME*

There is no legislation pertaining to CI and therefore no provisions regarding sharing of information or reporting. Reporting of cybersecurity incidents is not obligatory and done ad hoc.

Document: /	*Lead: Ministry of Economy*

CI operators and ES providers security requirements	
Operators Security plans are not foreseen for energy sector in the legislation as there is no legislation pertaining to CI nor has CI been identified.	
Document: /	*Lead: /*
Law on Information Security and regulation on cybersecurity measures define physical, technical and organizational measures based on the ISO 27001 and 27002 which are also prescribed standards. As legislation mentioned above pertains only to public sector and organizations accessing and processing information, the energy CII and OES are not obliged to follow said provisions.	
Law on Information Security; Regulation on Cyber Security Measures	*Lead: Ministry for Information Society and Telecommunications*

Standardisation	
The ISO standards 27001, 27002, 15408-1, and 15408-2 are adopted as national standards.	
Regulation on Standards in Information Security adopted by Ministry of Information Society, defines MEST ISO/IEC 27001 and 27002 as obligatory standards for implementation. However, the regulation only obligates public sector and organizations accessing and processing information and energy sector does not need to comply to the provisions.	
	Lead: Ministry for Information Society and Telecommunications; Institute for Standardization of Montenegro

Montenegro is located between several CPs and bordering with EU Members State Croatia and Italy. An interconnection with Italy is planned to be operational at the end of 2019, and others with Serbia and Bosnia and Herzegovina are also planned.[96] There is currently no gas market in Montenegro, but Montenegro have signed the Declaration Croatia and Albania for the construction of the Ionian Adriatic Pipeline (IAP), as sub-branch of Trans Adriatic Pipeline (TAP)[97]. When Montenegro will expand the electricity interconnection capacities and host the IAP, high level of cybersecurity coordination on national and regional level will be required.

5.6.3 Legislation at the national level

Strategy and action plans

The Cyber Security Strategy for Montenegro defines protection of critical information infrastructure in Montenegro as one of the main strategic goals. The Ministry of Public Administration has defined the list of critical information infrastructure (CII) in Montenegro, and the drafting of a Decree on measures for protecting CII is under way. However, the identification of CI has not yet been conducted as there is no legislative or regulative provision or strategic document.

---

[96] *European Commission Montenegro 2019 Report* https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20190529-montenegro-report.pdf

[97] *Available at: https://energy-community.org/regionalinitiatives/infrastructure/PLIMA/Gas16.html*

One of the objectives[98] of the "Cyber Security Strategy for Montenegro" for the period 2018-2021 is to carry out as many cyber exercises, trainings and simulations as possible, with the aim of strengthening the capacities of cyber defence.

Legislation against cybercrime

Montenegro has shown commitment to international cooperation by ratifying the Budapest Convention in 2005 with entry into force in 2010 and amended necessary articles and provisions to harmonize the legislative system.

Budapest Convention is implemented in: Criminal Code, The Law on Liability of Legal Persons for Criminal Acts, Criminal Procedure Code, Law on International Legal Assistance in Criminal Matters.

Energy sector relevant cybersecurity legislation

In October 2014 the Government of Montenegro adopted the Methodology of identifying CII and the Action plan for its implementation. This document was prepared and published despite the lack of a Law on critical infrastructure of Montenegro, and due to the importance of making additional progress in this area. This was the first national document related to CII in the Western Balkans.

Based on the information obtained from Cyber Security Strategy 2018-2021 the identification of sectors has been done. One of the identified sectors in the Strategy, conducted by The Ministry of Public Administration within Methodology for identification of CII, is also energy, with production, transfer, control and distribution system of electrical energy; production, refinery, protection and distribution of oil and oil derivatives; as well as production, protection, transport, control systems and distribution of gas. Among above mentioned subsectors and activities process of distribution of electrical, oil and oil derivative as well as gas are defined as ES. The ICT sector defines and identifies SCADA systems as CII without any connection to sector. The identification of operators has not yet been conducted; however Cyber Security Strategy recognizes the need for identification.

Parliament of Montenegro adopted the "Law on Information Security" in March 2010 pertaining to information protection and security, protection measures on physical, technical and organizational level for protection of information and ICT systems, responsibilities for implementation of the law as well as establishment and responsibilities of national CERT.

In 2016 amendments were made to the Law on Information Security. Added has been subchapter regulating CII and assignment of responsibility for implementation of the law and provisions pertaining to protection of CII was Ministry for Information Society and Telecommunications.

Pursuant to the Law on Information Security in September 2010 the Government of Montenegro adopted the Decree On Information Security Measures. This regulation defines and elaborates provisions set in the Law on

---

[98] The strategic objective for CIIs in the Cyber Security Strategy 2018-2021 is: "*The Government of Montenegro will continue to strengthen the CII defence capabilities, and since the National CIRT has a key role in this field - it must have adequate resources and tools to effectively understand, analyse and respond to the wide spectrum of threats in this field. The resources of state authorities in charge of safety control of CII must be adequate to the task, i.e. the state authorities must have staff members who understand threats and risks for specific CII belonging to their sector. Human and technical resources must be strengthened with the aim of efficient performance of this function.*"

Information security regarding physical, data, and information system protection, as well as prescribing measures for information security risk management. The Decree follows ISO 27002 standard. With adoption of Regulation on Standards of Information Security Montenegro set obligation for implementation of MEST ISO/IEC 27001 and 27002 standards for operators of public infrastructure and other organizations dealing with processing or accessing of information.

Moreover, in 2015, the Ministry for Information Society and Telecommunications developed the methodology for assessing the cybersecurity capacity maturity model.

The ISO standards 27001, 27002, 15408-1, and 15408-2 are adopted as national standards. Information security standards were adopted as national, based on recommendations of ENISA.

Other cybersecurity related legislation

Parliament of Montenegro in March 2010 adopted the Law on Information Security. The Law defined minimum requirements for implementation by public and other organizations processing and prepared circumstances to establish CERT, a separate organisational unit of a state administration body responsible for information society. CERT's responsibility is coordination of prevention and protection against computer security incidents on the internet and other information system security risks of authorities and other legal entities and natural persons.

5.6.4   National Cybersecurity Authorities

The following have been identified by the Cyber Security Strategy for Montenegro as the institutions accountable for cybersecurity in Montenegro:

- Ministry of Public Administration within which the national CIRT operates;
- National Security Agency;
- Ministry of Defence / Army of Montenegro;
- Ministry of Interior / Police Administration;
- Ministry of Justice;
- Ministry of Education;
- Directorate for Protection of Confidential Data.

The Information Security Council was formed by the Government in June 2017[99]. The Council will monitor also the implementation of the Cyber Security Strategy, by delivering quarterly reports submitted by the bodies identified as the main holders of activities defined by the Strategy the accompanying action plans.

---

[99] *Cyber Security Strategy for Montenegro 2013-2017 envisaged the formation of local CIRTs or appointment of contact persons in all state authorities, aimed at strengthening cyber infrastructure at the local level. A total of 31 local teams were created, in charge of cooperating with members of the national CIRT on the issues of protection against computer security incidents on the Internet.*

CIRT of Montenegro became operational in 2012. Montenegrin CIRT was established in accordance with the Law on Information Security of Montenegro as a separate organizational unit of the Ministry for Public Administration.

National Regulatory Authority for energy sector[100] neither exercise any rights or obligation pertaining to cybersecurity nor monitor or assess implementation of Cyber security strategy.

5.6.5 Cooperation and initiatives

In Cyber Security Strategy 2018-2021, Montenegro recognizes that only high level of communication, cooperation and integration on national and international level can strengthen the cybersecurity and allow efficient response to incidents, threats and risks. The Strategy sets plan of action for strengthening of public-private cooperation, drafting procedures for communication and cooperation, active participation in international activities pertaining to cybersecurity, establish international partnerships with other countries or within international organizations for purpose of sharing experience, information and knowledge.

Cooperation within Energy Community Parties

As an EnC contracting party Montenegro cooperates in the Cyber Security and Critical Infrastructure coordination group (CyberCG) of EnC for the purpose of promotion of high level of security of network and information systems and CI through strategic cooperation and exchange of information.

Cooperation with EU Member States

European Union with support of Council of Europe devised project CyberCrime@IPA[101] for strengthening of capabilities for fight against cybercrime in Montenegro. Project helped with raising awareness, enhancing cooperation between public and private sector as well as with international entities, organizations and foreign states.

Along with CyberCrime@IPA there was also iPROCEEDS[102] project created between EU, CoE and Montenegro for purpose of establishing search, seizure and confiscation of data and funds obtained by cyber criminals.

Cooperation with other parties

Montenegro103 is part of NATO's Membership Action Plan (MAP) programme[104]. Its' "Report on Implementation of the Fifth Annual National Programme of Montenegro in the period of intensified and focused discussions with NATO" contains an entire chapter on cybersecurity (chapter 4.2)[105], with four activities that are already part of the Action Plan for implementation of the National Cybersecurity Strategy.

---

[100] *Energy Regulatory Agency*

[101] *CyberCrime@IPA. https://www.coe.int/en/web/cybercrime/cybercrime-ipa*

[102] *iPROCEEDS BiH. https://www.coe.int/en/web/cybercrime/iproceeds*

[103] *8 Montenegro was officially invited to become the organisation's 29th member state on May 19, 2016. More information is available at: http://www.nato.int/cps/en/natohq/topics_49736.htm*

[104] *Available at: http://www.nato.int/cps/en/natolive/topics_37356.htm*

[105] *"Report on Implementation of the Fifth Annual National Programme of Montenegro in the period of intensified and focused discussions with NATO", available in Serbian only.*

In addition, Montenegro is a member of several regional organisations like:
- The South-East European Cooperation Process (SEECP)
- The South-East European National Security Authorities (SEENSA)
- The South-East European Military Intelligence Chiefs (SEEMIC)
- The Centre for Security Cooperation (RACVIAC)
- The Southeast European Law Enforcement Center (SELEC)
- The South-East European Prosecutors Advisory Group (SEEPAG)

The national CIRT of Montenegro became operational in 2012, with the assistance of the ITU-IMPACT programme. In cooperation with the ITU, CIRT.me organised a cyber drill in September 2015 for CIRT/CERTs from Europe. The CIRT.me participates in the FIRST as well.

Public-private partnership
A large part of critical information infrastructure in Montenegro belongs to the private sector. Therefore, it is necessary to clearly define cooperation with the private sector in the field of cybersecurity. With regard to the private sector, seven CIRTs were created for cooperation in cybersecurity within the companies Crnogorski Telekom, Telenor, M:tel, Wireless Montenegro, Telemach, M-kabl and Societe Generale Montenegro Bank, but no operators in the energy sector.
One of the best examples of cooperation with the private sector is the activities undertaken to organise joint promotional campaigns on the protection of children in cyberspace and the safe use of the Internet. Bearing in mind that CIRT recognised malware as one of the biggest threats in Montenegrin cyberspace, a pilot project was launched on 4 November 2016, in cooperation with the Agency for Electronic Communications and Postal Services (EKIP) and Internet providers in Montenegro.

Table 6: Overview of energy related cybersecurity cooperation initiatives

5.6.6   Overview of education and training programmes

The CIRT.me actively participates in the overarching TEMPUS project related to cybersecurity education in Montenegro.

Montenegro has an official university master-level program on cybersecurity policy, developed and delivered by the Donja Gorica University in Podgorica[106], which gives a unique mix of technical and policy-based knowledge on a variety of cybersecurity issues.

5.6.7   Gaps against EU legislation and standards

Cybercrime legislation
Montenegro is a party to the Council of Europe's Budapest Convention, which is largely transposed in the national legislation.

---

[106]   Based on the article "Cyber Security in Montenegro: Round Table with UK Representatives", by Aljoša Drobnjak, 4. 12. 2018

Identification of CI operators and OES

Methodology for identification of Critical Information Infrastructure (CII) and the Action plan for its implementation were adopted by the Government. Based on the information from the Cyber Security Strategy procedure for identification of CII/ES sectors has been conducted and an initial list of CII sectors has been developed. It is important to note that the Strategy explicitly mentions energy sector as one of CII/ES sectors.

Identification and designation of energy sector CI operators has not been conducted as the legislation is in the adoption process and is expected to be finished in Q3 2019.

National NIS strategy

The Cyber Security Strategy of Montenegro addressed cybersecurity objectives, challenges, risks and threats, overview of organizational responsibilities as well as cyber defence including analysis of objectives, capabilities, education and cooperation. Strategy complies with provisions of NIS Directive pertaining to national strategy.

Moreover, it defines also critical information infrastructure, which includes the energy sector, while specific risks and threats of energy sector were neither assessed nor addressed.

National Cybersecurity Authorities: Contact points

CIRT-ME serves as a National Cybersecurity Authority, SPoC and CSIRT based on the Law on Information Security.

Ministry of Economy serves as a responsible Ministry for energy sector. ECIP contact point for CI in energy sector is yet to be designated and relevant legislation adopted.

As there is no obligation for operators of CII/ES regarding reporting, there are no obligatory provisions pertaining to reporting of incidents or informing other EnCCI parties. Reporting of incidents is done on ad hoc basis to the national CERT. CERT exercises cross-border communication regarding incident reporting and sharing of information but those measures are not formally defined in the legislation.

Security plans and requirements

There is no obligation in the legislation pertaining to creation of security plan, but it will be defined with the adoption of the Law on CI. Entities defined in the Regulation on information security measures are obliged to implement measures but at the moment energy sector is not incorporated. There is no requirement to implement or align standards or good practices (international or national).

Standardization

The ISO standards 27001, 27002, 15408-1, and 15408-2 are adopted as national standards based on the recommendations of ENISA. Regulation on Standards in Information Security adopted by Ministry of Information Society, defines MEST ISO/IEC 27001 and 27002 as obligatory standards for implementation, however the regulation only obligates public sector and organizations accessing and processing information and energy sector does not need to comply with the provisions.

Operators level

There are no legislative or regulatory provisions pertaining to energy sector CII/ES operator's cybersecurity, however organizations in the energy sector began implementing measures themselves. There is no requirement to implement or align standards or good practices for operators of energy sector as the law on CI has not yet been adopted and the Regulation on Information Security Measures does not prescribe any standards for energy sector operators.

Cooperation

There are public-private cooperation's developed in Montenegro for joint promotional awareness raising campaigns for protection of children in cyberspace, on safe use of internet and information security threats. Strengthening of cooperation in the sphere public-private sector must be established as most of the operators of CI in energy sector are private companies and therefore collaboration is vital. Communication procedures are established between operators of CII/ES and national CIRT-ME.

Montenegro cooperates internationally with foreign state entities as well as international regional or global organizations for development of capabilities and information and good practice sharing.

5.7 North Macedonia

With regard to the national and regional security one of the main concerns of the Republic of North Macedonia are threats, risks and challenges regarding cyber-attacks and information security. North Macedonia does not have an overarching law dealing exclusively with cybersecurity. National Cyber Security Strategy for 2018–2022 sets strategic goals for identification of CII/ES operators including in the energy sector as it recognizes energy as one of critically important sectors. Strategy among other goals defines the need for implementation of legislation for cybersecurity and adoption of sector specific cybersecurity measures.

Currently there is no legislation and ongoing activities related to the ECI directive transposition in national legislation. The Law on Critical Infrastructure is in the development with foreseen adoption in Q3 of 2019.

NIS directive provisions related to strategy and CSIRT are implemented while the rest of provisions are covered in the Strategy action plan. Identification of energy sector CII/ES is planned for 2019, amendment of legislation in 2020 and development and implementation of relevant sectorial cybersecurity measures for energy sector CII/ES operators until 2021. Based on the information from the action plan, there is an ongoing study for detailed designation and identification of critical sectors and need legislative amendments. Identification of energy sector CII/ES operators is going to be conducted in scope of the Study in 2019.

Although energy sector operators are not obliged by the legislation to implement cybersecurity measures they recognized the need and are implementing them on a voluntary basis. They are developing communication channels with MKD-CIRT for cooperation and sharing of information and knowledge as well as incident reporting and response. National electricity TSO MEPSO started the development of internal cybersecurity policies and guidance that are following NIS directive requirements and international good practice.

5.7.1 SWOT analysis

S

STRENGTHS

Energy sector organizations recognize the need to implement cybersecurity regulations and are doing so voluntarily and developing communication channels with MKD-CIRT for cooperation, sharing of information and knowledge as well as cyber incident response and reporting (i.e. TSO MEPSO complies with the NIS Directive)

W

WEAKNESSES

As there is no legislation for CI, CII and operators of ES, there are no obligations for organizations in the energy sector pertaining to cybersecurity.

There is no CI protection point established and therefore gaps are present in regards to ECI directive implementation.

O

OPPORTUNITIES

North Macedonia cooperates in CyberCrime@IPA project with Albania, BIH, Croatia, Montenegro, North Macedonia, Serbia, Turkey and Kosovo* and it was the most agile Western Balkan country in utilising opportunities this programme gives and organised as much as three events which saw participation of experts throughout the region, including authorities responsible for drafting future legislative acts.

T

THREATS

Potential delays in implementation of action plan

National infrastructure operators have been recognised and contacted by the MKD-CIRT team, and they subsequently became constituents of MKD-CIRT. However, as there is no accepted definition of CI and no formal categorisation of CI assets it not clear if these include all the relevant organisations and their commitment

5.7.2 European Critical Infrastructure and Essential Services legislation requirements

Identification of EnCCI and ES

CI identification has neither been conducted nor any legislative provision or strategic document pertaining to it is in force. Study for the identification of CII and OES in the energy sector is ongoing. Based on the information obtained from the action plan the Study should have been finished until April 2019. Certain CII sectors have been identified in the Strategy including energy sector, although critical subsectors and services have not been mentioned. Based on the Strategy Action plan the beginning of identification/designation of operators is planned for 2019.

National Cyber Security Strategy Action Plan 2018-2022	*Lead: Ministry of Information Society and Administration (MISA); MKD-CIRT*

Criteria for CI designation and criteria for significant disruptive effect

At the current time there are neither the criteria for assessment of CI, CII and OES, nor the criteria for the assessment of significance of disruptive effect available. Study for the development of the criteria for the identification of CII is ongoing. Criteria is going to be used for assessment of criticality of CII and OES sectors and used for designation of CII until end of 2019.

National Cyber Security Strategy Action Plan 2018-2022	*Lead: MISA; MKD-CIRT[107]*

National NIS strategy

National Cyber Security Strategy for 2018-2022 is following NIS directive as it addressed all provisions regarding national NIS strategy. Strategy assessed risks and threats, challenges, set strategic objectives, defined stakeholders and responsible agencies, as well as set up an action plan for implementation of goals.

National Cyber Security Strategy 2018-2022	*Lead: Responsible authorities*

National CS organisational framework

Energy sector contact point for the coordination of ECI protection with other CP states is not established. However, the Ministry of Economy is responsible for energy sector.
Law on Electronic Communications defines MKD-CIRT as national CSIRT as well as cybersecurity SPoC, national authority for cybersecurity is not designated.

Law on Electronic Communications	*Lead: Ministry of Economy; MKD-CIRT*

Cooperation and communication between national infrastructure operators and MKD-CIRT has been established. However, it is not clear whether all necessary CI, CII and ES organization from energy sector have been included. There is no obligation for energy sector operators to communicate with responsible authorities regarding cybersecurity, but they recognized the need and have done that voluntarily.

Document: /	*Lead: MKD CIRT*

CI operators and ES providers security requirements

CI operators are not obliged to implement any security requirements or operator's security plan regarding CI protection as there is no legislation pertaining to protection of such infrastructure nor have the operators of CI been identified. North Macedonia does not follow ECI directive.
Law on Critical Infrastructure is in the adoption process and its adoption is foreseen in Q3 of 2019.
National TSO is, based on the provided information, compliant with pertinent NIS Directive provisions.

---

[107] *MKD-CIRT. Agency for electronic communications, National Center for Computer Incident Response, Kay Dimitar Vlahov 21, Skopje 1000, Republic of Macedonia*

Document: /	Lead: /

CII and OES including in the energy sector have not been identified yet. As there is no general or specific legislation pertaining to cybersecurity of CII/ES operators in the energy sector, operators are not regulated in regards to cybersecurity. North Macedonian legislative and regulative system is only partially following the NIS directive. Energy sector operators have to implement security measures voluntarily as well as establish communications channels with responsible authority in the cybersecurity sector for reporting of incidents.

Action plan foresees adoption and implementation of sectoral measures for cybersecurity pertaining to identified CII and ES, including in the energy sector, from 2020 to 2021.

Document: National Cyber Security Strategy Action Plan 2018-2022	Lead: /

Standardisation
Standardization Institute of the Republic of North Macedonia adopted MKC ISO/IEC 27001 and 27002 standards as well as ISO MKC ISO/IEC 15408-1,2,3.   There is no legislation pertaining to cybersecurity of CI, CII or OES in energy sector, therefore no international or national standards or good practices for either cybersecurity or technology and services are mandatory.
Lead: Standardization Institute

North Macedonia is geographically placed among other EnC CPs and EU Member States and has interconnections with all of them, with possible cascading effects to CPs Serbia and Kosovo* as well as EU Member States Greece and Bulgaria. North Macedonia and Kosovo*, signed in 2019 a Memorandum of Understanding for the Energy Sector under which they plan to revitalize electricity interconnection lines and potentially build a new gas interconnection, which would bring gas from nearby Skopje to Kosovo* thereby extending security of supply and need for coordination at cybersecurity level too.

5.7.3   Legislation at the national Level

Strategy and action plans

The National Strategy for Cyber Security 2018-2022, from July 2018, has been developed in accordance with The European Union's Cybersecurity Strategy and Policy and Commitment for cybersecurity of NATO to provide secure, safe, confidential and resistant digital environment for the benefit of citizens, businesses and the public administration. One of the strategic goals pertaining to CII and OES is the identification and designation process.

Action Plan for the implementation of goals and activities defined in the Strategy was presented on 11th December 2018. The purpose of this document is to define the steps in the implementation of the first National Strategy for Cyber Security of the Republic of Macedonia 2018-2022[108].

---

[108] *The action plan was developed for the period 2018-2022 and stated the 4 actions with the highest priority. The action plan set goals for: 1. Establishment of the National Council for Cyber Security; 2. Analysis of existing institutional capabilities for cyber security with the aim of instinctual identification of the body with operational facilities for cyber security; 3. Establishment of a body with operational capacities for cyber security as a newly formed independent body (agency,*

Strategic Defence Review 2018 predicted the development and implementation of a National Strategy for Cyber Security and based upon its principles, development of a Strategy for Cyber Defence by the end of March 2019.

Legislation against cybercrime

The North Macedonia ratified the Budapest Convention and its Additional Protocol through the Law on ratification of the Convention on Cybercrime in 2004 with entry into force in 2005. The provisions of the Budapest Convention were transposed in the Criminal Code and Criminal Procedure Code.

Budapest Convention is implemented in: Criminal Code, Criminal Procedure Code, The Law on Electronic Commerce, Law on Interception of Communications, Law on International Cooperation in Criminal Matters.

Energy sector relevant cybersecurity legislation

Operators of CI, either general or energy specific, have not been identified yet, as there is no legislation pertaining to CI. Legislation, mainly Law on Critical Infrastructure is in development with expected finalization in Q3 of 2019.

CII and OES are not identified as well. However, the identification process has begun, as a study and analysis on identification of critical sectors, CII and OES, responsible authorities and legislation is underway with finalization in 2019, based on the Cyber Strategy Action plan. Based on the results of the study identification of operators of CII and OES, including energy sector will be conducted. With critical energy subsectors and operators once identified, the responsible authorities, in this case MKD-CIRT and Ministry for Information Society and Administration, will create relevant sectoral guidelines, provisions and measures, which operators of CII and OES in energy sector will have to implement.

At the moment there is no obligation for energy sector operators as there is no legislation, however energy sector organizations recognize the need to implement cybersecurity regulations and are doing so voluntarily and developing communication channels with MKD-CIRT for cooperation, sharing of information and knowledge as well as cyber incident response and reporting. Example is national TSO MEPSO[109] that complies with the NIS Directive, based on the information provided in the questionnaires.

Standardization Institute of the Republic of North Macedonia adopted MKC ISO/IEC 27001 and 27002 standards as well as ISO MKC ISO/IEC 15408-1,2,3. However, no legislation pertaining to cybersecurity of CI, CII or OES in energy sector, therefore no international or national standards or good practices for either cybersecurity, technology and services are prescribed for operators of CII/ES operators.

---

directorate) or as a newly formed organizational unit or body within an existing body; 4. Preparation of a study on identification of CII (any information- communication systems whose maintenance, reliability and security are critical for national security, economy, public security and health) and Important Information Systems

[109] *https://www.mepso.com.mk/en-us/Default.aspx*

Other general cybersecurity related legislation

A number of legal documents touch upon some cybersecurity related issues – the Law on Personal Data, the Law on Electronic Commerce, the Law on Electronic communications, the Law on Interception of Communications, the Law on free Access to public Information, the Law on Data in an Electronic Form and Electronic Signature. In addition, the amendments to the Law on Criminal Procedure adopted in 2013 specifically tackle cybercrime and crimes committed with the use of computers, as well as the collection of digital evidence by the law enforcement authorities.

5.7.4 National Cybersecurity Authorities

In 2015, the MKD-CIRT was set up within the Agency for Electronic Communications (AEC) as the official national point of contact and coordination in dealing with security incidents in networks and information systems pursuant to the Law on Electronic Communications.

National infrastructure operators have been recognised and contacted by the MKD-CIRT team, and they subsequently became constituents of MKD-CIRT. However, as there is no accepted definition of CI and no formal categorisation of CI assets it was not clear if these include all the relevant organisations.

National Cyber Security Strategy 2018-2022 foresees the creation of a National Cyber Security Council, but the extent of its implementation is currently unknown. Council's responsibilities would be of a coordinative institution for implementation and monitoring of the Cyber Security Action Plan for 2018-2022, as well as serve as a body with operational cybersecurity capability. The Council would be responsible for amending and updating the strategic Action plan, identify challenges and manage cyber-crisis, cooperate with other stakeholders (including energy sector) and develop capabilities for operational assistance in response to cyber incidents among others.

National Regulatory Authority (Energy Regulatory Commission of the Republic of North Macedonia) for energy sector does not exercise any rights or responsibilities pertaining to cybersecurity nor does it monitor or assess implementation of Cyber security strategy.

North Macedonian main 24/7 contact point in investigative field of cybercrime and international cooperation is established under the Ministry of Justice in the General Prosecutor Office[110].

5.7.5 Cooperation and initiatives

North Macedonia recognized domestic and international cooperation as a strategic goal in the National Cyber Security Strategy 2018-2022. Strengthening of domestic public-private cooperation is recognized as a necessary goal as the largest part of CII and OESs are privately owned. International cooperation is recognized as a key segment in the effort to increase capacities for identifying and responding to incidents as well as a building of capabilities for exchange of information, experience and knowledge.

Cooperation within Energy Community Parties

---

[110] *General Prosecutor Office, Kay Dimitar Vlahov 21, Skopje 1000, Republic of Macedonia*

As an EnC contracting party North Macedonia cooperates in the Cyber Security and Critical Infrastructure coordination group (CyberCG) of EnC for the purpose of promotion of high level of security of network and information systems and CI through strategic cooperation and exchange of information.

Cooperation with EU Member States

Cooperation between EVN Austria and local EVN was established for purposes of information, know-how and expertise on cybersecurity sharing within Group Strategy for Cybersecurity.

As for its efforts in mitigating cybercrime threats, the EU has paired in this endeavour with the Council of Europe (CoE). Apart from its global project which (in three phases) included around 110 countries, two long-term projects have been organised specifically for the Western Balkans countries, under the framework of the Instrument for Pre-Accession (IPA) – CyberCrime@IPA(2010- 2013)[111] and iPROCEEDS (2016-2019)[112]. The CyberCrime@IPA project is titled "Regional Co-operation in Criminal Justice: Strengthening capacities in the fight against cybercrime" and its beneficiary countries were Albania, BIH, Croatia, Montenegro, North Macedonia, Serbia, Turkey and Kosovo*.

North Macedonia was the most agile Western Balkan country in utilising the opportunities this programme gives and organised as much as three events which saw the participation of experts from throughout the region – the first ATC was organised in October 2013 in Ohrid (North Macedonia) and titled "NATO Regional Summer School on Cyber Defence (NATO RSSCD)" in cooperation with Slovenia[113]; ATC "Terrorist use of cyberspace" was organised in December 2014 in Ohrid with Turkey as a NATO country co-organiser[114], whilst ARW was organised in March 2015 in Skopje (North Macedonia) with a Bulgarian organisation as a co-organiser and titled "Encouraging Cyber Defence Awareness in the Western Balkans"[115]

Signing of Memorandum of Understanding between MKD-CIRT and KOS-CERT, ALCIRT, SRB-CERT for purpose of information and good practice sharing.

Cooperation with other parties

MEPSO (TSO) cooperates internationally through ENTSO-E organization for the purpose of establishing high security standards for the protection of critical transmission systems infrastructure and in the field of cybersecurity also through different workshops, regulations and experience sharing initiatives.

North Macedonia cooperates with OSCE mission to Skopje in the field of cybersecurity for strengthening of capabilities, development of information procedures and institutional support. OSCE organized cybersecurity table top exercise for developing of cooperation among 38 government organizations and business representatives for protection of critical infrastructure.

North Macedonia cooperated with Republic of Korea on the topic of cybersecurity through workshops for strengthening of cybersecurity capabilities, experience sharing, and topic of national cybersecurity strategy as well as functioning of national CERT.

In addition, North Macedonia is a member of several regional organisations like:

The South-East European Cooperation Process (SEECP)

The South-East European National Security Authorities (SEENSA)

The South-East European Military Intelligence Chiefs (SEEMIC)

The Centre for Security Cooperation (RACVIAC)

The South-East Europe Cyber Security Centre (SEECSC)

The Southeast European Law Enforcement Center (SELEC)

The South-East European Prosecutors Advisory Group (SEEPAG)

---

[111] Available at: http://www.coe.int/en/web/cybercrime/cybercrime-ipa

[112] Available at: http://www.coe.int/en/web/cybercrime/iproceeds

[113] Available at: http://www.pf.uni-lj.si/media/nato_poster_ohrid.pdf

[114] Available at: http://sites.miis.edu/cyber/2014/12/20/executive-education-december-2014/

[115] Available at: http://www.atlantic-club.org/index.php?advanced-research-workshop-8220encouraging-cyber-defenceawareness-in-the-balkans8221

Public-private partnership

Public sector, in terms of the National Strategy for Cyber Security 2018-2022, includes Public sector authorities and other subjects, which in different ways represent the users of the cyber space and subjects that are obliged to apply measures that arise from the Strategy. Private sector with public sector authorities and regulatory bodies as affected parties by this Strategy, are subject to special regulations for critical infrastructure and the security and defence system. Same can be argued for other legal and business subjects which in different manners represent the users of cyber space and subjects and are obliged to apply the measures that arise from the Strategy. Such measures encompass legal and business entities, with regards to their scope of work, number of employees and markets which they cover.

5.7.6   Overview of education and training programmes

A national programme for cybersecurity awareness raising is yet to be established, led by a designated organisation (from any sector) addressing a wide range of demographics.

Cybersecurity awareness raising efforts are sporadic and mostly done on a voluntarily basis and with limited resources by non-governmental organisations (NGOs) and with ad hoc support from the government. However, North Macedonia has been active in promoting a safer Internet and has had a regular engagement with the EU's Safer Internet Day initiative since 2010.

Existing educational programs at all levels of formal education (primary, secondary and tertiary educational sectors) in the Republic of North Macedonia do not satisfy in full the needs for educating and training specialists in full to be able to respond to the latest challenges and trends in the cyber space. The need for enhancing cybersecurity education in schools and universities has been identified by the Government, in particular by the line Ministry, industry, and academic stakeholders. By 2016, two universities accomplished the accreditation for undergraduate and master's programmes specialising in cybersecurity. In particular one university which attracts most of the students in IT related subjects is also highly engaged in research and cooperating on the international level.

Late 2009 the government has pursued a national program called e-Macedonia, which was developed by the Ministry of Information Society, with priorities being: e-education, e-citizens, e-business, e-infrastructure, e-government and Information Security.[116]

MKD-CIRT is in the process of developing education and training initiatives for specialists in the field of information security, information security management, management of computer security incidents, penetration testing, vulnerability detection and analysis as well as forensics. Currently active trainings initiatives are based on the topic of implementation of ISO 27001, 22301, 27032 standards based on the information national TSO provided in the questionnaires.

---

[116] *Ministry of Information Society of Macedonia, "Developed Information Society," accessed on 15 March 2010, www.mioa.gov.mk/files/pdf/Broshura_MIO_design_FINALNO.pdf*

5.7.7 Gaps against EU legislation and standards

Cybercrime legislation

Legislation against Cybercrime is well implemented in the legislative system and allows investigation and prosecution of offences pertaining to cybercrime.

Identification of CI operators and OES

CII and IIS are defined in the National Cyber Security Strategy 2018-2022. One of activities planned by the strategy is establishing a cyber defence system for the national critical infrastructure. The strategy's Action Plan 2018-2022 foreseen the Study to identify the Critical Information Infrastructure shall be conducted by April 2019. The study should include identification of CII and operators, authorities and regulators of each critical sector and assessment for the needs for amendments of sector laws and provide recommendations.

The concept of cybersecurity in CI is in its infancy in North Macedonia. There is as yet no accepted definition of CI and no formal categorisation of CI asset.

National NIS strategy

No major gaps were identified in regards to NIS directive pertaining to national NIS strategies. The National Cyber Security Strategy 2018-2022 has addressed cybersecurity challenges, risks and threats including those of critical infrastructure of energy sector, as well as defined strategic goals, identified the stakeholders and created an action plan.

National Cybersecurity Authorities: Contact points

EC protection contact point has not been established or designated as there is no underlying legislation pertaining to CI, identification of operators or other organizational provisions. Ministry of Economy is designated as responsible Ministry for energy sector.

MKD-CIRT is designated as national cybersecurity authority, SPoC for NIS and national CSIRT based on the Law on Electronic Communications, however it is possible, that with creation of National Cyber Security Council, the designation of National Cyber Security Authority and possibly NIS SPoC will be transferred to the Council.

Legislative system does not foresee communication with other EnC contracting parties in case of incidents. However, MKD-CIRT does serve as a liaison with foreign authorities and organizations.

Security plans and requirements

Security plans and requirements do not follow NIS or ECI directive as there is no requirement or recommendations for preparation of security plan regarding operators of CI, CII or essential services in the legislation.

There was no risk assessment in the energy sector nor was it conducted in the energy information infrastructure as there is no legislative obligation.

Standardization

Standardization Institute of the Republic of North Macedonia adopted MKC ISO/IEC 27001 and 27002 standards as well as ISO MKC ISO/IEC 15408-1, 2, 3.

There are no international cybersecurity standards mandatory for operators of critical infrastructure, critical information infrastructure and essential services as there is no relevant legislation adopted that would govern the field of cybersecurity.

Operators level

North Macedonia did not adopt relevant legislative and regulative documents for cybersecurity of critical infrastructure, critical information infrastructure and essential service operators and therefore no cybersecurity standards or measures are mandatory for implementation. However, the energy sector organizations recognize the need to implement cybersecurity regulations and are doing so voluntarily. They are developing communication channels with MKD-CIRT for cooperation and sharing of information and knowledge as well as incident reporting and response. Based on the information acquired from questionnaires, national TSO MEPSO begun following NIS directive and internalizing international standards.

Cooperation

North Macedonia cooperates internationally with various foreign entities on the state and institutional level. Development of cooperation for purposes of information and good practice sharing among neighbouring countries and within international organizations allows North Macedonia to develop its capabilities, cooperate with other foreign entities for creating a safer cyber space. International organizations such as OSCE, EU, CoE and others are important partner to development of cybersecurity field.

Energy sector and institutions do not cooperate in international sphere with exception of TSOs that are a part of ENTSO-E and participate in their training and implement their recommendations.

MKD-CIRT does not participate in the FIRST.
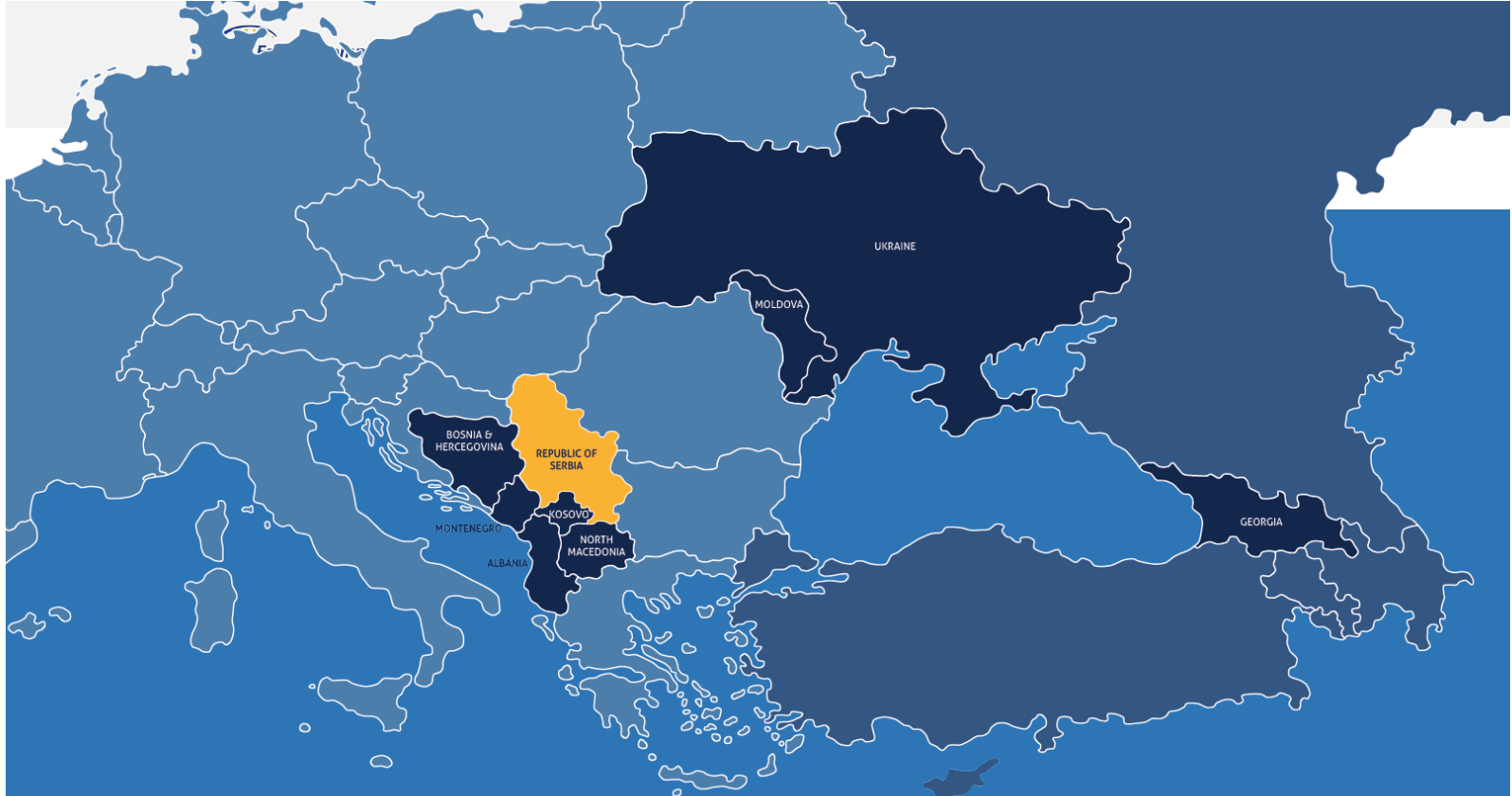
5.8 Republic of Serbia

Based on the Strategy for the Development of Information Security for the period 2017-2020 Serbia aligned the majority of its critical infrastructure and information security legislation with EU cybersecurity legislation in the period 2016 to 2018. The requirements of the NIS and ECI directives were transposed in the national legislation and are applicable to the energy sector. Although the Republic of Serbia transposed the majority of NIS and ECI directive to national legislation it should be noted that ECI-related provisions will come in power with accession of RS to EU.

The designation of CI is ongoing and energy sector stakeholders are included. Criteria for the assessment of CI encompasses dangers for national security, health, lives and security of citizens, damage to property, threat to economic stability, etc., but the detailed criteria/thresholds are classified.

The identification of CII/ES[117] operators is foreseen in the legislation and energy sector, with its electricity, gas and oil subsectors included. Based on the Law on Information Security cybersecurity requirements and obligations are established for CII/ES operators. Criteria for the identification of significant disruptive effect are not established or publicly available.

The cybersecurity requirements pertinent to CI/CII/ES operators are laid out in the legislation and are aligned with EU legislation, standards and good practices. Energy sector, including generation/production, transmission, distribution and marketplaces are obliged to prepare Operator Security Plans for CI and obtain its approval from the Ministry of Internal Affairs. CII operators, including designated stakeholders in the energy sector, shall prepare, maintain and review security and continuity plans. Specific requirements laid out in the *"Regulation about the closer regulation of protection measures information-communication systems of special importance"* are aligned with ISO 27002 guidance.

---

[117] *Designated as "ICT systems of special importance" in the Strategy for the Development of Information Security for the period 2017-2020*

5.8.1 SWOT analysis

STRENGTHS

Energy sector is the first in the list of critical infrastructure sectors in the Critical Infrastructure Law from 2018.

The identification of CI and EnCCI operators in Republic of Serbia has not yet been concluded. However, the sectoral identification of critical sectors does include the energy sector.

WEAKNESSES

Stakeholders in the energy sector that are in scope of this study are addressed in the CI and NIS related legislation as well as in the Strategy implementation action plan. However, Strategy and Action plan implementation activities are sometimes delayed.

OPPORTUNITIES

Energy sector operators in electricity, gas and oil subsector will be assessed and identified as CI against criteria for assessment of the CI established and adopted by the government

There is no legislative requirement related to standardisation in the area of information security for CI and NIS. However, there should in principle be no major obstacles for operators to obtain SRPS ISO/IEC 27001 certification.

THREATS

The Law envisaged the creation of the Body for the Coordination of Information Security, with the option of establishing expert working sub-groups that could include representatives of other public bodies, industry, the academic community and civil society.

Complex coordination between responsible authorities may slow down implementation of cybersecurity actions

5.8.2 European Critical Infrastructure and Essential Services legislation requirements

Identification of EnCCI and ES
The energy sector is the first in the list of critical infrastructure sectors in the Critical Infrastructure Law from 2018. The process of identification of energy sector critical infrastructure is underway, the identification criteria is established although not publicly available. The concept of ES from the NIS directive providers is implemented in the Law on Information Security. The Law identifies ICT systems of special importance in the energy sector (generation, production, transmission and distribution). Furthermore, "Regulation determining the list of activities in the fields in which activities of general interest are performed and in which information and communication systems of special importance are used" includes detailed list of stakeholders from electricity, gas, oil and coal production.

The Law on Critical Infrastructure 2018	*Lead: Competent Authorities and organizations*

Assessment of CI disruption and criteria for significant disruptive effect
Criteria for the identification of CI adopted with Government decree are based on the consequences of disruption of CI and are not publicly available. Basis for the criteria is defined in the Law on Critical Infrastructure and encompasses dangers for national security, health and lives of people, damage to property and environment, threat to security of citizens and economic stability and endangerment of functioning of Republic of Serbia.

The Law on Critical Infrastructure	*Lead: Competent Authorities and organizations*

National NIS strategy
Strategy for the Development of Information Security 2017-2020 addresses NIS directive provisions.

For time period 2017-2020	*Lead: The Body for the Coordination of Information Security of Ministry of Trade, Tourism and Telecommunications*

National CS organisational framework
Contact point for protection, domestic information sharing and coordination of critical infrastructure is the Ministry of Internal Affairs. Aforementioned ministry will acquire responsibilities related to ECI protection contact point with the accession to EU. The Ministry of Mining and Energy is responsible for energy sector and tasked with the creation of proposals for identification of CI operator in this sector.

The Law on Critical Infrastructure	*Lead: Ministry of Internal Affairs; Ministry of Mining and Energy*
The Ministry of Trade, Tourism and Telecommunications is responsible authority for ICT system security and national cybersecurity authority in accordance with the NIS directive. The Regulatory Agency for Electronic Communications and Postal Services CERT[118] is designated as the national CERT.	
Law on Information Security	*Lead: Ministry of Trade, Tourism and Telecommunications; RATEL CERT*
The Law on Critical Infrastructure	*Lead: Ministry of Internal Affairs; Energy sector operators*

---

[118] *Nacionalni CERT (SRB CERT), Palmotićeva 2, 11103 Beograd, Republika Srbija*

CI operators and ES providers security requirements

The Law on Critical Infrastructure defines tasks for operators in the energy sector to implement necessary security measures for protection of CI, operator's security plans and operator security risk management plan. Among others the legislative act stipulates information sharing, reporting, and protection of data, management and control of critical infrastructure. It is important to note that the Law on Critical Infrastructure designates a security liaison officer for protection of CI, which is responsible for adoption of internal documents pertaining to security of the systems, prepares security plans, controls and monitors risks and threats, coordinates response and has a reporting role to the competent authority for the CI and energy sector.

The Law on Critical Infrastructure	Lead: Energy sector organizations; Ministry of Internal Affairs

The Law on Information Security stipulates that operators of ICT systems of special importance adopt internal acts on ICT system security with dedicated protection measures, principles, methods and procedures, measures of supervision of their ICT systems and persons responsible to perform these tasks. The Law on Information Security sets obligation for reporting of operators of ICT of special importance as well as contracting external experts for assessment of compliance of implementation of ICT.

Law on Information Security	Lead: Energy sector organizations; Ministry of Trade, Tourism and Telecommunications

Standardisation

EU wide cybersecurity standards (and candidate standards) are adopted as national standards, namely: SRPS ISO/IEC 27001:2014, SRPS ISO/IEC 27002:2015, SRPS ISO/IEC 15408-1:2014, SRPS ISO/IEC 15408-2:2014, SRPS ISO/IEC 15408-3:2014 and SRPS ISO/IEC 27019.

There is no legislative requirement related to standardisation in the area of information security for CI and NIS. However, as mentioned in the section "Security plans and requirements" above and under the assumption that security plans are effectively implemented, there should in principle be no major obstacles for operators to obtain SRPS ISO/IEC 27001 certification.

Lead: Institute for Standardization of Serbia

Serbia is geographically located among EnC CPs (Bosnia and Hercegovina, Montenegro, Kosovo*, Northern Macedonia) and has interconnections with them with possible cascading effects to both CPs and EUMember States (Croatia, Hungary, Bulgaria and Romania). Gas company Srbijagas holds interconnections agreements with the Hungarian transmission system operator FGSZ and with Gas Promet Pale in Bosnia and Herzegovina

Since electricity and gas sector are on a transit route with high impact on stability of the energy supply in the region of West Balkan, the cybersecurity in Serbia energy sector with good coordination and cooperation framework needs to be high on agenda.

5.8.3   Legislation at the national level

Strategy and action plans

The Strategy for the Development of Information Security in the Republic of Serbia developed multiple strategic goals to strengthen cybersecurity and develop the information society encompassing security of information and communication systems of special importance, security of citizens, combating high-tech

crime, protection of services and ICT necessary for national security and international cooperation for improved cybersecurity and development.

The security of ICT systems of special importance is one of the strategic objectives covered in the Strategy for the Development of Information Security in the Republic of Serbia for the period 2017-2020, strategic measures include ICT systems in the energy sector. The Strategy designates the Ministry of Trade, Tourism and Telecommunications as the competent authority as well as coordinating and monitoring body for the implementation of the Strategy. The Action Plan for 2018 and 2019 for the implementation of the Strategy for development and support of the information technology industry for the period 2017-2020 is adopted and executed albeit with some delays.

The strategic goals pertaining to Security of ICT systems of special importance establish the need for identification of operators on which the CI depends upon and are CI themselves. The strategy defines that such operators are responsible to implement information security measures and communicate with the competent authority for cybersecurity. The Strategy recognizes the need for monitoring of such infrastructure and continuous information sharing practices for incident notifications, disruptions and assessment of risks. Among other goals, the Strategy recognizes the need to establish provisions for the implementation of an information security management system (ISMS) in operators of ICT system operators of great importance (CI and CII).

Legislation against cybercrime

The Republic of Serbia accessed the Budapest convention in 2009 and incorporated it in national legislation, starting with the Law on Ratification. Use of terms and substantive criminal provisions of the aforementioned convention are included in the Criminal code and Electronic communications Law and cover all necessary provisions either by direct implementation of new articles or in extent of existing provisions that can be used in cases of cybercrime. The provisions demanded in the procedural section of the Budapest convention are encompassed in the Criminal Procedure Code.

Budapest Convention is implemented in: Criminal Code, Criminal Procedure Code, Law on the Liability of Legal Entities for Criminal Offences, Electronic Communications Law, On Conducting Covert Interception of Communications, Law on Mutual Assistance in Criminal Matters, On Confidentiality of Information.

Legislation targeting OESs

The Republic of Serbia recognized the need to harmonise national legislation with international legislative documents and directives for purposes of maintaining and securing CI during everyday operations as well as during crises. Legislation targeting CI and OESs is based on the laws: Critical infrastructure Law from 2018 and Information security Law from 2016, amended in 2017.

The Critical Infrastructure Law is focused on the national and European critical infrastructure and regulates identification and determination of critical infrastructure of the Republic of Serbia, protection of critical infrastructure, authority and responsibility of the body and organizations in the field of critical infrastructure as well as information, reporting, decision support, protection data, management and control in critical infrastructure.

Section IV. of the Law is dedicated to the ECI and includes provisions for yearly reporting on designated CI to EU Commission and to the interested countries to which each critical infrastructure has an impact. Contact

point for the purpose of ECI information sharing and coordination is the Ministry of Internal Affairs. It should be noted that ECI related provisions of the law shall apply from the date of accession of the Republic of Serbia to the EU.

The energy sector is specifically listed in the Law in the list of CI sectors. Operators of CI are obliged to develop a Security Plan to manage risks and obtain plan approval from the Ministry of Internal Affairs. The methodology for Security Plan development is not yet defined. It shall be prescribed by the Minister of internal affairs.

Serbia's legal and institutional framework in the area of cybersecurity is based on the Law on Information Security (2016). The Law stipulates that the operators of CII/ES adopt an act on ICT system security with dedicated protection measures, supervision of their ICT systems and persons responsible to perform these tasks. Furthermore, the Law envisaged the creation of the Body for the Coordination of Information Security, with the option of establishing expert working sub-groups that could include representatives of other public bodies, industry, the academic community and civil society.

The Law on Information Security lays down protection measures against security risks in information and communication systems, liability of legal persons in the management and use of information and communication systems, defines competent authorities for the implementation of protection measures, coordination between protection factors and monitoring of their proper application. The Law is dedicated to the security of ICT systems of special importance. Among others those are the systems that are used for: production, transmission and distribution of electricity; research, production, processing, transport and distribution of oil as well as natural and liquid gas.

ICT systems of special importance are further specified in the *"Regulation on determining the list of activities in the fields in which activities of general interest are performed and in which IC systems of special importance are used (2016)"* that includes the list of sectors and subsectors in which activities of general interest are performed and where ICT systems of special importance are present. The energy sector is included encompassing electricity: generation, transmission and distribution, and organized electricity market. Listed oil and gas sector activities: research, production, processing, transport and distribution of oil, natural and liquid gas, as well as oil and petroleum products.

The operators of ICT systems of special importance are responsible for the security of ICT system and for the ICT system protection measures: establishment of an organizational structure, achieving the safety of remote work and use of mobile devices, adequate qualifications of persons working with these systems, identification of information assets and determination of responsibility for their protection, classification of data so that the level of their protection corresponds to the importance of the data in accordance with the identified risks. Information security requirements are further specified in the "*Regulation about the closer regulation of protection measures for information-communication systems of special importance"* that is in general following recommendations of ISO 27002.

Operators of ICT systems are obliged to inform the competent authority about incidents in ICT systems that can have a significant impact on information security breaches. Regulation on the procedure for submitting data, lists, types and significance of incidents and the procedure of notification on incidents in information and communication systems of special importance. Types of incidents as well as impact categories are listed but there are no specific thresholds (e.g. incident impacts a lot of customers. no definition/threshold of the meaning "a lot of").

Planned Amendment[119] of The Law on Information Security is under way. Public consultation on the amendments of The Law on Information Security has ended in February 2019.

Other general cybersecurity related legislation

Other general cybersecurity related legislation which is not energy specific or does not obligate energy sector CI, CII and OES, encompasses: Law on Organization and Competence of State Bodies for Combating High-Tech Crime; Law on Classified Information; Law on Personal Data Protection; Law on Ratification of the Convention on High-Tech Crime; Law on the Confirmation of the Additional Protocol to the Convention on High-Tech Crime on Criminalization of acts of racist and xenophobic nature committed through computer systems; Law on the Military Security Agency and the Military Intelligence Agency.

5.8.4   National Cybersecurity Authorities

The Body for the Coordination of Information Security has the task to achieve co-operation between the authorities and to coordinate the advancement of information security, initiate and monitor preventive and other activities in the field of information security and propose measures for the improvement of information, provide suggestions and proposals related to the preparation of strategic documents, by-laws and information security. The coordination body is managed by the Minister of Trade, Tourism and Telecommunications (the competent authority for NIS) with members from defence, Internal Affairs (Critical infrastructure), Foreign Affairs, Justice, Military Security Agency, Military Intelligence Agency, Office of the National Security and Protection of Classified Information Council, Government Secretariat, Regulatory Agency for Electronic Communications and Postal Traffic and Directorate for Common Affairs of the Republic authorities.
The Ministry of Internal Affairs (referenced in the law as the Ministry) regulates plans, coordinates, controls activities, and communicates information regarding critical infrastructure. Operators of CI must have a Liaison officer or a person that liaisons with the Ministry. Furthermore, the Liaison officer is nominated by the Ministry based on the CI operator proposal. Requirements for Liaison officers are laid out in article 9. The Ministry issues a licence to the Liaison officer. The Centre for reaction to attacks on information system (CERT) is in the scope of the Ministry, which cooperates with national and foreign CERTs.
The Competent Authority for the ICT system security is the ministry responsible for information security, i.e. the Ministry of Trade, Tourism and Telecommunication. It should be noted that in the Serbian legislation providers of essential services as defined in NIS are operators of ICT systems of special importance. Having this in mind and in correlation with a definition of ICT systems of special importance (see paragraph related to legislation above) the Ministry of Trade, Tourism and Telecommunication is CA for NIS. The Ministry supervises the work of the national CERT. The Competent authority has the authority to establish international cooperation in the field of ICT systems security in case of risks and incidents which surpass national capacities or can have impact on more than one country.
The national CERT (SRB CERT) performs coordination, prevention and protection against security risks in ICT systems in the Republic of Serbia at the national level and is established within the Regulatory Agency for Electronic Communications and Postal Services. SRB CERT is responsible to perform continuous risk and incident assessment and to share security risk and incident information with relevant ICT stakeholders in the RS. It was established and became operational in 2017. Establishment of cooperation mechanisms with international CERT organisations, foreign CERTs and special registered CERTs was planned for the end of

---

[119] *Planned in the "Action Plan for 2018 and 2019 for the implementation of the Strategy for the Development of Information Security in the Republic of Serbia for the period 2017-2020" for Q3 2018*

2018[120] but not yet completely realised. SRB CERT also keeps records of the registered special CERT teams in the Republic of Serbia. Registered special CERT teams perform prevention and protection tasks related to security risks in ICT systems within legal entities, groups of legal entities, business sectors, etc.
Several other CERTs exist: the academic CERT is part of the Academic Network (AMRES) and protects the network of education, scientific and research institutions; the Ministry of Interior has established its own CERT to protect sensitive citizens' databases and the system that operates the databases; the national Internet domain registry RNIDS is setting up the CERT for national domains .rs and .srb. The registration of special CERTs is regulated[121], SRB CERT is obliged to maintain the register of special CERTs.

The Centre for security of ICT system in republic authorities (CERT of republic bodies) is established in the scope of the Office for Information Technologies and eGovernment. This CERT performs tasks related to protection against incidents in ICT systems of republic authorities, except for the ICT system of independent operators.

The National Regulatory Authority for energy sector[122] neither exercise any rights or obligation pertaining to cybersecurity nor monitor or assess implementation of Cyber security strategy.

5.8.5   Cooperation and initiatives

The Strategy for the Development of Information Security in the Republic of Serbia for the period 2017-2020 recognises the need of cooperation between the public and private sectors, non-governmental organizations, the academic community and other relevant stakeholders as a key factor to raise the capacity to fight cybercrime and respond to incidents. International cooperation is one of the strategic priorities based on the above-mentioned strategy for the purposes of confidence building, experience, information sharing and capacity building.

Cooperation within Energy Community Parties
As a contracting party, Republic of Serbia cooperates in the Cyber Security and Critical Infrastructure coordination group (CyberCG) of the EnC for the purpose of promotion of high level security of network and information systems and CI through strategic cooperation and exchange of information.
Cooperation with EU Member States
The European Union with support of the Council of Europe launched the CyberCrime@IPA[123] project to strengthen the capabilities for the fight against cybercrime in the Republic of Serbia. The project helped

---

[120] *Action Plan for 2018 and 2019 for the implementation of the Strategy for the Development of Information Security in the Republic of Serbia for the period 2017-2020*

[121] *Rule book on terms and conditions for enrolment in the register of special centres for prevention of security risks in information communication systems*

[122] *Energy Agency*

[123] *CyberCrime@IPA. https://www.coe.int/en/web/cybercrime/cybercrime-ipa*

to raise awareness, enhanced cooperation between public and private sector as well as international entities, organizations and foreign states.

Along with CyberCrime@IPA the iPROCEEDS[124] project was also created joining EU, CoE and Republic of Serbia in the purpose of establishing search, seizure and confiscation of data and funds obtained by cyber criminals.

The high-tech crime prosecutor's office was involved in the preparation of standards, guidelines and procedures in scope of Council of Europe and European Union Project Global Action on Cyber Crime + (GLACY +).

Cooperation with other parties

In 2007 Serbia joined NATO Science for Peace and Security (SPS) Programme and has become increasingly active over time. In late 2017 staff from the Office of the National Security Council and Classified Information Protection of the Serbian Government were trained to deal with information systems security (INFOSEC) in real life situations, within the NATO SPS.

Serbia participates in the Project "Cooperation in combating crime in cyberspace targeting assets obtained via Internet crime in South East Europe and Turkey".

Public-private partnership

The "Petnica Group" cooperation initiative was established as a result of OSCE Mission to Serbia, DiploFoundation and the Geneva Centre for the Democratic Control of Armed Forces (DCAF) strategic partnership with the Petnica Science Centre. "Petnica Group" has regular meetings related to the national strategic priorities, preparation and adoption of the national Strategy for the Development of Information Security, as well as needed and possible modalities of cooperation in the field of cybersecurity. One of the parties involved is public enterprise "Elektroprivreda Srbije". The Group also conducted the first national policy-focused cyber exercise. OSCE published two issues of the Guide through information security in the Republic of Serbia in 2017 and 2018.

Provisions of the Law on Information Security related to cooperation of national CERT with special CERTs[125] (either public or private legal person or an organizational unit within a legal person, which is entered in the records of special CERTs managed by the National CERT) are established for prevention and protection against ICT security threats.

5.8.6   Overview of education and training programmes

Awareness campaign "Smart and Safe" is established in Serbia by the Ministry of Trade, Tourism, and Telecommunications for the purpose of educating, raising awareness about necessity of people, academics and economy involvement in modern digital world.

The Education, Audiovisual and Culture Executive Agency (EACEA) of the European Union finances two national Erasmus+ Capacity Building in the field of Higher Education (CBHE) implemented in the 2017 to 2020 period (projects ImprESS[126] and ISSES[127]). The ultimate goal of these projects is to develop new laboratories and higher education study programs in information security at multiple Serbian higher education institutions. According to the original project plan, the University of Novi Sad planned to develop a Critical Infrastructure and Industrial System Security Laboratory (CIISS Lab) and related research and training capabilities, with a

---

[124] iPROCEEDS BiH. https://www.coe.int/en/web/cybercrime/iproceeds

[125] Register of special CERTs is accessible at https://www.ratel.rs/uploads/documents/empire_plugin/Cert%20-%20ratel.xlsx

[126] Improving Academic and Professional Education Capacity in Serbia in the Area of Safety & Security (by Means of Strategic Partnership with the EU). http://impress.kpu.edu.rs

[127] Information Security Services Education in Serbia – ISSES. https://isses.etf.bg.ac.rs

specific focus on the energy sector. The joint Master 4.0 study program accredited as a collaboration of multiple Serbian universities in 2019 contains a limited number of cybersecurity courses, but does not contain a named cybersecurity module.

The legislative system of Serbia does not set requirement for energy sector companies to have staff trained as cybersecurity specialist, therefore no such training programme exists.

5.8.7 Gaps against EU legislation and standards

Cybercrime legislation

Legislation against Cybercrime is well implemented in the legislative system and allows investigation and prosecution of offences pertaining to cybercrime.

Identification of CI operators and OES

ECI designation is foreseen with the accession to the EU.

All energy sector stakeholders are identified as critical infrastructure in the legislation, the preparation of the list of specific organizations in the energy sector that will be designated as CI is underway.

The concept of providers of essential services from NIS directive is implemented in the Law on the Information Security through the notion of "ICT systems of special importance". The Law identifies ICT systems of special importance in the energy sector (generation, production, transmission and distribution).

National NIS strategy

The content of the Strategy for the Development of Information Security 2017-2020 is in compliance with NIS directive provisions pertaining to national NIS strategy. The Strategy encompasses security of ICT systems of special importance and is applicable to the energy sector. The Action Plan for 2018 and 2019 for the implementation of the Strategy for development and support of the information technology industry for the period 2017-2020 is adopted and executed albeit with some delays.

National Cybersecurity Authorities: Contact points

The Ministry of Internal Affairs is designated in the law as the ECIP contact point but its designation will come to power with the accession of RS to the EU. The Ministry of Internal Affairs is the contact point for protection, domestic information sharing and coordination of critical infrastructures.

Although there are several bilateral agreements related to cybercrime, there is no SPoC for international cooperation and energy sector cybersecurity information sharing with EnC CP/EU.

The Ministry of Trade, Tourism and Telecommunications is responsible authority for ICT system security and national cybersecurity authority in accordance to the NIS directive. The Regulatory Agency for Electronic Communications and Postal Services (RATEL) CERT is designated as the national CERT.

The Law on Information Security sets obligation for energy CI operators to designate responsible persons – a liaison officer. The responsibilities of the liaison officer are among others defined for communication with responsible contact point (ECI) for CI in Serbia – the Ministry of Internal Affairs. The transposition of such provision is in accordance with the provisions set in the ECI Directive.

Security plans and requirements

The security requirements defined in legislation are aligned with EU and international standards and good practices. Energy sector, including generation/production, transmission, distribution and marketplaces are obliged to prepare Operator Security Plans for CI and obtain approval of plans from the Ministry of Internal Affairs. Operators of ICT systems of special importance, including stakeholders in the energy sector, shall prepare, maintain and review security and continuity plans. Specific requirements laid out in the "Regulation about the closer regulation of protection measures information-communication systems of special importance" are in general aligned with ISO 27002 guidance.

Standardization

No gaps were identified, as EU wide cybersecurity standards (and candidate standards) are adopted as national standards, namely: SRPS ISO/IEC 27001:2014, SRPS ISO/IEC 27002:2015, SRPS ISO/IEC 15408-1:2014, SRPS ISO/IEC 15408-2:2014, SRPS ISO/IEC 15408-3:2014 and SRPS ISO/IEC 27019.

Operators level

Organisations in the energy sector comply with the legislative and regulative provisions laid out in the Law on Information Security and related regulations. Technical and organisational measures foreseen in the legislation are aligned with the ISO 27002 good practice. Although there is no legislative requirement on which standards are to be implemented, the organizations in the energy sector are beginning to implement or are following the ISO 27000 series standards.

Cooperation

Yearly report on ECI is adopted by the Government and submitted to the European Commission and to the interested countries to which each critical infrastructure has an impact.

The contact point for information exchange and coordination of activities related to European critical infrastructure with other EU member states and EU bodies is the Ministry of Internal Affairs.

The national CERT collects and exchanges information on the risks to the ICT systems security, and the events that jeopardize the ICT system security, and informs, warns and advises individuals who manage ICT systems in the Republic of Serbia, as well as the public.

5.9 Ukraine

Being a target of sophisticated cyber-attacks against energy critical infrastructure Ukraine began developing legislative and organizational capabilities on the national as well as energy sector level, including SOCs, incident response teams, technical security and management systems based on international standards and good practice. Partial gaps regarding the implementation of NIS and ECI directive and related EU good practice were identified.

The identification of energy infrastructure the disruption or destruction of which would have a significant impact on neighbouring countries has not been conducted. "Important facilities " and operators of electricity[128], gas and oil[129] are designated with decrees of Cabinet of Ministers but designation criteria are not publically available. Contact point for coordination and protection of critical infrastructure with EnC CPs has not been established. The Law on Critical Infrastructure Protection addressing CI identification and protection is expected to be adopted in 1 to 2 years.

The Law on the Basic Principles of Cyber Security provides basis for the identification of CII/ES operators including operators in energy sector. Cabinet of Ministers with a decree[130] adopted CII/ES operators' cybersecurity requirements that are in accordance with EU and international standards. As the procedure for designation of operators of CII/ES is not yet finished it is unclear whether energy sector operators must comply with the new cybersecurity requirements.

Operators in the energy sector are obliged to implement information security measures laid out in the energy sector specific legislation. Those provisions that are also applicable to SCADA systems are not completely aligned with EU cybersecurity legislation and good practice especially in the area of organizational controls and monitoring.

Cybersecurity authorities as well as energy sector operators are aware of existing deficiencies and started activities to address identified shortcomings with the implementation of technical and organizational cybersecurity measures, including technical security management systems as well as implementation of EU and international good practices. Ministry of Energy and Coal Mining is implementing centralized Industrial Centre for Cybersecurity for energy sector.

---

[128] *On approval of the list of especially important objects of the electric power industry, including the territories of the forbidden zone and the controlled zone of the hydraulic engineering structures, which are subject to protection by the departmental paramilitary security.*

[129] *On approval of the list of especially important objects of the oil and gas industry.*

[130] *On Approval of General Requirements for cyber-protection of Critical Infrastructure Objects*

5.9.1 SWOT analysis

S **STRENGTHS** Ukraine has been working towards implementation and strengthening of cybersecurity as it has been a target of series of sophisticated cyber-attacks against energy critical infrastructure.	**W** **WEAKNESSES** New Law on Critical Infrastructure is in adoption process with the aim to provide systemic measures and obligations for CI and CII protection including cybersecurity. Adoption timeline for the document is not clear but it is to be adopted in 1 to 2 years.
O **OPPORTUNITIES** Ministry of Energy and Environmental Protection of Ukraine specifies additional implementation of Complex System of Information Protection on SCADA infrastructure. The recent activities in set up of new responsible coordination bodies for cybersecurity activities have been accelerating recently.	**T** **THREATS** Ukraine adopted multiple cybersecurity laws and provisions, but as the energy sector CII operators and OES are not identified, they do not need to comply with such provisions. Individual actions (e.g. Ministry of Energy defining own compliance measures) are still defragmented.

5.9.2   European Critical Infrastructure and Essential Services legislation requirements

Identification of EnC Critical Infrastructure and Essential Services	
At the moment ECI/EnCCI is not identified and designated, however it is foreseen that it will be addressed in the Law on Critical Infrastructure Protection which is in the adoption. It should be noted that "Critical infrastructure facilities" in the energy sector were designated by two Decrees of Cabinet of Ministers based on the sectorial legislation but the criteria for the designation are not publicly available. The identification of CI (encompassing CII) and OES is foreseen in the national Cyber Security Strategy of Ukraine and in the Law on the Basic Principles of Cyber Security, with energy sector included. Criteria for CI identification and designation of CI/ES operators are not yet defined.	
Cyber Security Strategy of Ukraine, Draft Law on Critical Infrastructure, Law on the Basic Principles of Cyber Security in Ukraine, Decrees of Cabinet of Ministers[131]	*Lead: National Security and Defence Council of Ukraine*
Criteria for significance of disruptive effect are not defined in the legislation nor have been adopted that disruption based criteria for identification and designation of ECI/CI and CII/ES operators. Currently in the legislation there is no requirement for the definition of ECI/CI identification criteria. The Law on Basic Principles of Cyber Security defines the need for adoption of criteria for identification of information systems critical for the operation of CI and ES, however the related legislation is not yet adopted.	
Law on Basic Principles of Cyber Security	*Lead: /*

National Network and Information Security Strategy	
Cyber Security Strategy of Ukraine with its yearly Action plans addresses NIS directive provisions.	
Cyber Security Strategy of Ukraine	*Lead: National Security and Defence Council of Ukraine*

National Cyber Security organisational framework	
CI contact point that coordinates CI protection issues within the state and with others states is not designated. Ministry of Energy and Environmental Protection is responsible for the energy sector domestic cooperation.	
/	*Lead: Ministry of Energy and Environmental Protection*
Law on the Basic Principles of Cyber Security in Ukraine defines the State Service on Special Communication and Information Protection of Ukraine as the national cybersecurity authority responsible for coordination of CI related matters. CERT-UA is designated SPoC for cybersecurity and also designated CSIRT.	
Law on the Basic Principles of Cyber Security in Ukraine	*Lead: CERT-UA, State Service on Special Communication and Information Protection*
The General Requirements for Cybersecurity in Critical Infrastructure objects oblige CI/ES operators to implement measures and develop communication and reporting practices. Energy sector "Critical infrastructure facilities" and (CII/ES) operators were designated by two Decrees but not yet designated as CII/ES according to the new General Requirements so it is not clear whether they have to report and share information according to General Requirements.	
The General Requirements for Cybersecurity in Critical Infrastructure objects	*Lead: Ministry of Energy and Environmental Protection*

---

[131] Cybersecurity Strategy Of Ukraine

Security requirements for operators of Critical Infrastructure and providers of Essential Services

Ministry of Energy and Environmental Protection of Ukraine laid out information security requirements that shall be implemented by the operators in the energy sector in the Complex System of Information Protection (KSZI). KSZI standards are partially outdated and do not encompass all organizational controls foreseen in the EU cybesecurity standards and good practice.

With adoption of the Law on the Basic Principles of Cyber Security and General Requirements for Cybersecurity in Critical Infrastructure objects, Ukraine adopted legislation pertaining to CI protection of cybersecurity and recognized the need for their protection. The decision goes in detail on creation of security plan, implementation of necessary measures, designation of responsible person or unit and sets obligation to follow standards and good practices.

New Law on Critical Infrastructure Protection addressing the need to ensure stable and uninterrupted operations of CI, facilitate cooperation between public and private sector, need to prevent unauthorized interference, prevent crisis situation, and increase the level of protection with sector specific measures, including cybersecurity, as well as designation of responsible Authority and development of National critical infrastructure protection plan is in the adoption process. It is foreseen that it will be adopted in 1 to 2 years.

The General Requirements for Cybersecurity in Critical Infrastructure objects, Complex System of Information Protection, Basic Principles of Cyber Security	*Lead: Energy sector organizations; Ministry of Energy and Environmental Protection*

Standardisation

ISO 27001, 27002 and 15408-1, 2 and 3 standards have been adopted by Ukraine but are not obligatory for energy sector.

Ministry of Energy and Environmental Protection of Ukraine developed Information Security Policy for Energy sector operators which prescribes implementation of "Complex System of Information Protection". Main standards of this framework are national, and encompass DSTU 3396 0-96, DSTU 3396 1-96, DSTU 3396.2-97, DSTU 1.5: 2003, and TZI 1.6-002-03 although are in need of modernisation as they are not in compliance with international and European standards.

Lead: Research and Training Center of Standardization, Certification and Quality

Besides CP Moldova, Ukraine has electricity interconnections with the EU Member States associated with possible cascading effects to Poland, Slovakia, Hungary and Romania. The Ukrainian gas transmission system is well interconnected with vast capacity with all neighbours, namely Russia, Belarus, Poland, Slovakia, Hungary, Romania and Moldova. Ukraine is the most important gas transit country for Russian gas going to the EU Member States, therefore the cybersecurity aspect related to the gas sector in Ukraine, especially to Ukrtransgaz as the leading company engaged in transmission and storage of natural gas in Ukraine.

5.9.3   Legislation at the national Level

Strategy and action plans

National Security and Defence Council of Ukraine adopted Cyber Security Strategy (Strategy) for ensuring protection of CII, safe cyber space, its safe use for individuals, society and government. Main focus is on the development of institutional and legislative system pertaining to cybersecurity, strengthening the security and defence sector capabilities, ensuring security of CI and state information sources. Strategy combined with

annual action plan allows progress assessment, timeframe setting, prioritisation and evaluation of needs and changes that have to be implemented.

The Strategy outlines the need to harmonize and improve the legislative system for protection of CII and to establish criteria for evaluation of ICT systems of critical nature. The needed changes are outlined in the Strategy as a need for regulation encompassing requirements related to protection and strengthening the cybersecurity of CII/ES operators. In addition, development of communication and information exchange capabilities between operators of CII, private sector and state agencies are foreseen. Strategic goal related to cooperation describes the need for owners or operators of CII/ES to establish cyber defence units for protection of infrastructure. The Strategy among other strategic goals identifies the need to determine necessary employee qualification criteria, their periodic performance assessment and their compliance with adopted criteria.

Legislation against cybercrime

Ukraine is a ratifying party of the Budapest Convention and through the changes in legislative system managed to incorporate and implement provisions. The definitions demanded by the Budapest Convention have been implemented and accepted in the Law on Telecommunications, Law on Protection of information in Telecommunication systems, Criminal procedure code as well as Criminal code, allowing Ukraine to define criminal acts defined in the Budapest Convention and prosecute them as well. Ukraine is in the process of further harmonization of its legislative system to fully implement the Budapest Convention mainly in the area of international cooperation.

Budapest Convention is implemented in: Law on Protection of Information in Telecommunication Systems, Law on Telecommunications, Criminal Code, Criminal Procedure Code, Law on Preventing and Combating Cybercrime.

Energy sector relevant cybersecurity legislation

Law on the Basic Principles of Providing Cyber Security of Ukraine recognizes the need to designate energy sector CII/ES operators as well as state infrastructure of importance for security and defence. The Law defines the legal and organizational foundation for protection of state interests, people, society and cyber space. The Law aims to establish capabilities and state policies in the field of cybersecurity and defines the need for institutions to adhere to basic cybersecurity principles and to facilitate cooperation for providing greater level of security in the cyberspace. The Law foresees the assessment of CI, CII and OES operators and infrastructure as well as creates an obligation for operators to implement related regulations. For that reason, Cabinet of Ministers of Ukraine adopted General Requirements for Cybersecurity in Critical Infrastructure objects[132].

The General Requirements obligate operators of CII/ES to create security policy plans, designate information security officer or unit, define responsibilities of the users and their access, define a list of software and hardware resources needed for operation and the level of their criticality, implement information security risk management policy that has to follow recommendations of DSTU ISO / IEC 27005. Operators must implement user identification and authentication measures, security incident and event management platform,

---

[132] *General Requirements for Cybersecurity in Critical Infrastructure objects,   https://zakon.rada.gov.ua/laws/show/518-2019-п?lang=en*

protective measures for networks and infrastructure, implement business continuity management policy including redundancy systems.

CII/ES operator's top management must conduct a yearly assessment of cybersecurity, ensure software/hardware is up to date and implement comprehensive information/cybersecurity system encompassing awareness raising activities for employees, sharing of information and cybersecurity education.

Although the energy sector has been deemed critical by legislative provisions, it is not clear whether all energy sector operators must comply with such standards and provisions mentioned above, as they have not been designated yet. Despite of that the institutions in energy sector recognized the need to strengthen the cybersecurity and are implementing measures.

Ministry of Energy and Environmental Protection of Ukraine developed Information Security Policy for Energy sector operators which prescribes implementation of "Complex System of Information Protection (KSZI)" also applicable to SCADA infrastructure. Main standards of this framework are national (e.g. DSTU 3396 0-96, DSTU 3396 1-96, DSTU 3396.2-97, DSTU 1.5: 2003, and TZI 1.6-002-03), relatively outdated and not in compliance with international and European standards especially in the area of organizational controls. It is important to note that the Ministry of Energy and Environmental Protection is developing energy sector specific cybersecurity strategies, regulations and incident response capabilities.

ISO 27001, 27002 and 15408-1, 2 and 3 standards have been adopted by Ukraine but are currently not obligatory for energy sector[133].

At the time of writing of this report the Law on Critical Infrastructure Protection was in the adoption process and is expected to be accepted in 1-2 years. Energy sector is defined by the draft Law as CI sector and more comprehensive criteria should be developed for identification of CI/ES operators. The draft Law does address the need to ensure stable and uninterrupted operations of CI, facilitate cooperation between public and private sector, the need to prevent unauthorized interference, prevent crisis situation, and increase the level of protection with sector specific measures, including cybersecurity, as well as designation of responsible Authority and development of National critical infrastructure protection plan.

The Law foresees development of legislation related to criteria for critical objects and vital services, stipulation of public-private partnership, exchange of information, definition of an authority responsible for development and implementation of a policy for critical infrastructure protection and development of National critical infrastructure protection plan.

Ukrainian legislative framework includes multiple documents[134] pertaining to cybersecurity specific for business sectors/services which is not applicable to energy sector.

5.9.4 National Cybersecurity Authorities

One of the Cyber Security Strategy goals was to establish national cybersecurity system with the goal of cooperation in the area of cybersecurity. Different stakeholders from state agencies, local government,

---

[133] *https://zakon4.rada.gov.ua/laws/show/v2170323-14*

[134] *: Law of Ukraine On State Service of Special Communication and Information Protection of Ukraine No 3475-IV of 23 February 2006; Law of Ukraine On Protection of Information in Telecommunication Systems No 80/94-BP of 5 July 1994; Law of Ukraine On Information No 2657-XII of 2 October 1992; Law of Ukraine On Telecommunications No 1280-IV of 18 November 2003; Law of Ukraine On State Secrets No 3855-XII of 21 January 1994; Law of Ukraine On Personal Data Protection No2297-VI of 1 June 2010; Criminal Code of Ukraine No 2341-III of 5 April 2001.*

military, law enforcement, research and education institutions, non-governmental organizations, private organizations, operators of CI would be included in a platform for cooperation, experience, knowledge and information sharing.

Key step towards that goal was establishment of National Cyber Security Coordination Center. It is a working organisation of the National Security and Defence Council. The Center serves as a supervisor, analyses national cybersecurity and assesses preparedness to combat cyber threats. It is responsible for detection and estimation of potential and actual threats. It organizes and participates in international or interdepartmental cybersecurity training courses and exercises.

State Service of Special Communication and Information Protection of Ukraine has the authority to define and implement national cybersecurity policy as well as to coordinate activities of other state bodies in terms of cybersecurity and implementation of Strategy. State Service for Special Communication and Information Protection of Ukraine has developed CERT-UA to strengthen the incident response capabilities.

CERT-UA is national CERT responsible for protection of the state information resources and ICT systems from unauthorized access, misuse of data or violation of privacy, integrity and availability. CERT-UA cooperates internationally as well as domestically for mitigation of threats, cooperation, sharing of information and good practices.

Security Service of Ukraine (SBU) is responsible for fighting cyber terrorism and serious cybercrime, including investigation of the cyber incidents involving critical infrastructure, implement counterintelligence and operational-investigative measures to combat cyber espionage, computer emergency response for national security and protection of vital information sources. Security Service of Ukraine currently operates MISP system for exchange of information about cyber-attacks and good practice sharing.

National Police is responsible for fighting, preventing and investigating cybercrime incidents through its specialized Cyber Police unit. The Cyber Police unit is designated as a 24/7 single point of contact for purposes of information sharing regarding to cybercrime, international assistance in criminal matters as well as investigation and cooperation with international entities and agencies.

Ministry of Defence of Ukraine is responsible for cybersecurity with responsibilities pertaining to cyber defence, international cooperation with NATO and establishment of capabilities for joint protection and defence, and cybersecurity of CI of MoD in cooperation with State Service of Special Communication and Information Protection as well as Security Service of Ukraine.

National Regulatory Authority for the energy sector[135] neither exercise any rights or obligations pertaining to cybersecurity nor monitor or assess implementation of Cyber security strategy.

5.9.5   Cooperation and initiatives

In the Cyber Security Strategy Ukraine recognizes the need for cooperation on domestic and international level. Ukraine also recognizes the need to strengthen the cooperation between public and private sector as well as the cooperation with civil society for cybersecurity and defence. On the international level Ukraine recognizes the importance of international cooperation for building trust and confidence as well as creating a cooperative approach to combat and prevent cybercrime, threats and prevention of use of cyber space for unlawful and military purposes.

---

[135] *National Energy and Utilities Regulatory Commission (NEURC)*

Cooperation within Energy Community Parties

As an EnC contracting party Ukraine cooperates in the Cyber Security and Critical Infrastructure coordination group (CyberCG) of EnC for the purpose of promotion of high level of security of network and information systems and CI through strategic cooperation and exchange of information.

Cooperation with EU Member States

Ukraine cooperates in EU and CoE Eastern Partnership Region[136] programmes and initiatives (CyberCrime@EAP). CyberCrime@EAP II has been focused on improving mutual legal assistance in international cooperation on the basis of Budapest Convention as well as developing and designating the SPoC for 24/7 communication and cooperation – Cyber Police department. CyberCrime@EAP III has been focused on enhancing public-private cooperation for purposes of prosecution, cooperation and exchange of data between law enforcement and ISP. There have been multiple cooperation programs with British and Estonian Partners that provided modern hardware and software for investigative and forensic activities of Cyber Police department.

Within the AAP 2018[137] framework Ukraine cooperates with EU for consolidation of legislative framework in the field of cybersecurity in line with EU acquis as well as building of capabilities of Ukrainian institutions to protect critical infrastructure and resilience.

Cooperation with other parties

Republic of Ukraine is active in international cooperation with other countries. Ukraine together with Georgia, Azerbaijan and Moldova developed GUAM[138] – regional organization which tackles issues in the cyber-domain among others. Through working groups on cybersecurity above mentioned parties discuss wide range of issues pertaining to combating and prevention of cybercrime, amendments to national legislation, procedures and operative situation as well as exchange information and good practices.

NATO is helping Ukraine with establishment of a cyber-incident response centre, which will be responsible to help with incidents or attempts to interfere into their cyber networks and critical infrastructure. The NATO Trust Fund on Cyber Defence for Ukraine aims to provide Ukraine with the necessary support to develop CSIRT-type technical capabilities, including laboratories for cybersecurity incident investigation. Security Service of Ukraine is responsible for conducting organizational and institutional changes and implementation of necessary provisions for achieving above mentioned objectives. Ukraine cooperates with partner countries within NATO, such as Romania, Albania, Estonia, Hungary, Italy, Portugal, Turkey and United States. There have been NATO exercises and trainings organized for Ukrainian institutions and stakeholders responsible for protection of national defence infrastructure.

Ukraine cooperates internationally in the field of cybersecurity in the energy sector through different international bi- or multi-lateral programmes as well as support and aid programmes like USAID, NARUC and Utility Cyber Security Initiative for the Black Sea Region.

Public-private partnership

---

[136] https://www.coe.int/en/web/cybercrime/cybercrime-eap-iii

[137] Improving Cyber Resilience in the Eastern Partnership Countries: https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/c_2018_8184_f1_annex_en_v1_p1_1000418.pdf

[138] GUAM. https://guam-organization.org/en/1st-meeting-of-guam-working-group-on-cyber-security/

Ukraine cooperated in international program created by EU and CoE in the Eastern Partnership region for development of close cooperation between public and private sector. The program allowed establishment of a dialogue between law enforcement agencies and ISPs for sharing of data, building confidence and strengthening cooperation for prosecuting and preventing cybercrime.

MISP-UA has been established by Security Service of Ukraine as a platform for voluntary exchange of information about cyber incidents. Platform allows sharing of information pertaining to cybersecurity with State Service of Ukraine and receive support from SBU for counter measures for greater cybersecurity. Organizations from energy sector have cooperated trough MISP-UA platform with SBU for greater coordination, cooperation, communication and support in the field of cybersecurity and implementation of necessary measures for greater security. Under law only state or public institutions are obliged by law to communicate with either CERT-UA, through MISP or with police. Private sector cooperates only voluntary.

5.9.6   Overview of education and training programmes

There is an official Specialist of Cyber Security university study programme in Ukraine (Bachelor of Science).

Organizations in the energy sector recognize the need to educate specialists for cybersecurity and to raise the cybersecurity awareness. Energy sector organizations are conducting educational activities to strengthen the information security culture through training and awareness raising campaigns as well as started to develop and train specialized staff for monitoring and incident response.

There are various stakeholders conducting activities in the field of cybersecurity awareness raising such as CERT-UA, Cyber-Police and Security Service of Ukraine among others. But there is no formal program on the national level that would encompass all of the relevant stakeholders as all the activities and awareness raising campaigns are done ad hoc for specific sector, demographic group or others.

Trainings are often organized or done ad hoc by Security Service of Ukraine or Cyber-Police department for CI/ES operators and public organizations. State Service of Special Communication and Information Protection of Ukraine organizes trainings for auditors as well as certifies them.

There have been trainings organized under international cooperation and support initiatives and programmes, e.g. NATO Task Force Cyber Defence exercise where multiple stakeholders were trained for protection of CI in case of a major cyber-attack.

Local chapter of ISACA organized multiple trainings for the purpose of awareness raising and educating on cybersecurity issues and threats.

5.9.7   Gaps against EU legislation and standards

Cybercrime legislation
Legislation against Cybercrime is partially implemented in the legislative system and allows investigation and prosecution of offences pertaining to cybercrime. Legislation should be fully harmonized with the Budapest Convention and implemented in legislative system.
Identification of Critical Infrastructure and OESs

Legislation pertaining to cybersecurity outlines energy sector as critical sector, however no criteria has been set or is publicly available for identification of CI and EnCCI. Operators in the energy sector were designated with the resolutions of Cabinet of ministers but criteria for the identification are not known in addition, it would be possible that the lists are incomplete and that some of the critical infrastructure is not included in the publicly available lists.

National Network and Information Security strategy

Cyber Security Strategy of Ukraine and related yearly Action plans address NIS directive provisions including: the need to identify CII and ES, challenges related to national cybersecurity system of different stakeholders, CII and ES cybersecurity and protection, training initiatives, implementation of international standards. The Strategy does not address in detail energy specific risks or threats.

National Cybersecurity Authorities: Contact points

As the Law on Critical Infrastructure is not yet adopted Ukraine did not establish an ECI or CI contact point. However National Security and Defence Council of Ukraine is responsible for coordination of activities regarding protection of CI and thus performing CI contact point activities.

Law on the Basic Principles of Cyber Security in Ukraine defines CERT-UA as SPoC for cybersecurity and CSIRT, while State Service on Special Communication and Information Protection of Ukraine is defined as national cybersecurity authority and coordinating body for matters of CI.

National Security and Defence Council of Ukraine is responsible for measures and coordination regarding protection of CI and CII, with National Cybersecurity coordination Center responsible for cybersecurity coordination.

Security plans and requirements

Implemented security requirements also audited by inspectors are partially outdated and do not encompass all necessary organizational controls as foreseen in the international or European standards. Security requirements in the more recent legislation adopted in last year is aligned with EU and international standards but it is not clear whether operators of energy sector must comply with the provisions, as they have not yet been designated as CI or ES.

Energy sector operators recognize the need to implement EU and international cybersecurity standards and good practice but it can take some time to achieve appropriate maturity level. Ministry of Energy and Coal Mining is working on setting up the Industrial Centre for Cybersecurity.

Standardization

No gaps were identified, ISO 27001, 27002 and 15408-1, 2 and 3 standards have been adopted by Ukraine.

Operators level

Organisation in the energy sector shall implement requirements laid out in "Complex System of Information Protection (KSZI)" also applicable to SCADA infrastructure; implementation is monitored by ministry inspectors. KSZI is relatively old and does not completely follow international good practice especially related to the organisational controls. Ministry of Energy and Environmental Protection is in the process of development of cybersecurity strategies, sector specific provisions as well as development of capabilities for incident response.

Although the cyber-security legislation is in the process of renewal, organizations in the energy sector like gas TSO Ukrtransgaz and electricity TSO Ukrenergo have started implementation of international standards (e.g. ISO 27002), developing monitoring and incident response capabilities, as well as technical and organizational measures for protection and cybersecurity.

Cooperation

Ukraine developed multi-level approach to cybersecurity creating possibilities of cooperation among public institutions. The public-private cooperation is currently in development as platforms for voluntary information sharing on incidents (MISP) has been developed.

Communication procedures pertaining to communication between energy sector, Central Cyber Security Authority and EU Member States or EnC CPs must be established as currently legislative system does not foresee communication between them but only within the country. Currently CERT-UA does exercise cross border liaison function and could be used for communication activities but formalization and adoption of necessary legislation must be conducted.

Ukraine cooperates in international organizations and bilaterally with other foreign entities, states and their institutions. Example of this would be cooperation within GUAM, USEA – UCSI and USAID as well as NATO.

6 Overview of cyber threats and risks for EnC CP

The energy sector cybersecurity threat landscape in 2019 for EnC Contracting Parties made a significant shift in focus towards critical infrastructure protection. The possibilities of domino/cascading effect (cross-sectorial and cross-national as well) during cybersecurity incidents are becoming a significant security risk as legacy systems are overlapped with new technology (smart grid, virtual power plant etc.). The source of those developments was a shift in motives and tactics of the most important threat agent groups, namely cyber-criminals and state-sponsored actors hence a significant rise of cyberwarfare in energy as a threat. The cybersecurity risks assessment was done by keeping these changes in mind.

Cybersecurity refers to security of cyberspace, where cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalised telecommunications and/or information technology network and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that Cyberspace. Cybersecurity therefore encompass the CIA triad paradigm (confidentiality, integrity and availability) for relationships and objects within cyberspace and extend that same CIA triad paradigm to address protection of privacy for legal entities (people and corporations), and to address resilience (recovery from attack).

In the energy sector cybersecurity is of crucial significance as IT and OT systems are connected through cyberspace delivering/transmitting data and executing controls to energy systems. The dynamics of changes in those relations for EnC members means a new level of commitment in developing their resilience against the cyber risks.

Moreover, cyber risk is the likelihood that something bad will happen that causes harm to a cyber asset (or the loss of an asset). Vulnerability is a weakness that could be used to endanger or cause harm to a cyber asset. A threat is anything (man-made or act of nature) that has the potential to cause harm. The likelihood that a threat will use a vulnerability to cause harm creates a risk. When a threat does use a vulnerability to inflict harm, it has an impact. In the context of cybersecurity, the impact is a loss of availability, integrity, and confidentiality.

The energy sector cybersecurity threat landscape changes in 2018 for EnC members made significant shift in focus towards critical infrastructure protection. The possibilities of domino/cascading effect during cybersecurity incidents are in rise as legacy systems are overlapped with new technology (smart grid, virtual power plant etc.). The source of those developments was a shift in motives and tactics of the most important threat agent groups, namely cyber-criminals and state-sponsored actors. Hence a significant rise of cyberwarfare in energy as a threat.

The **cybersecurity risk assessment's methodology** used in the study follows good practice[139] and encompass the following key steps:

- Risk assessment context establishment encompassing definition of impact assessment criteria, probability categories and organisations included in the risk assessment
- Analysis of risk before the application of the risk reduction measures and controls (inherent risks)[140]
- Preparation of energy sector specific risk scenarios that address most critical inherent risks
- Scenario-based risk assessment per CP.

Risk assessment context establishment

In order to have a systematic and unified framework for risk assessment across all CPs, as well as across the gas and electricity sectors, a framework for defining the different classes for likelihood and probability that will be used for the calculation of the risk level for the various scenarios considered in the context of this study.

Likelihood

The likelihood of threat occurrence was assessed based on relevant national security assessments[141], previous incidents, on the exposure level or vulnerability of the CI to the initiating hazard and/or to the loss of the service of another CI. information was combined with data from well-known sources and available country/region historical data.

Table 7: Likelihood levels

Likelihood level	Description (Likelihood level assigned if one of criteria met)	Indicative frequency (expected)
Almost certainly	The stakeholder is exposed to this threat on a daily basis; common threats (e.g. malicious code).	daily
Probably	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)	monthly
Possibly	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	yearly
Rarely	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	Once in several years

---

[139] *ISO/IEC 27005 Information technology — Security techniques — Information security risk management*

[140] *So called Inherent risk*

[141] *Primary source where available.*

Impact

The categories for assessing and quantifying **impact** were based on the respective categories stipulated in the EU legislation and are listed below:

- H - Human impacts (usually measured in numbers)
- EE - Economic and environmental impacts (usually measured in Euros)
- PS - Political/social impacts

The impacts were mapped to a semi-quantitative scale comprising classes:

- Catastrophic/ Disastrous (CA)
- Significant/Very serious (VS)
- Moderate/Serious (SE)
- Minor/ Substantial (MI)

The recommended approach complies with cross-cutting criteria of the ECI directive, namely:

- casualties criterion (assessed in terms of potential number of fatalities or injuries);
- economic effects criterion (assessed in terms of the significance of economic loss including potential environmental effects);
- public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life; including the loss of essential services).
- loss of asset criterion (assessed in terms of the impact on asset usability and/or degradation of products or services; including the loss of essential services).

In essence, the impact assessment recommendations are compatible and very similar. The loss of energy service in CI directly translates to loss of vital services and affects citizens. However, one needs to assess the social effects of the hazard, but also the damage. In addition, the analysis requires a detailed mapping of potential dependency chains among CIs.

Societal impact will be assessed based on the SEGRID Risk Management Methodology model represented in "*Figure 13: Political/Social impact (PS) impact assessment criteria*"

Wherever applicable, **Human impacts (H)** are determined based on the country specific criteria.

Economic and environmental impacts (EE) are determined based on the country specific criteria if available[142]. In country-specific data are not available, the assessment scale is calculated according to the following formula

$$8*\log_{10}(loss\ in\ UR/1.000.000)/\log_{10}(Country\ BDP/1.000.000)$$

---

[142] *It should be noted that the country cyber incident impact assessment criteria might be classified.*

Resulting assessment tresholds are represented in "*Table 8: EE assessment criteria*"

LOSS RANGE	BDP RANGE 10.000.000.000 €	25.000.000.000	50.000.000.000	100.000
1.000.000 €	0	0	0	0
10.000.000 €	2	2	2	2
50.000.000 €	3	3	3	3
100.000.000 €	4	4	3	3
1.000.000.000 €	6	5	5	5
10.000.000.000 €	8	7	7	6

Table 8: EE assessment criteria

Political/social impacts (PS) are determined based on the adapted SEGRID[143] impact assessment methodology using country population aware function for the assessment of impacted population. Mapping between outage duration, population affected and impact level is represented in the "*Figure 13: Political/Social impact (PS) impact assessment criteria*".
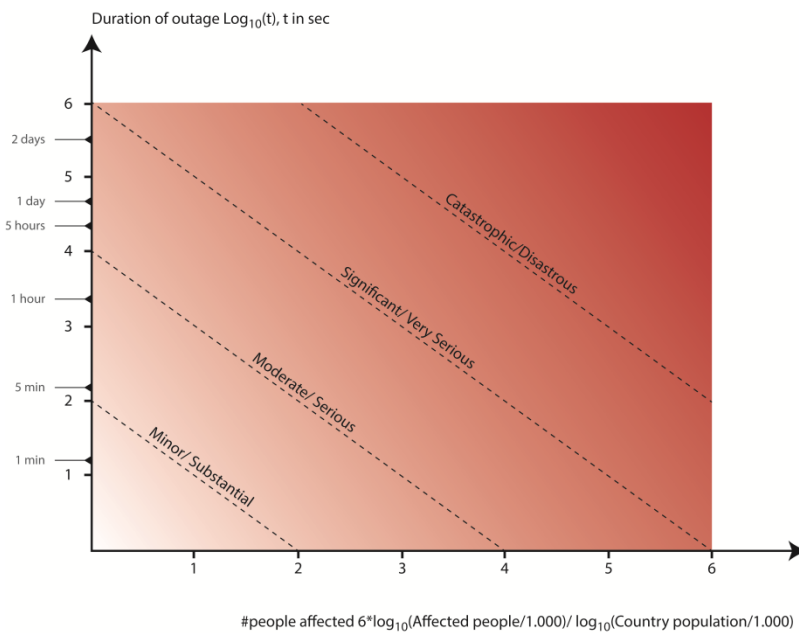
Figure 13: Political/Social impact (PS) impact assessment criteria

---

[143] https://segrid.eu/

Risk level

Risk evaluation level is defined on matrix function that maps assessed impact consequence (from threats valorized through vulnerabilities) and impact likelihood (the possibility of such threat to occur) to risk level:

$$Risk_{map}(Impact, Probability) \rightarrow Risk\ level$$

.

Likelihood Consequence	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

Table 9: Mapping of Impact and probability to risk level

Vulnerabilities Identification

Vulnerabilities were identified based on the categories identified below:

- Hardware
- Software
- Network
- Personnel
- Site
- Organization

In the risk assessment model developed in the context of this study, the stakeholders of the energy sector were grouped as shown in the list below, where each particular group is characterised by the same or very similar inherent risk.

- 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[144]

The following risks were also taken into account in the context of the assessment performed in this study:

- Risks related to organized energy balancing/trading infrastructure;
- Risks related to digital service providers;
- Risks related to telecommunication operators and providers; and
- Cross-sectorial cascading risks

Analysis of risk before the application of the risk reduction measures and controls

The risk analysis was performed for each energy stakeholder following the steps outlined below

- determination of assets (per group),
- assessment of highest possible impact without any implemented security measures, and
- identification of threats

resulting in the evaluation of energy sector inherent cyber risk.

Key information systems related to the energy sector stakeholder's groups (determined in a previous step of risk assessment) were identified as a first step of analysis. As an part of this process, the steps carried out for each on of the stakeholder groups are represented in a *"Table 11: Sample of impact assessment (Gas TSO)"* along with the respective analysis results. For each asset group considered, potential impacts were assessed, considering also any potential lack of the appropriate risk mitigation measures or the required risk controls. The highest possible impact reflects the situation where the maximum impact is considered across all impact categories (H, EE, and PS). Moreover, and in order to further assess the impact that might have to the energy sector compromised of the identified assets, different scenarios were developed, analysed, and assessed. Impact scenarios were later used of the development of the specific risk scenarios.

Cyber threats were also identified and categorised based on the ENISA threat landscape 2018 report and amended with recent publicly available information. For the purpose of this assessment cyber threats were grouped in eight (8) general categories, as listed below:

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

---

[144] *Note that a balancing market system was defined and assessed as a part of TSO/DSO infrastructure. Those systems/processes differ from pure trading platform based financial instrument energy markets being analysed in this group*

Based on the ENISA reports these are the details regarding energy sector related general threats taken into account in the stakeholder-specific threat scenario identification:

Table 10: Threat categories

Malware	Malware, short for malicious software, is a kind of software that can be installed on a computer without approval from the computer's owner. There are different kinds of malware that can hurt computers, such as viruses and Trojan horses. The term also includes other intentionally harmful programs, such as spyware and ransomware. These programs can steal passwords, delete files, collect personal information, or even stop a computer/system from working at all.
Web Based Attacks/Web application attacks	A web threat is any threat that uses the World Wide Web to facilitate cybercrime. They benefit cybercriminals by stealing information for subsequent sale and help absorb infected PCs into botnets or to gain access to internal systems through web interface.
Social engineering/Phishing/Spam	Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme. It mostly poses threat to confidentiality. Phishing and spam are threat tools used mostly in such schemes.
Denial of Service (DoS)	A denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet or its internal network. A denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.
Insider Threat	An insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems. The threat may involve fraud, the theft of confidential or commercially valuable information, the theft of intellectual property, or the sabotage of computer systems. The insider threat comes in three categories: 1) malicious insiders, which are people who take advantage of their access to inflict harm on an organization; 2) negligent insiders, which are people who make errors and disregard policies, which place their organizations at risk; and 3) infiltrators, who are external actors that obtain legitimate access credentials without authorization.
Cyber Espionage/Cyberwarfare	Cyber espionage, is the act or practice of obtaining secrets and information without the permission and knowledge of the holder of the information from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet, networks or individual computers through the use of proxy servers, cracking techniques and malicious software including Trojan horses and spyware.

Botnet	A botnet is a number of internet-connected devices, each of which is running one or more bots. Botnets can be used to perform distributed denial-of-service attack (DDoS attack), steal data, send spam, and allows the attacker to access the device and its connection. The owner can control the botnet using command and control (C&C) software.
Ransomware	Ransomware is a type of malware that prevents users from accessing their system or data. Ransomware spreads through e-mail attachments, infected programs and compromised websites. Usually it encrypts user documents, sends the encryption key to a remote C&C server and demands a ransom to be paid before allowing the victim access to the decryption key.

Summary results per stakeholder group and per threat categories are represented in the *"Table 12: Energy stakeholders inherent risk "*.

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 distraction 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				

Table 11: Sample of impact assessment (Gas TSO)

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

Table 12: Energy stakeholders inherent risk assessment

Risk level is presented is described in colours; red represents high risk (deep red is critical risk), yellow is medium risk and green is low risk. Risks are divided by categories of potential threats/stakeholder for the energy sector.

Risk analysis

Energy sector stakeholders' specific risk scenarios covering significant impacts and inherent risks were developed for each stakeholder group. Scenarios were developed based on identified threats, energy sector stakeholders and their IT assets considered in the scope of the risk analysis, prior to the application of the risk reduction measures and controls. To ensure credibility each risk scenario was developed having in mind incidents that have occurred in the energy sector. For each stakeholder least two threat group/impact scenarios are defined, as well as an number of additional cascading effects scenarios (if applicable) to ensure adequate coverage of the cyber risk assessment. The list of the developed risk scenarios used per CP risk assessment is given in the *"Table 13: List of used combinations of stakeholders and cyber risk scenarios "* with one randomly selected example in the Figure 14: Example of risk scenario Complete description of risk scenarios is in the Chapter *"6.1 Inherent risk assessment of impact scenarios"*.

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
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

Table 13: List of used combinations of stakeholders and cyber risk scenarios

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.

Threat	Vulnerability	Likelihood	Quantified Impact on Energy Sector		
			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				

Figure 14: Example of risk scenario

Some infrastructural/process parts of the Gas TSO were identified which are considered critical but have a moderate or low impact due to the fact that those systems are usually operated in high security environments. More specifically, case gas storage is basically considered a critical process/system, especially during development phase, but when developed it is operated in high security surroundings with manually override implemented as compensating controls which makes possible impacts much lower.

Regarding balancing markets, especially if they are connected to EU balancing markets through ENTSO-E or ENTSO-G impacts are lowered as these processes/systems are not only supervised and monitored by TSO but also by the ENTSO-E or ENTSO-G. In some cases, cross border exchange of balancing services started to emerge on bilateral/trilateral level among CPs, which again implies lower impact probability.

6.1 Inherent risk assessment of impact scenarios

Inherent risk assessment of developed scenarios was performed to provide a baseline to which can be compared per Contracting Party risk assessment provided in the next Chapter. The inherent risks were assessed based as baseline on the likelihood and impact of the scenarios defined in the previous Chapters. The result is represented in *"Figure 15: Spider chart presentation of risk scenarios – inherent risk"* where the number reached on the diagram from a scenario is the level of inherent risk measured by risk model
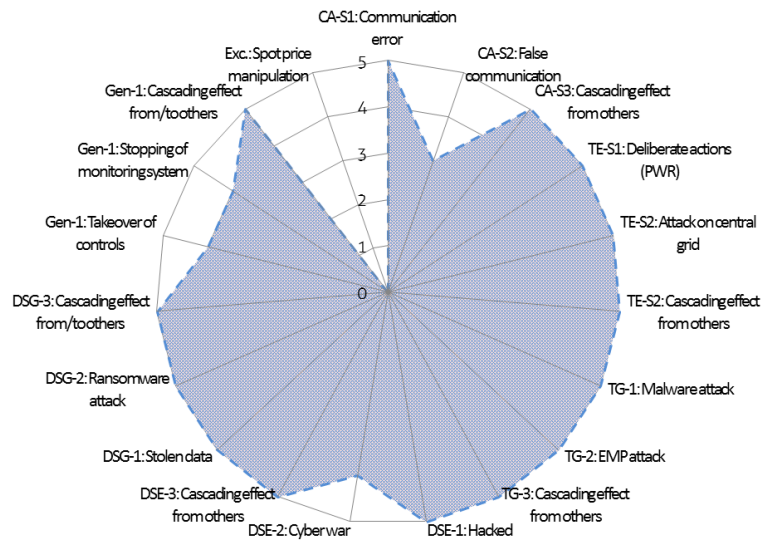
Figure 15: Spider chart presentation of risk scenarios – inherent risk

Larger number on the spider chart represents larger risk (scale from 0 to 5 is used). We can conclude that sectorial inherent cybersecurity risks are quite high for almost all the scenarios. This shows us that we had chosen scenarios with properly high impact. The inherent risk levels can give us a clear picture if compared to each country's risk.

The most important inherent cyber risks for energy sector stakeholders in EnC CPs are based on the performed assessment:

NRA/CA

- Lack of regulatory framework for defining and supervising cyberspace (missing critical infrastructure and/or essential services regulation)
- Missing interoperability with other organisations, a cascading effect high risk (Insider Threat, Cyberwarfare)
- The inability to communicate with other stakeholders and/or provide sufficient expertise in a case of an incident, a cascading effect critical risk (DoS, Social engineering)

TSOs in general[145]

- Lack of regulatory framework for defining and supervising cyberspace (missing critical infrastructure and/or essential services regulation)
- Infection of OT systems (SCADA etc.) and legacy systems through IT network (Malware, Ransomware, Botnet)
- Sabotage on OT, a cascading effect high risk (Insider Threat, Cyberwarfare, Ransomware, Botnet)
- The inability to react in a case of an incident, a cascading effect high risk (DoS, Social engineering, Phishing, Spam, Ransomware)

---

[145] *As the same remarks are proper for both electricity and gas sector TSOs we did not segregated them to include separate conclusions, the same statement is valid for DSOs*

DSOs in general

- Lack of regulatory framework for defining and supervising cyberspace (missing critical infrastructure and/or essential services regulation)
- Sabotage on OT, a cascading effect high risk (Ransomware)
- The inability to react in a case of an incident (Social engineering, Phishing, Spam, Ransomware)

Power generation

- Lack of regulatory framework for defining and supervising cyberspace (missing critical infrastructure and/or essential services regulation)
- Infection of OT systems (SCADA etc.) and legacy systems through IT network (Malware, Ransomware, Botnet)

The medium and low risks of other stakeholders may not represent such critical impact for an EnC CP in this context but are also very important for future more detailed local assessment and risk management.

Contracting Parties cyber risk assessment

Assessment of country specific risks in Chapters from 6.2 and 6.10 is based on the publicly available information as well as on the information provided by energy sector stakeholders in scope of this study. Obtained Contracting Party cyber threats specific information and information on implemented controls at energy sector stakeholders was assessed according to risk assessment methodology and mapped to risk level for each scenario. CP risk profile is represented in a spider chart on which is also presented inherent risk as a baseline.

The spider charts for each CP encompass blue part which represents inherent risks and grey part which is the CP risk profile assessed based on cyber risk. Number 5 in the spider chart radial axis corresponds with high risk and number 1 with low risk.

6.2 Albania country specific risks

The Republic of Albania has recognized multiple threats and risks to national security in its National Security Strategy 2014. They are categorized in three different levels on the basis of likelihood of occurrence and possible consequences. Albania recognized corruption and organized crime, cyber-attacks by state and non-state actors as 1st level threats, with high likelihood and high impact, as well as possible terrorist attacks, religious radicalism, military conflicts and armed tensions under 2nd level, and espionage activities in the 3rd level, which could be a precursor or trigger for manifestation of cyber threats and risks. The National Security Strategy 2014 recognized the importance of ICT and computerization, its effect on economy and society, but it mentioned that the risk posed by cyberattacks have the possibility to severely damage the operations of state and critical infrastructure and cause breakdown of vital services.

Although the National Policy Paper on Cybersecurity (2015-2017) does not incorporate risk assessment nor does the legislative system demand such actions to be carried out, the paper does express types of criminal offences committed in years 2013 and 2014 and statistics connected with them which could be understood as cyber-risks and threats. Such threats and risks are defined in the NAECCS regulation on Cyber incidents and the format & elements of reporting, setting a standardized template for reporting of incidents.

The military recognized two threats in its Strategy for Cyber Defence. First is identified as cyber incidents dealing with cyber-attacks on critical and important information-communication systems for the purpose of sabotaging the operations of such systems. Second is identified as espionage activities with the purpose of acquiring access to information and data to read, add, manipulate or to deny availability.

Based on stated risks we modified the likelihood and impact for inherent risks (visible and overlapped blue part of the chart) and formed a chart related to country specific risks (coloured grey on the chart) in Albania. The control gaps from country overview were also taken into consideration when assessing scenarios.

As we see on the chart the country specific risks are larger than those inherent risks of the energy sector which is due to constant high-level threat vectors, with high likelihood and high impact (cyberwarfare, cyberespionage and cyber-attacks). This risk level combined with low level of controls by EU standards which is often mixed with non-proper segregation of duties makes Albania a high-risk country regarding cybersecurity in the energy sector with huge potential of inducing a cascading effect not only to neighbours but also to other EU member states and/or EnC CPs.
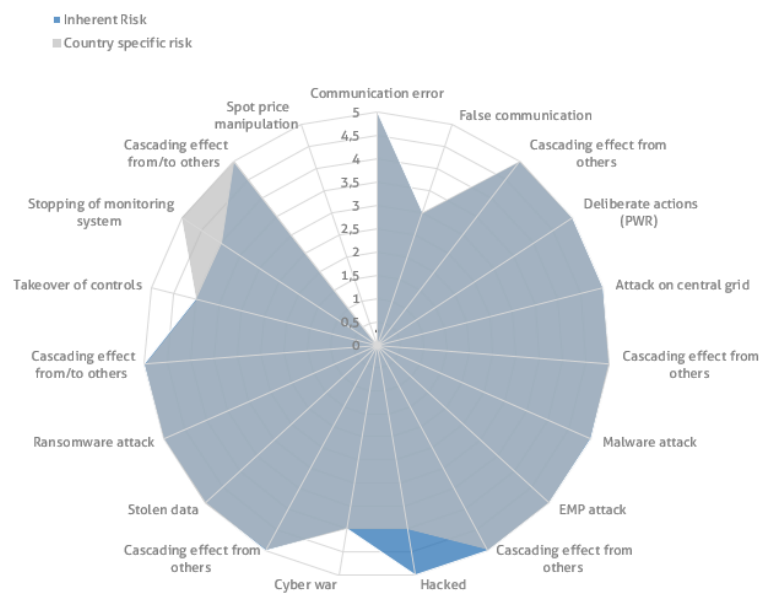
Figure 16: Albania risk profile

6.3 Bosnia and Herzegovina country specific risks

Security challenges in National Security Strategy (Defence White Paper of Bosnia and Herzegovina 2005) are characterized in 3 levels: global, regional and internal.

Global level threats are international terrorism and organized crime with their use of ICT and are also addressed in strategies as potential threats to critical infrastructure.

Regional level threats are attempts for secession, autonomy and independence by certain ethnic groups in combination with past events and military capabilities which could trigger conflicts in the region.

Internal level represents political and social tensions from past political and armed conflict supported by nationalistic tensions and extremism.
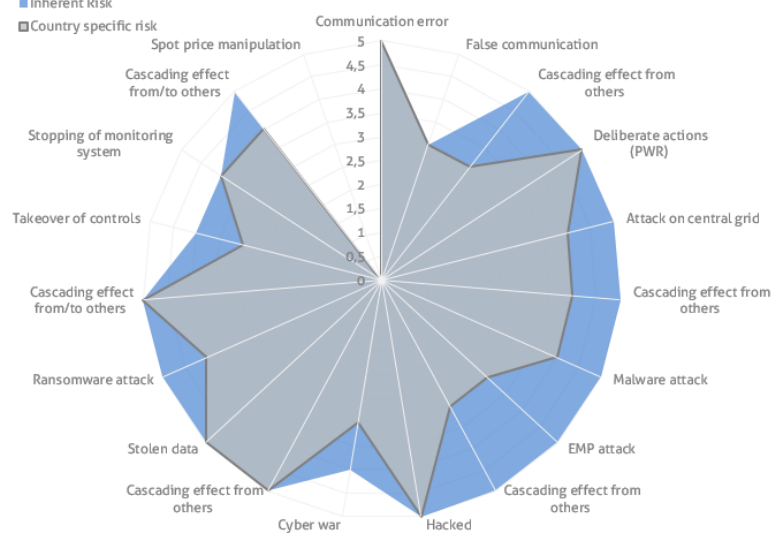
Figure 17: Bosnia and Herzegovina risk profile

Based on stated risks and publicly available data we modified the likelihood and impact for inherent risks to form a chart related to country specific risks (coloured in grey on the chart) in Bosnia and Herzegovina. The control gap from country overview was also taken into consideration when assessing scenarios.

It is important to note that there had been a stress test was made in 2014 by the Energy Community and European Commission on the short-term resilience of the EU Member States and EnC CPs gas sector. For purpose of that analysis a scenario has been developed for assessment of supply disruption, but the analysis did not include the cyber-security perspective. On the page 6 of the document there is a conclusion that "In the cooperative scenario the effects of the disruption are significantly dampened in those EU Member States and Energy Community Contracting Parties most affected and most particularly Bulgaria, Estonia, Bosnia and Herzegovina, the former Yugoslav Republic of Macedonia and Serbia". Our analysis shows that in a case of cyber-attack from the same reasons stated in the document (absence of

full cooperation of BandH entities on cybersecurity matters in energy sector) the country risk is higher than of those stated countries that started cooperation measures with their neighbours.

On the chart some country specific risks are reaching or are bigger of inherent risks of overall energy sector which is due to segregated energy environment, usage of legacy systems and low level of controls by EU standards. As the energy sector in Bosnia and Herzegovina is pretty much divided in three parts, during the assessment we needed to assess the country risks keeping this fact in mind. On the other hand, this segregated environment is also in some cases positive as the cascading effects may be stopped on gateways of those segregated systems. For the government it will be a hard imperative to manage the risks as a whole and implement regulation on every energy subject.

6.4 Georgia country specific risks

Georgia has developed its National Security Concept where it defines threats and risks to the national security. Out of described risks multiple could lead to manifestation of cyber incidents, namely: Escalation of tension between Georgia and Russian Federation; The risk of renewed military aggression; Conflicts in the Caucasus; International terrorism and transnational organized crime; Cyber threats.

Cyber-war encompasses possibility of recurrent risk of massive cyberattack supported with disinformation campaign with cyber-means to influence the population of Georgia. With the enhanced capabilities and sophistication of the threat actor as well as digitalization of Georgia, the threat poses greater risk than during war in 2008.
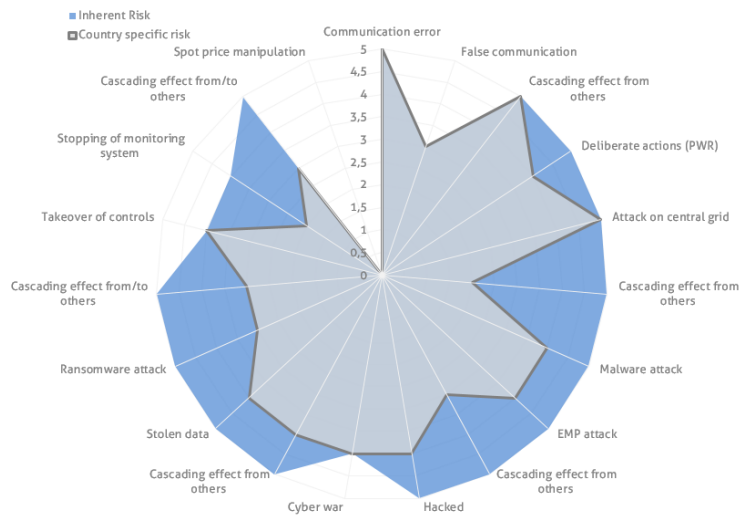
Figure 18: Georgia risk profile

Cyber-terrorism includes use of cyberattacks by a terrorist organization or state sponsored actor against critical or public infrastructure as well as enablement of terrorist acts with the use of ICT. Cyber-intelligence activities comprise of all activities by state intelligence agencies in the process of collection of classified, secret or closed information with the use of ICT. Other activities directed against Georgia in cyber-space covers threats against critical and/or public information systems that are providing critical service to Georgia and lower level acts of denial of access to information or proper operation ICT as well as cybercrime.

Based on stated risks we modified the likelihood and impact for inherent risks to form a chart related to country specific risks (coloured in grey on the chart) in Georgia. The control gaps from country overview was also taken into consideration when assessing scenarios.

Georgia is a country under a constant potential cyberattack and the cyberwar is a recurrent risk to be considered. Keeping this in mind Georgia started to develop its cyber defence which does lower some country risks and is also cooperating actively with others (NATO). This brings us to results of our chart which shows that the country risks are often started to be managed but inherent risks are to be considered also with implementing of controls which are in EU obligatory. The ISO27000 standard used in some cases is now just a framework, making it obligatory would put up new risk management possibilities to energy sector stakeholders.

6.5 Kosovo* country specific risks

Kosovo* recognizes multiple security challenges and threats to its sovereignty in its Strategic Security Sector Review (2012). They are categorized in 3 security environments: global, regional and internal. Among those are threats which could materialize in cyber space. In global security environment such threats pose terrorist activities, transnational and organized crime as well as cybercrime. In regional security environment such threats pose regional political instabilities, ethnic and religious extremism and organized crime. Internally such threats pose ethnic and religious extremism, organized crime, contested/undetermined border and cybercrime.

Kosovo* recognizes multiple threats to ICT in the National Cyber Security Strategy 2016-2019, defining them on the basis of skills and motivation for cyber-attacks. Among mentioned are cyber-attacks carried out of curiosity or revenge by insiders or less skilled attackers, for monetary gain by organized crime, for espionage by foreign intelligence services, activism by politically or socially motivated groups, for purposes of terrorism by terrorist or cyber terrorist groups and for national security by foreign state-sponsored actors. Kosovo* expresses and outlines risks against CI as such infrastructure is becoming targeted more frequently and by more complex cyber-attacks.

Based on stated risks we modified the likelihood and impact for inherent risks to form a chart related to country specific risks (coloured in grey on the chart) in Kosovo*. The control gaps from country overview were also taken into consideration when assessing scenarios. During the assessment of the risks Kosovo* was looking as a promising country but mostly promising for those who plan to attack others with cascading effect. They made a plethora of strategic documents none of them still operationally implemented in legal framework nor are they on any level obligatory for their stakeholders. If we keep this in mind during the analysis of their chart, we can recognize the pattern that the country risks are based on the facts that they mostly depend on domestic power generation but are very susceptible to cascading effect because of lack of cyber controls in energy sector. For Kosovo* it is very important to operationally start to handle the risks (country risks and inherent risks as well) as they are threat not only for them but also for the other EnC CPs and EU Member States as well.
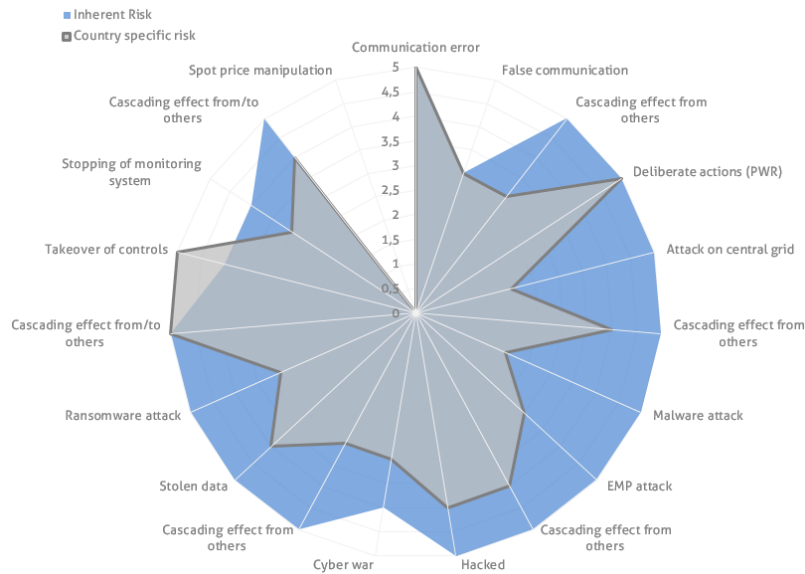
Figure 19: Kosovo* risk profile

6.6 Moldova country specific risks

Republic of Moldova recognizes multiple threats and vulnerabilities to its sovereignty in the National Security Concept 2005 and National Defence Strategy 2018 that could be a trigger for manifestation of cyber incidents and attacks. As threats and risks to national security Moldova defines Transnistrian conflict and internal separatist tensions, foreign coercion and propaganda, organized crime, hybrid security threats, international terrorism and information-communication technology threats.

Information-communication technology threats are described in the Digital Moldova 2020 as: threat of cyber-attacks against important and critical infrastructure and services, unauthorized access to cyber infrastructure, manipulation and deletion of data, cyber espionage, loss of property through harassment and/or blackmail of individuals and legal entities of public and private sector.

Information Security Strategy 2019-2024 of Moldova recognizes hybrid security threats as well, describing them as cybercrime, espionage, influence activities and propaganda, diversion and exploitation of data for political purposes. Among above mentioned threats and risks Moldova understands the importance of ICT and possibilities of abuse which would lead to unfair competition, confrontation and espionage, terrorism and crime, privacy violations, misinformation and spreading of hatred as well as inciting violence with the use of modern technology.

Moldova recognizes the progressive expansion of ICT in the affairs of the state as well as in defence system and understands the importance of cybersecurity for protection of vital information infrastructure, services and networks. Moldova understands that the process of protecting CI is not limited to defence, economy and energy sector only but to others as well.
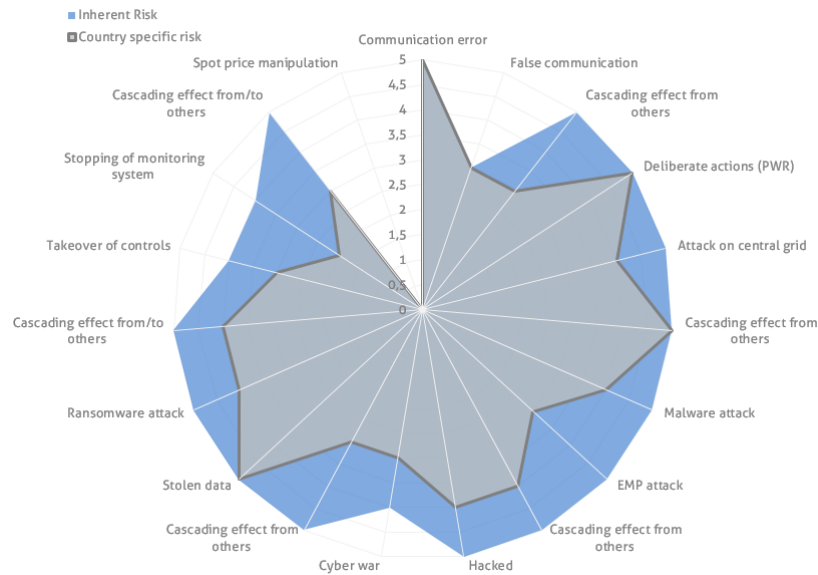
Figure 20: Moldova risk profile

Based on stated risks we modified the likelihood and impact for inherent risks to form a chart related to country specific risks (coloured in grey on the chart) in Moldova. The control gaps from country overview was also taken into consideration when assessing scenarios.

Moldova has been working on risk management already as shown on charts so we see a lot of difference between country and inherent risks. We took into consideration country's active cooperation with NATO also. However, there is lot to be done not only on legislative level but also on operational implementation of controls equal of those in EU.

6.7 Montenegro country specific risks

Republic of Montenegro has adopted Strategy of National Security of Montenegro in 2008. Strategy recognizes multiple threats and risks to Montenegrin sovereignty and national security that could be a trigger for manifestation of cyber-attacks and incidents.

Strategy recognizes threats connected to regional instability connected with past experience and events, crises and conflicts in the region, terrorism, organized crime and information-communication technology related threats because of ever growing computerisation of society. Strategy recognizes that digitalization and increased use of ICT creates new vulnerabilities and threats to vital and essential systems and infrastructure, degradation of functions of which would cause serious damage and disruption to state, public and private organizations.

With adoption of Cyber Security Strategy of Montenegro 2018-2021, Montenegro identifies hacktivism, espionage, sabotage, cyber and organized crime, cyber terrorism and cyberwarfare as threats to the security of network and information systems through use of cyber-attacks and other information security related incidents.
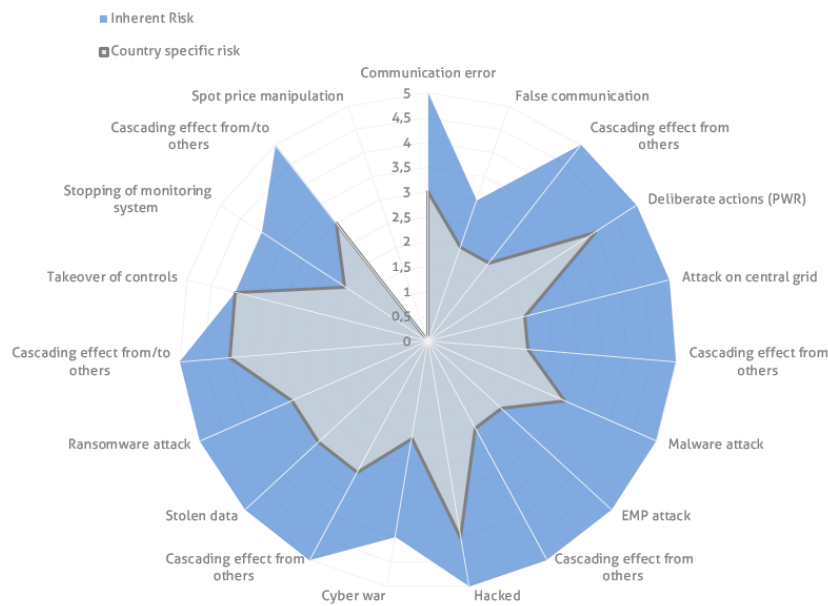
Figure 21: Montenegro risk profile

Montenegro recognizes that the numbers of cyber incidents are on the rise and are getting more sophisticated. Among above mentioned threats, the Strategy recognizes the threats and risks connected to unpredictability of natural and human made disasters as well as risks caused by human error in use of information-communication technology as well as human malicious actions in the organization – insider threat.
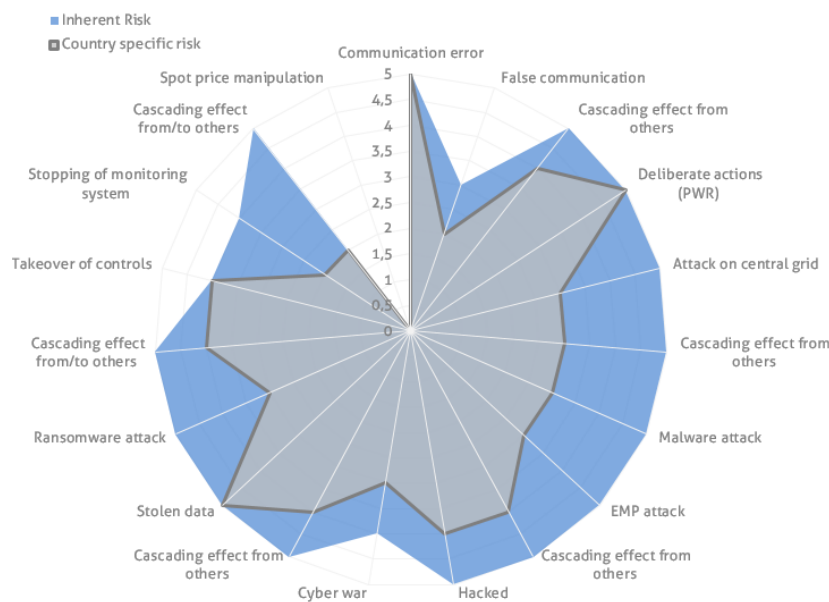
Based on stated risks we modified the likelihood and impact for inherent risks to form a chart related to country specific risks (coloured in grey on the chart) in Montenegro. The control gaps from country overview was also taken into consideration when assessing scenarios.

If we analyse the country risks on the chart, we recognize significantly lower risks than of inherent risks thanks to ISO 27000 implementation and active cyber resilience during 2018/2019. Nevertheless, as an interconnected country Montenegro must pay attention in forthcoming period to inherent risks especially the cascading ones because country's interdependencies with others will significantly grow after finishing the strategic investments in energy sector.

6.8 North Macedonia country specific risks

Republic of North Macedonia recognizes multiple threats and risks to its sovereignty in the Strategic Defence Review 2018[146] that could be a trigger for manifestation of cyber incidents and attacks. As threats and risks to its sovereignty North Macedonia defines: organized crime, hostile foreign intelligence services, violent extremism and radicalism, terrorism, cyber-attacks and risks to information security. It is

---

[146] http://morm.gov.mk/wp-content/uploads/2018/07/SDR-Paper-dated-05-July-2018.pdf

important to note, that Republic of Macedonia assessed the likelihood of threat of cyber-attacks and risks to information security for medium and long term, up to 10 years, is assessed high and medium in the short term.

In the National Cyber Security Strategy 2018-2022 Republic of North Macedonia recognized the risks of cybercrime, threats and risks relating to the use of social media and personal data, vulnerabilities and malicious software as well as compromised hardware and software, ransomware, threats against critical and important information infrastructure, threat of botnets and distributed denial of service attacks, cyber espionage and malicious crypto currency mining. Threats to critical information infrastructure and critical industrial control systems are defined in detail by sectors among which is energy sector as well. North Macedonia recognizes the need for protection of critical infrastructure, as it understands the possibility of destruction or dysfunctionality of such infrastructure could bear fatal consequences or cause extensive physical or monetary damage.

Figure 22: North Macedonia risk profile

Based on stated risks we modified the likelihood and impact for inherent risks to form a chart related to country specific risks (coloured in grey on the chart) in North Macedonia. Control gaps from country overview were also taken into consideration when assessing scenarios.

It is taken into notice that the country actively cooperates with ENTSO-E and NATO, but on the chart we still have a huge dose of country risk which is mainly a result of underdeveloped cybersecurity defence infrastructure of the government. Those risks will be managed if the existing strategic documents are to be fulfilled on operational level. There are also a not addressed inherent risks to be managed for North Macedonia.

6.9 Republic of Serbia country specific risks

The Republic of Serbia recognizes multiple threats and risks to its sovereignty in its National Security Strategy from 2009. Recognized threats could be a trigger for manifestation of cyber incidents and attacks. Serbia divides threats in three categories namely: global- and regional environment, as well as the security of the Republic of Serbia.

In the global environment Serbia recognizes threats of regional or local conflicts, ethnic and religious extremism, terrorism and organized crime. On the regional level Serbia recognizes threats of armed conflicts in South Eastern Europe, separatist aspirations in the region, terrorism, organized crime, national, religious and political extremism. In the security environment of the Republic of Serbia, it recognizes secession tensions, organized crime, terrorism, armed rebellion, national and religious extremism, espionage, financial and high tech-crime connected to cybercrime and threats to telecommunication systems.
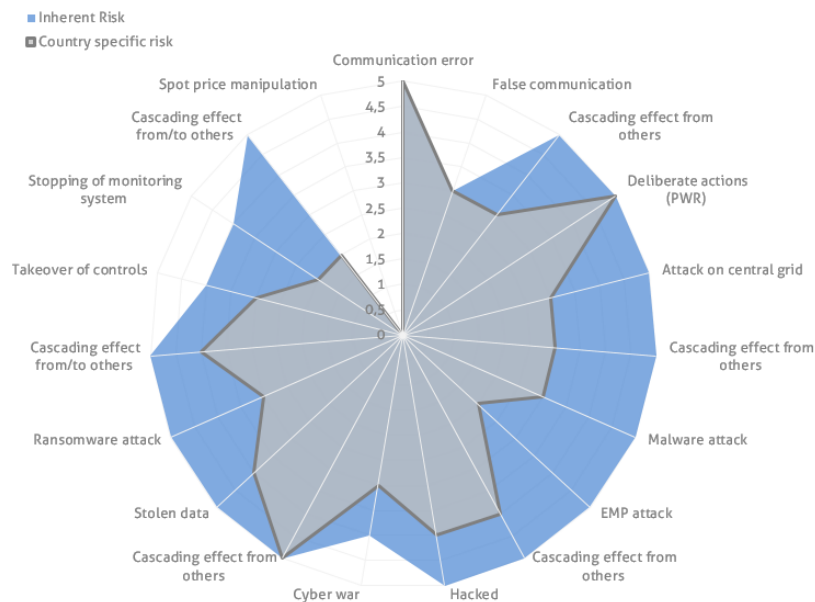
Figure 23: Serbia risk profile

Serbia recognizes high-tech crime as one of threats to its sovereignty and national security. The notion of high-tech crimes is developed in detail in the national cybersecurity strategy. The adopted Strategy for Development of Information Security in the Republic of Serbia 2017-2020 recognizes threats of cybercrime, abuse of ICT for purposes of violating security of individuals, threats to state, business or organization ICT infrastructure and threats to national security through information technology.

It is important to note that the Strategy for combating high-tech crime 2019-2023 goes into more detail explaining the risks and threats posed by the abuse of ICT and cyber criminals, naming cyber-attacks, malware, scams, cybercrime-terrorism nexus as well as crimes facilitated with use of ICT, explicitly naming fraud as well as recording and sharing of child pornography.

Based on stated risks we modified the likelihood and impact for inherent risks to form a chart related to country specific risks (coloured in grey on the chart) in Serbia. The control gaps from the country overview were also taken into consideration when assessing scenarios.

During the last couple of years Serbia implemented laws and regulations on CI and cyber. Those established an organisational level defence against cyber threats. However, we still see numerous country level risks which all refer to the lack of the energy sectorial specific cyber defence architecture. To manage those threats Serbia needs to address not only internal risks but also the risks coming through cascading effects from the neighbours. The inherent risks are also to be actively managed.

6.10 Ukraine country specific risks

National Security and Defence Council of Ukraine adopted Strategy of National Security of Ukraine[147] in 2015 following escalation of tensions with Russian Federation. Ukraine recognizes multiple threats and risks to its sovereignty and national security, among which are threats that could be a trigger for manifestation of cyber incidents and attacks. National Security Strategy defines conflict with neighbouring country, threats to information and cybersecurity and security of information resources as well as threats to critical infrastructure. Among those mentioned above Ukraine recognizes the threat of "hybrid" war in its Doctrine of Information Security of Ukraine[148] as well.

One of the threats described in the Strategy of National Security of Ukraine are threats to information and cybersecurity as well as against security of information resources. Ukraine understands the ever-growing need and dependence on ICT and the threats that emerge from its use. Cyber Security Strategy[149] lists cyber-terror attacks, cyber espionage, cybercrime and cyber war and defines such threats and risks in more detail.

It is important to note, that Ukraine recognizes the threat of cyberattacks against critical infrastructure following major sophisticated cyber-attacks against energy sector and began implementing necessary legislative provisions pertaining to addressing the risks and threats as well as creating capabilities for defence and security, which were not envisioned in the Strategy of National Security of Ukraine.

Based on stated risks we modified the likelihood and impact for inherent risks to form a chart related to country specific risks (coloured in red on the chart) in Ukraine. The control gaps from country overview was also taken into consideration when assessing scenarios.

---

[147] *Strategy of National Security of Ukraine. https://zakon.rada.gov.ua/laws/show/287/2015*

[148] *Doctrine of Information Security of Ukraine. https://zakon.rada.gov.ua/laws/show/47/2017*

[149] *Cyber Security Strategy. https://ccdcoe.org/uploads/2018/10/NationalCyberSecurityStrategy_Ukraine.pdf*
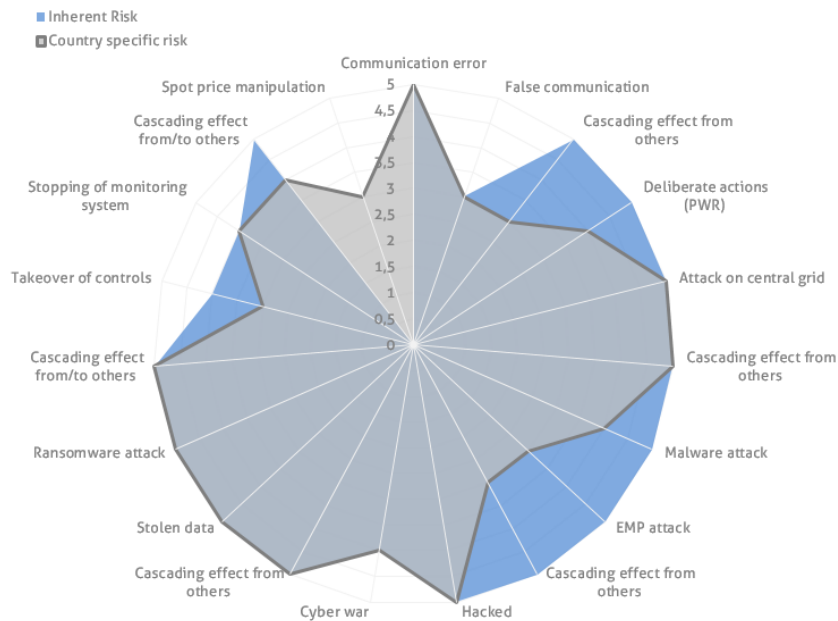
Figure 24: Ukraine risk profile

The country is under constant cyberattack so during the assessment this appeared in likelihood and impact estimation. Although Ukraine implemented very strong cybersecurity measures on operational level and introduced a cooperation with EU and NATO, there is still a high probability of cyberattacks due to the geopolitical conflict. The overall improvement of cyber resilience is noticed but must be further on constant level.

6.11 Conclusion on country specific risks

Generally, we can conclude that EnC CPs have different levels of risks which is mostly induced by geopolitical situation.

In the first group of countries we can put Western Balkans EnC CPs (Albania, Bosnia and Herzegovina, Kosovo*, Republic of Serbia, Montenegro and North Macedonia) which all have by EU standards smaller sized energy markets and are coping with similar if not the same cybersecurity issues (risks, incidents). In this group by cybersecurity maturity level the two most advanced countries (Serbia and Montenegro) may contribute lot to the region overall cybersecurity level
by cooperating actively with their neighbours. That would lower the risk of the whole group. If regional cooperation is somehow more deepened with cooperating energy CSIRTs and joint exercises and early warning system, we believe this will put risks on much acceptable levels.

The second group with higher risk levels members are Georgia and Moldova which are practically under constant risk of cyber-war type of incidents. Those two countries need more investment in high tech cyber defence and must engage very skilled professionals to have some kind of progress in managing cyber risks not to forget active cooperation on cyber issues with friendly neighbours and cyber capability defence of NATO.

And in the third group is Ukraine which is a risk assessment story for itself as being in state of hybrid war not only in cyberspace but for real. Ukrainian energy market is huge amongst other EnC CPs and of large strategic interest not only for EU but USA and Russia as well. As Ukraine's cyber risks are of critical levels the country is managing them pretty fast and in their best knowledge. Nevertheless, all neighbouring countries must be aware of those risks during any kind of cooperation in energy sector and must adjust their respective systems/processes to be able to handle the same level of risks (this includes EnC also).

For all EnC CPs is imperative closing the gaps in regulatory discussed in "*Chapter 5* Overview, assessment and gaps of cybersecurity related institutional and legal frameworks in the energy sector of Contracting Partiesof the document. Before this is done the overall country risks will remain just the same.

6.12 Cyber risk scenarios

Chapter gives detailed descriptions of cyber risk scenarios, which have been used to conduct the risk analysis, structured by specific stakeholders group as defined in *"Table 13: List of used combinations of stakeholders and cyber risk scenarios"*. Beside each scenario, detailed description of Vulnerabilities, Likelihood and Quantified impact on energy sector is given.

6.12.1 Stakeholder: Country cybersecurity authority (CA) and/or National Regulatory Agency (NRA)

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.

Threat	Vulnerability	Likelihood	Quantified Impact on Energy Sector		
			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				

Scenario 2 – False communication			CA/NRA

An attacker was able to penetrate the Virtual Private Network (VPN) of the CA and using IP address and email spoofing techniques was able to send an email that triggered an emergency condition that consequently forced the energy sector companies to start operating according to the procedures enforced in cases of critical conditions. As a result of a 24-hours-a-day shift was introduced at gas TSO critical supervisory operation control room unit. The reporting requirement was upgraded to once a minute. The triggering of a false emergency condition by the attacker forced the government, according to the national emergency plan for energy, to hold a special meeting to discuss the cyberattack. The government releases a special note to inform the public about the incident. After the internal investigation of the incident by CA and the realisation that the emergency condition was triggered by a spoofed email address containing false information, CA unsuccessfully tries to revert the situation, but the notice has already been published with the related consequences for the society and the economy.

Threat	Vulnerability	Likelihood	Quantified Impact on Energy Sector		
			Health/Safety	Economic	Social
Phishing	Lack of security awareness	Probably	1	2	2
	Lack of proof of sending or receiving a message				
	Unprotected sensitive traffic				
	Lack of e-mail usage policy				

Scenario 3 - Cascading effect from others						CA/NRA

Cascading effect scenarios are with scenarios 1 or 2 evaluated for vendors, suppliers or third-party service personal of CA/NRA.

Threat	Vulnerability	Likelihood	Quantified Impact on Energy Sector		
			Health/Safety	Economic	Social
Cyberwarfare	Lack of procedures of risk identification and assessment	Possibly	1	4	2
	Lack of monitoring mechanisms				
	Inadequate recruitment procedures				

6.12.2 Stakeholder: Country Transmission System Operators (TSO) Electricity

Scenario1 – Administrator's revenge

A former employee of the TSO uses his access card to enter the control room. Since his access rights and privileges, both related to computer systems and physical access, were not removed when the employee left the TSO, he is able to enter the control room and install a malicious software that deletes all databases and their backups of the SCADA system. Since the TSO does not have backup in other physical media stored in a secure place, it is not possible for the SCADA system to be recovered and the TSO to return to normal operation. The SCADA system needs to be re-installed and commissioned on a new server, a procedure that causes significant problems in managing the transmission network for seven (7) days causing a number of power outages ranging from two (2) minutes to six (6) hours.

Threat	Vulnerability	Likelihood	Quantified Impact on Energy Sector		
			Health/Safety	Economic	Social
Insider threat	Inadequate or careless use of physical access control to buildings and rooms	Probably	4	5	4
	Lack of identification and authentication mechanisms, e.g. user authentication				
	Lack of continuity plans				

Scenario 2 – Attack on central grid

A cyberwarfare group has managed to penetrate the VPN of the TSO. By takes advantage of a zero-day exploit, the group manages to get access to the servers hosting the OT systems of the TSO and deletes all OT systems that are installed on the affected servers, thus making them unavailable for the management and operation of the transmission network. Since re-installing and commission the affected OT systems required two (2) weeks, half of the country is without power for 3 days, in some parts the recovery lasts 2 weeks. During that 2 week the army is engaged in restoring civil order.

Threat	Vulnerability	Likelihood	Quantified Impact on Energy Sector		
			Health/Safety	Economic	Social
Social engineering Cyberwarfare Ransomware	Well-known flaws in the software	Possibly	4	4	5
	Unprotected password tables				
	Unnecessary services enabled				
	Lack of back-up copies				
	Insecure network architecture				

Scenario 3 - Cascading effect from others

The national TSO is experiencing a cyberattack that exploits a vulnerability that affects the Inter-Control Center Communications (ICCP) protocol that is commonly used by TSOs and DSOs worldwide. Due to the fact that there is no cross-border communication infrastructure in place for data exchange between TSOs and/or DSOs, a formal early warning monitoring system does not exist. As a result, the attacker is able to also attack neighbouring TSOs that results in affecting the interconnections between the neighbouring countries that soundly affect the cross-border exchange of energy.

| Threat | Vulnerability | Likelihood | Quantified Impact on Energy Sector | | |
			Health/Safety	Economic	Social
Cyberwarfare	Lack of procedures of risk identification and assessment	Possibly	3	4	5
	Lack of monitoring mechanisms				

6.12.3 Stakeholder: Country Transmission System Operators (TSO) Gas

Scenario1 – Malware attack

Due to lack of security policies in the personal computers of the TSO, a user visits a website that takes advantage of the ability to execute JavaScript code at the user's computer and installs a malicious software that exploits a zero-day vulnerability of the host operating system of the SCADA and Energy Management System (EMS) of the TSO, allowing remote access to the said systems by a malicious user. As a result, false indications are shown in the SCADA system and arbitrary control command are sent to the TSO substations and field devices. The commands send by the attacker cause an explosion at a critical infrastructure valve, which result in severe personnel injuries. The fire from the explosion spreads to local facilities and the situation is hard to contain due to the flammable gases. The fire is contained and partially distinguished after 24 hours. As the country's gas supplies in its only underground storage facility are on critical low level and the incident stopped the critical supply delivery there is a widespread shortage of gas for more than a 14 days causing sever political, social, and economical problems.

| Threat | Vulnerability | Likelihood | Quantified Impact on Energy Sector | | |
			Health/Safety	Economic	Social
Malware, Spam Cyberwarfare	Uncontrolled downloading and use of software	Rarely	4	5	5
	Insecure network architecture				
	Lack of procedure of monitoring of information processing facilities				
	Lack of established monitoring mechanisms for security breaches				
	Single point of failure				

Scenario 2 – EMP attack

During an EMP[150] (electromagnetic pulse) attack, protection relays which did not comply with the respective standards and were not immune to Electromagnetic Interference (EMI) were severely damaged. Similar damages were also experienced by the servers hosting the TSO SCADA system that were not properly shielded against EMI. Due to the lack of spare protection relays in the inventory of the TSO, the protection relay vendor can deliver the new relays only thirty (30) after the incident. The process of resorting the TSO SCADA systems involved the installation of a clean SCADA system and its commissioning, followed by the restoration of the databases backups. This process lasts seven (7) days. For fifteen (15) days the gas transmission is halted, after that period the TSO transfers to manual handling. On the arrival of the new protection relays, the TSO realises that is missing the commissioning manuals. Therefore, it asks the protection relay vendor to urgently provide assistance in commissioning the protection relays. The system is again operational only after sixty (60) days.

Threat	Vulnerability	Likelihood	Quantified Impact on Energy Sector		
			Health/Safety	Economic	Social
DoS attack	Sensitivity to electromagnetic radiation	Possibly	2	3	5
	Lack of periodic replacement schemes				
	Lack of documentation				
	Lack of back-up copies				
	Single point of failure				
	Lack of procedures of risk identification and assessment				

Scenario 3 - Cascading effect from others

The wide-area power outage resulting from an EMP attack affects several sectors, including the gas sector where electricity-powered gas compression stations and the central gas control stations stop to operate, thus interrupting the gas delivery throughout the country.

Threat	Vulnerability	Likelihood	Quantified Impact on Energy Sector		
			Health/Safety	Economic	Social
Cyberwarfare Spam, Malware	Lack of procedures of risk identification and assessment	Possibly	3	4	3
	Lack of monitoring mechanisms				
	Lack of continuity plans				
	Lack of regular management reviews				

6.12.4 Stakeholder: Country Distribution System Operators (DSO) Electricity

Scenario 1 – DSO Hacked

By exploiting a zero-day vulnerability in the hosting operating systems, attackers were able to compromise the IT systems of several DSO in the country. As a result, temporarily power outages were experience by the customers of the DSOs. Getting access to the corporate network was made possible via spear-phishing emails carrying malicious Excel documents with macros to infect computers in the targeted network. The attacker was able to operate remotely controlled circuit breakers and sectionalisers, as well as to attack other DSO infrastructure, such as RTUs, protection relays, etc. Servers' hard disks hosting the IT and OT systems of the DSO were also erased. Moreover, a denial-of-service attack was conducted in parallel that resulted in user not having access to the DSO customer service and related webpages, thus having no information on the size, the severity, and the estimated recovery time for the power outage. In total, up to 73 MWh of electricity was not supplied. The complete recovery lasted more than 30 days.

---

[150] The EMP attack is more probable to cause severe damage in gas TSOs as the electricity sector is usually more aware of electromagnetic risks and more prepared for mitigation of those risks.

Threat	Vulnerability	Likelihood	Quantified Impact on Energy Sector		
			Health/Safety	Economic	Social
Social engineering Phishing, DoS Cyber warfare Malware	No or insufficient software testing	Possibly	3	3	4
	Uncontrolled downloading and use of software				
	Lack of identification and authentication of sender and receiver				
	Unnecessary services enabled				
	Lack of continuity plans				
	Insufficient security training				
	Lack of e-mail usage policy				
	Inadequate network management (resilience of routing)				
	Insecure network architecture				

Scenario 2 – Cyber war

A cyberwarfare group is attacking the public ICT infrastructure of the country using denial-of-service attacks, as well as spear-phishing emails carrying malicious Excel documents with macros to infect computers in the public sector networks, as well as targeting the IT and OT systems of the DSO. As a result, public sector ICT infrastructure, including telecommunication operators, and the DSO SCADA and DMS systems were compromised by the attackers. By installing "trojan horse" viruses and password key loggers, were able to gain administrator access to the various sensitive systems of the DSO. The attack to the substation of the DSO and the remotely connected devices was initiated only after 60 days. During that period, the attackers had access to the DSO systems suing the backdoors opened by the "trojan horse" viruses. Due to attack and the compromise of the IT and OT systems, the customers of the DSO experienced sudden power outages. A total of 8,000 customers were impacted by the power outages.

Threat	Vulnerability	Likelihood	Quantified Impact on Energy Sector		
			Health/Safety	Economic	Social
Social engineering Cyberwarfare Phishing, Botnet	Lack of policies for the correct use of telecommunications media and messaging	Possibly	2	3	2
	Unprotected password tables				
	Unnecessary services enabled				
	Lack of e-mail usage policy				
	Lack of back-up copies				
	Insecure network architecture				

Scenario 3 - Cascading effect from others

Since in scenarios 1 and 2 the vast majority of the national and DSO-specific ICT systems were compromised and considering the cross-border interconnections between the regional TSOs, as well as the fact that the in scenario 2 the attack was not executes, and thus not identified, for a period of 60 days, the attack is propagated to neighbouring countries.

Threat	Vulnerability	Likelihood	Quantified Impact on Energy Sector		
			Health/Safety	Economic	Social
Cyberwarfare	Lack of procedures of risk identification and assessment	Possibly	3	4	4
	Lack of monitoring mechanisms				
	Lack of proper allocation of information security responsibilities				
	Lack of established monitoring mechanisms for security breaches				

6.12.5 Stakeholder: Country Distribution System Operators (DSO) Gas

Scenario1- Stolen data

Due to a malicious attachment contained in an email with spoofed email address that was opened by a DSO employee, as well as due to the lack of security policies applied to the user personal computer ,a "trojan horse" virus was installed in the shared folder of the network storage server that allowed the attacker to have remote access to the various data that were stored in the network storage server. Upon detection of the attack from the national natural gas pipeline DSO, the communication of the ICT infrastructure with the outside world was temporarily suspended, until the malicious software was remover and damage analysis were performed. No gas-related services were interrupted, but the DSO was not able to list the data stolen, since the attacker removed all of its trails from the log files of the various systems.

Threat	Vulnerability	Likelihood	Quantified Impact on Energy Sector		
			Health/Safety	Economic	Social
Social engineering / Cyber espionage / Web based attack	No or insufficient software testing	Almost certainly	2	3	4
	Well-known flaws in the software				
	Incorrect parameter set up				
	Immature or new software				
	Lack of identification and authentication of sender and receiver				
	Insufficient security training				
	Lack of regular audits (supervision)				
	Lack of procedures for reporting security weaknesses				

Scenario 2 – Ransomware attack

Due to a malicious email containing an attached PDF with a link to an archive, disguised as an invoice, all files on the server hosting the local DSO SCADA were encrypted. The recovery of the files was not possible. The process of resorting the DSO SCADA systems involved the installation of a clean SCADA system and its commissioning, followed by the restoration of the databases backups. This process lasted sixty (60) days. During this period the DSO was vulnerable to other types of attacks in their OT infrastructure.

Threat	Vulnerability	Likelihood	Quantified Impact on Energy Sector		
			Health/Safety	Economic	Social
Ransomware	Well-known flaws in the software	Possibly	1	2	4
	No "logout" when leaving the workstation				
	Wrong allocation of access rights				
	Lack of back-up copies				
	Insecure network architecture				

Scenario 3 - Cascading effect from/to others

Since stolen data from scenario 1 contain account credentials for both the VPN connections of the DSO with the national DSO, as well as for cross-border VPN connections this affects neighbouring DSOs and TSOs. Moreover, via the said VPN connections the ransomware expand rapidly and encrypt the systems of interconnected networks resulting in power outages in transmission ranging from two (2) hours to one (1) day.

Threat	Vulnerability	Likelihood	Quantified Impact on Energy Sector		
			Health/Safety	Economic	Social
Ransomware / Malware / Phishing / Cyber espionage	Lack of procedures of risk identification and assessment	Possibly	3	4	4
	Lack of monitoring mechanisms				
	Lack of established monitoring mechanisms for security breaches				

6.12.6 Stakeholder: Country Generation/production

Scenario1 – Takeover of controls

Due to a malicious email containing an attached PDF with a link to an archive, disguised as an invoice, attackers managed to gain access to the SCADA system of the DSO and were able to issue control commands to the various assets of the DSO.

Threat	Vulnerability	Likelihood	Quantified Impact on Energy Sector		
			Health/Safety	Economic	Social
Phishing / Cyber espionage / Social engineering	No or insufficient software testing	Possibly	2	2	3
	Well-known flaws in the software				
	Lack of audit trail				
	Wrong allocation of access rights				
	Lack of identification and authentication of sender and receiver				
	Poor password management				
	Insufficient security training				
	Lack of regular audits (supervision)				
	Lack of procedures for reporting security weaknesses				

Scenario 2 – Stopping of monitoring system

A massive national-wide cyberattack resulted in taking offline one of the country's power plants, forcing the personnel to use manual control. The attackers exploited a zero-day vulnerability and compromised the ICT systems of the telecommunication company that was providing communication services to the power plant. Due to the cyberattack, the website of the power plant which informs the partners of any incident occurring went offline for three (3) days when the communication issues were resolved.

Threat	Vulnerability	Likelihood	Quantified Impact on Energy Sector		
			Health/Safety	Economic	Social
Ransomware / Spam / Cyber warfare	Well-known flaws in the software	Probably	1	3	2
	Lack of identification and authentication mechanisms like user authentication				
	Uncontrolled downloading and use of software				
	Insufficient security training				
	Lack of regular audits (supervision)				

Scenario 3 - Cascading effect from/to others

Threat	Vulnerability	Likelihood	Quantified Impact on Energy Sector		
			Health/Safety	Economic	Social
Ransomware / Malware / Phishing, / Cyber warfare	Lack of procedures of risk identification and assessment	Possibly	2	3	4
	Lack of monitoring mechanisms				
	Lack of established monitoring mechanisms for security breaches				

6.12.7 Stakeholder: Country Energy Exchange

Scenario1- Spot price manipulation

The website of the gas exchange company was hacked and hackers falsified the information of spot prices for three (3) hours. No security of supplies was affected.

Threat	Vulnerability	Likelihood	Quantified Impact on Energy Sector		
			Health/Safety	Economic	Social
Web application attack	No or insufficient software testing	Possibly	1	1	1
	Well-known flaws in the software				
	Wrong allocation of access rights				
	Poor password management				
	Insufficient security training				
	Lack of regular audits (supervision)				

6.13 Criteria for the Identification of Large-scale Cybersecurity Incidents and Crisis

It is important to notice that cybersecurity incidents with impact to the energy sector might easily propagate from one country to another and thus impact not only specific CP but also other EnC CPs as well as Title III-parties and Title IV-parties. Cybersecurity event/incident information sharing and coordinated response on the EnC level is one of key pillars for successful prevention and limitation of damage. A prerequisite for any organisational and procedural approach to large-scale cyber incidents and crisis handling is a definition of criteria for large-scale incidents.

For the purpose of this study we define a large-scale cybersecurity incident as an event on critical energy infrastructure located in CPs that is beyond the ability of the affected CP to mitigate it successfully or that would have a significant impact on at least two out of: EnC CPs, EU Member States or Title III/IV parties. While the decision about the ability to handle internal cybersecurity incidents is in the realm of affected country, cross border impacts criteria should be established to address risks related to underestimation or overestimation of potential impact of specific event.

Criteria for the assessment should in accordance to EU good practice encompass:

- Potential number of fatalities or injuries
- Economic effect
- the impact that incident could have, in terms of degree and duration, on economic and societal activities or public safety

Based on the existence of criteria and thresholds[151] for the assessment of impacts according to above listed impact categories the proposed approach is to base criteria for large-scale cybersecurity incidents on the CPs' risk assessment. Decision if a specific incident is designated large-scale cybersecurity incident is based on the aggregation of CPs' risk assessment based on the criteria laid out in the Table 6: Large-scale cybersecurity incident.

---

[151] *More detailed information per CP can be found in the chapter 3, CP overview subchapter Criteria for CI designation and criteria for significant disruptive effect.*

Number of affected countries / CP 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
Low				

Table 6: Large-scale cybersecurity incident

It should be noted that due to different reasons CPs' impact/risk assessment criteria differs. Accuracy, credibility and acceptability of large-scale cybersecurity incidents and crisis declaration criteria might be further improved based on the following recommendations:

- Sharing of information about impact criteria, which is classified information in some CPs, and incidents with warning structure on EnC level would enable further refinement of criteria defined in the Table 6: Large-scale cybersecurity incident.
- Criteria for impact should not rely only on number of consumers or overall capacity but also on their structure (cross-cutting criteria)
- Grid topology should be taken into the account in the impact assessment (e.g. single points of failure)

6.14 Conclusions on country specific risks

Generally, we can conclude that EnC CPs have different levels of risks which is mostly induced by geo-political situation.

In the first group there are countries of Western Balkan EnC CPs (Albania, Bosnia and Herzegovina, Kosovo*, Republic of Serbia, Montenegro and North Macedonia) which all have by EU standards smaller sized energy markets and are coping with similar if not the same cybersecurity issues (risks, incidents). In this group by cybersecurity maturity level the most advanced countries may contribute lot to the region overall cybersecurity level by cooperating actively with their neighbours. That would lower the risk of the whole group. If regional cooperation is somehow more deepened with cooperating energy CSIRTs and joint exercises and early warning system, we believe this will put risks on much acceptable levels.

The second group with higher risk levels members are Georgia and Moldova which are practically under constant risk of cyber-war type of incidents. Those two countries need more investment in high tech cyber defence and must engage very skilled professionals to have some kind of progress in managing cyber risks not to forget active cooperation on cyber issues with friendly neighbours and cyber capability defence of NATO.

And in the third group is Ukraine which is a risk assessment story for itself as being in state of hybrid war not only in cyberspace but for real. Ukrainian energy market is huge amongst other EnC CPs and of large strategic interest not only for EU but USA and Russia as well. As Ukraine's cyber risks are of critical levels the country is managing them pretty fast and in their best knowledge. Nevertheless, all neighbouring countries must be aware of those risks during any kind of cooperation in energy sector and must adjust their respective systems/processes to be able to handle the same level of risks (this includes EnC also).

For all EnC CPs is imperative closing the gaps in regulatory discussed in "*Chapter 5 Overview, assessment and gaps of cybersecurity related institutional and legal frameworks in the energy sector of Contracting Parties*"

7 Proposed measures, activities and organisational structures

Recommendations laid out in this chapter were developed based on the overview and assessment of gaps in *"Chapter 5 Overview, assessment and gaps of cybersecurity related institutional and legal frameworks in the energy sector of Contracting Parties"* between Contracting Parties legislation and EU wide energy sector cyber security legislation and standards in *"Chapter 4.2 EU legislation overview"* as well as EnC wide and Contracting Parties specific energy sector cyber security risk assessment.

One of the main observations of the study is the lack of provisions related to critical infrastructure identification and consequently gaps in legislative requirements related to operators' security plans and communication and reporting mechanisms. Somewhat more developed is local legislation related to essential services however important gaps were identified also in this area.

Consequently, we propose to adapt and encompass EU cybersecurity legislation into the EnC thus providing the basis to harmonise cybersecurity approach on the level of EnC. Once the amendments are adopted implementation activities can be started on the EnC level and Contracting Parties' level.

Other recommendations on the EnC level encompass:

- Recommendations on the support to Contracting Parties in the implementation of legislative requirements in the form of awareness campaigns, capacity building and training activities.
- Recommendations related to more operational activities, encompassing sharing and coordination of essential cybersecurity information and activities between Contracting parties, including contact points, ISAK and CIRTs.
- Recommendations about cyber security certification framework and harmonisation of Contracting Parties' cyber security standards with EU wide standards and good practice.

General Recommendations on the CP level address gaps identified in the majority of Contracting Parties and encompass recommendations on organisational structures, reporting and further alignment with foreseen changes of EnC acquis. In addition to CPs general recommendations, Contracting Parties specific recommendations were developed addressing CPs' gaps and risks, consequently the extent of these recommendations can vary between CPs.

It should be stressed that energy sector stakeholders are aware of cybersecurity risks and are implementing security measures. However only a harmonised and balanced approach at the EnC level can effectively address cross border cyber security risks and contributes to the operational efficiency of energy sector stakeholders'' cybersecurity efforts.

7.1 Energy Community

Following the general recommendation regarding adaptation of NIS and ECU directives to EnC CPs the chapter introduces recommendations on the EnC level in following structure:

- EnC level framework.
- Operational cooperation mechanism.
- Certification schemes and procedures.
- Awareness and training.

7.1.1 Recommendations for the EnC level framework

General recommendation is to adapt NIS and ECI directives to the EnC stakeholders and adopt them as a part of the EnC acquis (beyond PROCEDURAL ACT OF THE MINISTERIAL COUNCIL OF THE ENERGY COMMUNITY, 2018/2/MC-EnC: on the Establishment of an Energy Community Coordination Group for Cyber-Security and Critical Infrastructure A).

Regarding the further development of EnC cybersecurity organisational structure is recommended including segregation of cooperation levels to subgroups and thus foster successful and secure exchange of information on different levels:

- The organisational, IT and other infrastructure capabilities of Energy Community Cyber CG established in November 2018 should ensure adequate protection of information because some of the data handled during group operation could come from EnC CP labelled EU restricted up to EU confidential. Within this subject we propose to have segregated Cyber CG secretariat also.

- On the top of the Cyber CG organisation should be the **Cyber CG Action Group** (Cyber CGAG) with EnC CP responsible National Ministries representatives (from ministries designated as CI competent authorities) as members. Since "all cybersecurity initiatives are destined to fail without support from leadership", the Cyber CGAG main purpose is to give the cooperation framework the much-needed leadership and involvement in key decisions. The Cyber CGAG would be also responsible for any arbitrary issue of the operational level.

- To establish NRA coordination group for cybersecurity and critical infrastructure in energy sector, EnC **Cyber CG NRA Working Stream** between the respective specialized EU agencies and bodies (such as Eurojust, Europol's European Cyber Crime Centre, European Network and Information Security Agency - ENISA[152]) and EnC Contracting Parties NRAs for exchange of information about potential threats regarding energy sector stakeholders.

- To establish a fully operational TSO working stream for cybersecurity and critical infrastructure for cooperation in energy sector between the EnC CPs TSOs (e.g. **EnC Cyber CG TSO Working Stream**) for exchange of information about potential threats/vulnerabilities as well as cooperation on cybersecurity issues regarding energy sector participants. The Cyber CG TSO Working Stream should be partly segregated to electricity and gas. This cybersecurity body's goal is to establish active cooperation with ENISA, ENTSO-E and ENTSO-G and should have the capability to transfer information about potential threats/incidents regarding energy sector participants to their members which don't take regularly part in ENISA, ENTSO-E and ENTSO-G activities.

---

[152] *A further developed operational results based on existing initiatives https://www.enisa.europa.eu/news/enisa-news/enisa-meets-energy-community*

- To establish E-CSIRT working group related to CSIRT/CERT Network by seeking contacts with national CERTs/CSIRTs. This function should serve as a medium of exchange between EnC CPs on CSIRT/CERT level (after signing respective MoUs). For this purpose, Enc should provide not only technical support in the form of data exchange platform but also energy expert resources to verify the incoming data. We strongly suggest that EnC establish EnC CPs E-CSIRT working group and provide sufficient budgetary and human resource support. This new cyber organisation within EnC primary duties would be:
  - Establish official contacts with ENISA in order to exchange relevant data regarding energy sector.
  - Organize EnC CPs level joint cybersecurity exercises.
  - organize EnC CPs level joint cybersecurity awareness activities and education platform
  - Assist EnC CPs to set up and implement certification schemes for general processes, special energy sector-based processes, risk management processes, system security, human resource (cybersecurity auditors, chief information security officers, etc).
  - Operate an information sharing and analysis platform for energy companies/organisations (DSOs, power generation, small businesses etc.)

- To establish an information sharing and analysis centre for energy sector (eg. **EnC CP E-ISAC**), which will support energy companies/organisations from EnC CPs (DSOs, SMBs, institutions etc.). E-ISAC would help energy companies to improve the cyber security and resilience of their grid by enabling trust-based data and information sharing. ISACs are public private partnerships in which participants exchange experiences and information about incidents and attacks within their own organization in order to protect the industry as a whole an is able to set up lasting relationships of trust with partners across the entire value chain. Such CPs specific ISAC for energy sector should cooperate with EE-ISAC and other ISACs for energy sector from EU Member States and other EnC CPs. on any mutual cybersecurity issue.

As a provision of existing acts an early warning communication system should be established between Energy Community Contracting Party's (NRAs, TSOs) and EnC cybersecurity body to have a capability to inform EU organizations in a case of critical impact incidents with cross-border. On a conceptual level, a successful cyberattack early warning system would require several facets, including:

- A methodology for near real-time monitoring of the IT/OT infrastructure.
- Ability to recognize, collect and profile system anomalies to identify potential threats and/or attacks.
- The capability to pass immediately the information about the incident to all relevant parties.

The EnC CP NRAs should develop capabilities to understand the issues, transfer the information (to local CA and/or Govt) and participate in the operational and legal decisions on EnC level about potential threats/incidents regarding energy sector stakeholders (e.g TSO, DSO), especially regarding energy CI protection. As NRAs in Contracting Parties lack should improve those capabilities we recommend EnC to provide training to develop these capabilities and thus empower

Such established Cyber CGNRA Working Stream would handle issues of:

- Providing EnC CPs high level cooperation in changing local cybersecurity in energy legislative in the field of requirements for EnC CII, NIS, education, awareness and certification
- Providing EnC CPs high level cooperation in EnC E-CSIRT and enforcing cooperation of EnC CP energy CSIRTs
- Providing EnC CPs high level cooperation in EnC E-ISAC enforcing cooperation of EnC CP E-ISACs
- Providing EnC CPs high level cooperation in organising EnC level cybersecurity training activities

- Providing EnC CPs high level cooperation in organising EnC level cybersecurity awareness activities
- Providing EnC CPs high level cooperation in organising EnC level coordination in application of technical standards on cybersecurity (ISO 27K, ISO 31000)
- Providing EnC CPs high level cooperation in organising EnC level coordination in certification of technology (accreditation and standardization)

7.1.2 Recommendations regarding the development of proposed operational cooperation mechanism on the EnC level

When developing cooperation mechanism one should have in mind that trust is one of the key factors in successful and effective cooperation in a field of cybersecurity. Following recommendations that should be taken into the account during the implementation of organisational structures proposed in a previous chapter are based on energy sector specific good practice[153]:

- Trust is a key component of information sharing.
- Participants in information sharing initiatives are more committed and willing to contribute information when their organisation backs them. Time, resources and knowledge are some of the constraints faced by the participants that may hinder information sharing.
- Only few energy sector specialists have in-depth understanding of both the complexities of the energy systems and cyber security.
- Energy security issues are often addressed only at the EnC CP country level, maintaining for example a national focus only, without taking into account the complexity of the interdependence of CPs and EU in multiple aspects of the energy area, including cyber security.
- The legal and policy context is complex and fragmented.
- The quality of the shared information is not always at the required level, due to inconsistent use of the applicable taxonomy for example.
- There is a need to create public-private partnerships when sharing information.
- Information is shared between heterogeneous players.
- Many companies in the sector give more importance to the safety of their physical infrastructure than to the security of their computer, process systems and data.
- Few good practices have been identified on the subject, and the current information sharing initiatives lack visibility within companies in the energy sector.

---

[153] *Source: https://www.enisa.europa.eu/publications/information-sharing-in-the-energy-sector*

Based on ENISA observations and SWOT analysis of the proposed operational cooperation mechanism on the EnC level have been prepared.

S
STRENGTHS

Participants in information sharing initiatives are more committed and willing to contribute with information when their organisation backs them.

Trust is a key component of information sharing.

There is a need to create public-private partnerships when sharing information.

W
WEAKNESSES

The legal and policy context is complex and fragmented.

Energy security issues are often addressed only at the EnC CP country level, maintaining for example a national focus only, without taking into account the complexity of the interdependence of CPs and EU in multiple aspects of the energy area, including cyber security.

Few good practices have been identified on the subject, and the current information sharing initiatives lack visibility within companies in the energy sector.

O
OPPORTUNITIES

ECS can lead the establishment of E-ISAC for EnC CPs and position itself as the CSIRT/CERT Network Secretariat for EnC CPs

As a provision of existing acts an early warning communication system should be established between EnC CPs (NRAs, TSOs)

T
THREATS

Unverified cyber incident information exchanged between EnC CPs could cause distrust.

Cascading cross-border cyber incidents could cause significant damage to EnC CPs and also to EU

7.1.3 Recommendation on how to align certification schemes and procedures

For EnC CPs it is crucial to have unified certification schemes and procedures aligned with respective EU ones. The purpose of the EU cybersecurity certification framework under the Regulation (EU) 2019/881 is to establish and maintain the trust and security on cybersecurity products, services and processes. The similar goal should be achieved with Energy Community certification schemes and procedures. We propose that the EnC CP E-CSIRT secretariat should act as a formal body for recommending EnC CPs the standards and best practices in cybersecurity. Until there is no final ENISA recommendation of specific standards in energy we propose the following to be done by EnC CP E-CSIRT secretariat:

- Recommend the usage of ISO 27000 family of standards in EnC CPs energy sector companies (TSOs, DSOs, power generation etc.) for defining information security processes
- Recommend the usage of ISO 27019 standard in EnC CPs energy sector companies (TSOs, DSOs, generation etc.) for defining information security controls in relevant OT environments[154]
- Recommend the usage of ISO 31000 in EnC CPs energy sector companies (TSOs, DSOs, generation etc.) for risk assessment and risk management[155]
- Recommend the ISO 27001 certification audit of processes in energy sector companies with EnC CI or ES
- Recommend the ISO 3100 certification audit of energy sector projects in energy sector companies with EnC CI or ES
- In the case that later on ENISA define in certification schemes standards for the same purposes which differs of those proposed the EnC CP E-CSIRT secretariat should prepare the mapping from already recommended standards to those.
- In the case of vendor system certification schemes to recommend all those systems, standards and solutions which will ENISA provide[156] in the future
- In the case of human certification schemes, it should endorse EnC CPs to establish university degree and qualification in cybersecurity with energy sector specific specialisation. On the long term this certification should comply to ENISA certification scheme.
- Until the EnC CPs reach the goal of establishing university degree and qualification in cybersecurity with energy sector specific specialisation it should recommend the following certifications to be used:
    - For Chief Information Security Officer position in energy sector companies with Enc CI or ES - CISA[157], CISM[158] or CISSP[159]
    - For IT auditor position at NRA or in energy sector companies with Enc CI or ES – CISA or ISO 27001 Lead auditor[160]
- Obligate the EnC CPs NRAs to influence their own governments about complying to recommendation as well as conducting sectorial audits regarding cyber security especially in the field of security of supplies and CI.

---

[154] https://www.iso.org/standard/68091.html

[155] https://www.iso.org/iso-31000-risk-management.html

[156] At this moment ENISA is in preliminary phase of preparing the system certification schemes

[157] http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Pages/default.aspx

[158] http://www.isaca.org/CERTIFICATION/CISM-CERTIFIED-INFORMATION-SECURITY-MANAGER/Pages/default.aspx

[159] https://www.isc2.org/Certifications/CISSP

[160] https://pecb.com/en/education-and-certification-for-individuals/iso-iec-27001/iso-iec-27001-lead-auditor

7.1.4 Recommendations regarding awareness and training

Based on the assessment of current availability of cybersecurity experts and training programmes in EnC energy sector (e.g. CA, NRA, TSO) and taking into the account foreseen changes to EnC acquis as well as EnC level organisational structures we propose to establish EnC Cybersecurity education programme with the purpose to facilitate implementation of proposed recommendations.

Goals of the programme might encompass following topics:

- Transposition of EnC acquis cybersecurity requirements into local legislation
- Development of criteria for the identification of CI, ESP and significant disruptive effect
- Contents and implementation of requirements related to Operators security plans (implementation of NIS requirements)
- Topics related to CSIRT and ISCA implementation and operation
- Training on cybersecurity EU wide standards and good practice
- Cybersecurity aspects of new and emerging technologies in energy sector

7.2 Contracting Parties General Recommendations

Based on the recommendations on the Energy Community level and recommendations developed for Contracting Parties, major general recommendations for all Contracting Parties are given bellow:

- The National Cyber Authorities, together with the NRAs should develop and prescribe requirements certification scheme for CISO position in energy sector (e.g. based on ISO 27019 lead auditor IRCA certification standard or other international certifications as CISA, CISM and CISSP).

- Contracting Parties should establish bilateral cooperation's through country energy CSIRT and ISAC[161] with neighbouring countries to address cascading risks.

- For the energy sector companies, it is of outmost importance for successful managing the cybersecurity risks to completely and successfully finish the unbounding process and the segregation of unnecessary interconnected IT/OT systems.

- The TSOs (both electricity and gas) should continue implementing EU wide and international cybersecurity good practices (ISO27000 framework, especially ISO 27019) and establish a continuous risk management process that is regularly reviewed. Similar recommendation applies to DSOs.

7.2.1 Competent Authorities general recommendations

Based on the EU cybersecurity legislation and proposed adoption of adapted ECI and NIS directives in the EnC acquis and having in mind the key role of National Competent Authority, the most important general recommendations for national Competent Authorities are given below:

- It is highly recommended that the CA, the NRA, and the responsible Ministry(ies) starts as soon as possible with the implementation of the legal framework and to provide sufficient budgetary

---

[161] CSIRT and ISAC to which energy sector communicate.

resources during implementing laws, legal documents and strategies for the cyber protection in the energy sector. It is recommended that the CA organizes a sector specific CSIRT or at least 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(ies) 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.

- During the establishment of energy specific CSIRT, 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 to make the management process more compliant with EU processes.

- For the smaller DSOs, generators or new type of market participants in energy sector 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.

7.2.2 National Energy Regulatory Authorities general recommendations

NRAs in EnC CPs need to be actively involved in the establishment of national energy sector related cybersecurity capacities and contribute to adaptation of local legislation. In order to enhance cybersecurity related capabilities on NRA level and to empower CPs NRAs with cybersecurity supervision capability in energy sector we have the following general recommendations:

- 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 which 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 Cyber CGNRA 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.

7.2.3 Electricity sector general recommendations

Key electricity sector specific recommendations are given:

- The electricity TSOs also should focus on handling new type of vulnerabilities which may come also from vendors and/or service providers. It must be also recognized that the risks are coming not only to damage Windows/Linux based systems but also PLCs, smart metering/synchronisation or other OT units.
- The TSOs should disconnect all critical networks from direct public access infrastructure thus limiting remote access. Only screened and online monitored personnel may access the OT systems.
- Mandatory information security audit and cross- system penetration tests are highly recommended. During this process we highly recommend forming of expert level SOC in for monitoring events and handling incidents.
- The personnel managing cybersecurity in the electricity market operator should have international certification of capability such as CISM, CISA or CISSP. Additionally, all administrators of high-risk systems should pass the certifications of information security capability from the vendors.
- It would be mandatory that the TSO take an active role in the process of forming energy ISAC in the Contracting Party, as well as providing information and expert content in it.
- The electricity DSOs should form their own cyber security protection environment capability for issues as smart metering and managing large scale IoT systems.
- The electricity smart metering project should be constantly monitored and audited for cybersecurity threats. The formation of 7/24 SOC for smart metering, SCADA and IoT is highly recommended.
- During the realisation of projects of smart grid, energy management system (EMS) and smart metering, it is highly recommended to implement high security standards ISO 27000, ISO 27019, ISO 31000. When purchasing and installing IT/OT strict vendor security checkout shall be mandatory. It is recommended that all the installed systems have security by design framework approved construction, especially the smart grid component.
- Members and observers of ENTSO-E shall actively cooperate within cybersecurity related working groups to benefit from initiatives driven by ENTSO-E and assure that the national activities will be synchronized with other European electricity TSOs.

7.2.4 Gas sector general recommendations

Key electricity sector specific recommendations are given:

- For the gas TSOs one of main focus should be to recognize legacy IT and OT systems and their known and yet-to-be- found cybersecurity vulnerabilities in order to mitigate them.
- During yearly control of pumps and metering (the ones that does have smart features and interconnection) a security test during the security audit is recommended.
- The TSO should disconnect all critical networks from the direct public access infrastructure thus limiting remote access. Only screened and online monitored personnel may access the OT systems.
- During developing complex data systems, a security development lifecycle should be in place.
- The gas TSO should conduct an assessment of potential effects caused by CMI (coronal mass injection) on CI and should also manage those risks.
- The gas DSOs should address risks concerning IT operations and IT security when the segregation from TSOs is done completely especially with systems connected through TCP/IP protocol.

- For gas TSOs and DSOs it is highly recommended to implement ISO 27001 process-based ISMS as well as to form cyber security defence environment capability for issues as managing large scale IoT systems.
- The experts in gas sector managing cybersecurity should have international certification of capability such as CISM, CISA or CISSP and administrators of high-risk information systems should have certifications of information security capability from the relevant vendors.
- Members and observers of ENTSO-G shall actively cooperate within cybersecurity related working groups to benefit from initiatives driven by ENTSO-G and assure that the national activities will be synchronized with other European gas TSOs.

7.3 Contracting Parties specific recommendations

In the following chapters EnC CPs specific recommendations are given. The asymmetry of Contracting Parties specific recommendations is due to the existing state of cybersecurity related legislation, standards, organisational frameworks cybersecurity requirements and certifications schemes as well as risk assessment and other EnC CPs related facts. For each EnC CP three key recommendations are given.

7.3.1 Albania

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.

As the Kosovo* and the Albania Working Group are developing an action plan for joint power exchange we propose that the Ministry of Infrastructure and Energy implements ISO 27k, ISO 27019[162] and ISO 31000[163] based processes for cybersecurity from the first moments of planning so the newly formed IT systems can be certified from the first moments.

During the realisation of the project converting Vlore thermal power plant to gas as a source, it is highly recommended to implement high security standards ISO 275, ISO 27019, ISO 31000. When purchasing and installing IT/OT strict vendor security checkout is mandatory.

---

[162] *https://www.iso.org/standard/68091.html - Information security controls for the energy utility industry*

[163] *https://www.iso.org/iso-31000-risk-management.html - Risk management*

7.3.2   Bosnia and Herzegovina

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

During the planning and execution of Tuzla 7 lignite power plant project the TSO should conduct a targeted security risk assessment about foreign vendors supplying networking ICT equipment. Also, the impact of cascading risks to TSO must be identified and efficiently considered and mitigated. The cooperation of the TSOs of Bosnia and Herzegovina, Montenegro and Serbia, NOS BiH, CGES and EMS in Security Coordination Centre (SCC) should be expanded to handling cybersecurity incidents with yearly capability exercises.

During the CrossBow[164] project cooperation the TSO (NOS BiH) should conduct their own real time risk assessment on the proposed smart grid solutions by considering especially potential cross-border risks.

7.3.3   Georgia

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.

Georgia is a country which, despite doing a lot in cybersecurity, is in need to expand its defence capabilities even more especially in energy sector. The energy related governmental organisations and private companies must provide sufficient budget for developing more complex cyber defences (such as

---

[164] *Source: http://crossbowproject.eu/about-crossbow/*

APT defence, OT systems high-security authorisation infrastructure etc.) as well as an energy security simulator platform [165] for exploring/modelling cyber warfare tactics in energy infrastructure

The National Cyber Security Authority (DEA) must extensively expand its capabilities to react in energy related cyber incident issues by organizing dedicated 7/24 energy CSIRT as well as respective energy ISAC for PPP purposes. CA must establish the system for early warning and exchange of information on cyber threats / provision of assistance in energy.

National Regulatory Authority for energy sector (NRA) should cooperate with DEA to define/identify energy sector CI or OES operators and organizations. The NRA must develop its own cyber security expertise in energy sector to successfully cooperate with DEA. The cyber 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 to make the management process more compliant with EU processes.

Georgia need to establish constant bilateral cooperation through state energy CSIRT and energy ISAC with neighbouring countries if possible, to address cascading risks. We also recommend forming a NATO supervised joint energy CSIRT as a regional cooperative cyber security body in energy sector to resolve and handle issues about cyber incidents in energy.

Georgia's Improved Power Transmission (GIPT) Project was finalised 2015 so we recommend the TSO should conduct a targeted security risk assessment especially about the possible impacts of cascading risks in smart grid component and transformer gas monitoring system.

As legacy systems are prevailing in parts of electricity and gas infrastructure the DEA must take strict supervision of TSOs and DSOs in order to manage risks regarding them.

7.3.4   Kosovo*

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.

The electricity TSO (KOSTT) and KEK [166] must provide joint continuous cyber risk assessment (ISO 31000 preferred) and management of cyber assets of KOSOVA A and B power plants in order to defend the critical

---

[165] *An integrated distributed laboratory which facilitate the modelling, testing and security assessment of energy systems beyond the capacities of each single entity, enabling remote access to software and equipment anywhere in the state, by establishing a real-time interconnection to the available facilities and capabilities*

[166] *Korporata Energjetike e Kosovës http://kek-energy.com/kek/*

assets as well as to audit the cyber security controls of the plants. The same refers with a focus in planning and vendor controls for the "Kosova e Re" power plant which is under development.

During the planning and realisation of the project of the Albania-Kosovo Gas Pipeline (ALKOGAP), it is highly recommended to implement high security standards ISO 27000, ISO 27019, ISO 31000. When purchasing and installing IT/OT strict vendor security checkout is mandatory.

7.3.5   Moldova

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.

Moldova need to urgently build its resilience to a new era of hybrid threats. The 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.

During implementation of more efficient and competitive mechanisms for cross-border trading and balancing[167] Moldova TSO must assess and manage cyber risks, especially regarding cascading risks from and to Ukraine. This is also highly recommended for Power Transmission Network Rehabilitation project.

In order to increase the capacity of the Moldova – Ukraine interconnection it is envisaged a new 330kV voltage line "Balti-Novodnestrovsk" project. We recommend the TSO should conduct a simulated security risk assessment especially about the possible impacts of cascading risks in grid components and transformer station monitoring system with focus on quantification of risks in order to properly develop a cyber security budget for it.

Project Energy II, which provides power equipment modernization and a new metering system, now completed, and a new SCADA system has been installed. We also recommend the TSO to conduct a security audit of the newly introduced systems.

RES-E grid integration, the renewable resources distribution in the Republic of Moldova, and their potential smart grid integration plans should also trigger a cybersecurity risk assessment of the subject.

---

[167]   https://ua.energy/media-2/news/ukrenergo-moldelectrica-and-the-energy-community-to-improve-processes-accompanying-cross-border-power-exchange-between-ukraine-and-moldova/

During the planning and developing the Ungheni-Chisinau project[168] it is mandatory to implement ISO 31000 standard for overviewing and managing risk as well as ISO 27001 for managing processes in security. Also, strict vendor and supplier control must take in place as well as security development lifecycle management during development of complex IT and OT systems.

As legacy systems are prevailing in parts of electricity and gas infrastructure, the NRA must take strict supervision of TSOs and DSOs in order to manage risks to be able to provide the needed security level of supplies.

7.3.6 Montenegro

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.

During CrossBow project cooperation the potential future TSO (CGES) should conduct their own real time risk assessment on the proposed smart grid solutions in testing especially regarding the potential cross-border risks.

In May 2019, Montenegro joined the not-so-large group of countries that managed to cover the entire electricity demand over a certain period of time from domestic renewable energy sources. For National Energy Regulator of Montenegro (RAE) is recommended that all small and medium scale renewable power companies get sufficient cyber security information by helping them joining the energy ISAC as a source of information, analysis and remediation solutions.

All the cybersecurity risks when developing infrastructure for Adriatic Pipeline and the Ionian-Adriatic Pipeline (TAP and, IAP[169]) must be on-time addressed and managed to prevent cascading incidents. It is imperative to put up a SOC during development and to coordinate it with Albania, Greece and Italy gas TSO similar organisations. We believe that in present geo-political surrounding Montenegro should prepare all it need to handle cyber risks of those developments.

At present, no gas market exists in Montenegro hence no recommendation.[170]

---

[168] *Involves the construction of a new gas transmission pipeline with a length of 120km, three gas delivery stations (two in Chisinau and one in Ungheni, Semeni locality) and equipping the steering and dispatching centre in Ghidighici.*

[169] *Source: https://en.wikipedia.org/wiki/Ionian_Adriatic_Pipeline*

[170] *Source: https://energy-community.org/implementation/Montenegro/GAS.html*

7.3.7 North Macedonia

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.

As day-ahead market (DAM) is scheduled for the end of November 2019, while the go-live of Bulgaria and Macedonia (BG-MK) market coupling will follow in January 2020, we propose to Ministry of Economy to force implementing ISO 27k, ISO 27019, ISO 31000 based processes for cybersecurity so the newly formed IT systems can be certified.

During CrossBow project cooperation the TSO (MEPSO) should conduct their own real time risk assessment on the proposed smart grid solutions in testing especially regarding the potential cross-border risks.

As the government established Macedonian Energy Resources (MER), to oversee construction of an internal gas distribution network during this development ISO 27k based cyber risk analysis is recommended.

During the planning and realisation of the project Nea Mesimvria – Skopje gas pipeline, it is highly recommended to implement high security standards ISO 27k, ISO 27019, ISO 31000. When purchasing and installing IT/OT strict vendor security checkout is mandatory.

During CrossBow project cooperation the DSO (ELEM) should conduct their own real time risk assessment on the proposed smart grid solutions in testing especially regarding the potential cross-border risks.

7.3.8 Republic of Serbia

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.

The Ministry of Mining and Energy and the NRA should be also focusing on achieving an obligatory national educational and certifying scheme for the CISO position in the energy sector companies based on ISO 27019 lead auditor IRCA certification standard or other international certifications such as CISA, CISM and/or CISSP.

As day-ahead market (DAM) is in place from 2016 on SEEPEX. Serbia and Hungary are hoping that the planned merger between their respective power exchanges, SEEPEX and HUPX, will take place by the end of 2019. We propose to the NRA to force implementing ISO 27k, ISO 27019, ISO 31000 based processes for cybersecurity so the interconnected IT systems may be certified.

The Republic of Serbia TSOs (Elektromreža Srbije - EMS, SrbijaGas, JugoRosGas) should implement ISO 27019 in the processes 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 not be subcontractors but full-time employees, especially the obligatory CISO position to fulfil segregation of duties requirements.

During the CrossBow project cooperation, the TSO (EMS) should conduct their own real time risk assessment on the proposed smart grid solutions in testing especially regarding the potential cross-border risks.

As the government appointed Gastrans to lead TurkStream pipeline development an ISO 27k based cyber risk analysis of the project is recommended for the gas TSO.

During the planning and realisation of the project of Banatski Dvor gas storage facility expansion, for SrbijaGas it is highly recommended to implement high security standards ISO 27k, ISO 27019, ISO 31000. When purchasing and installing IT/OT strict vendor security checkout is mandatory.

The electricity DSO (Elektroprivreda Srbije - EPS) should form their own cybersecurity defence environment capability for issues as smart metering and managing large-scale IoT systems. The formation of 7/24 SOC for smart metering, SCADA and IoT is highly recommended. The personnel managing DSO cybersecurity must have international certification of capability such as CISM, CISA or CISSP.

7.3.9 Ukraine

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 and Energorynokmust.

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.

As Ukraine has been a target of series of sophisticated cyber-attacks against energy critical infrastructure it is in state of hybrid war. In this perspective it was very hard to give proper operational recommendations as available data is often too obscure – of national security reasons. If some of the proposals and recommendation are in place, we suggest further improvement in a continuous PDCA cycle[171].

On operational level the 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.

As electricity market and DAM is in phase of planning 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 in the processes 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 position to fulfil segregation of duties controls.

During the second half of 2019, 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 will take place. 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 (UGS)[172] it is highly recommended to implement high security standards ISO 27k, ISO 27019, ISO 31000 on Naftogaz/UGS. When purchasing and installing IT/OT strict vendor security checkout is mandatory.

---

[171] *https://en.wikipedia.org/wiki/PDCA*

[172] *Source: https://annualreport2015.naftogaz.com/en/operacijna-dijalnist/pidzemne-zberigannja-gazu/*

8 Impact assessment of implementation of proposed measures and acts

The goal of this section is to list the proposed measures, describe their expected outcomes, economic and human costs, as well as an expected impact level on the overall cybersecurity capabilities of the EnC CPs. The measures are grouped into the following, distinctly different groups:

- Legislative measures
- Organizational measures
- Cooperation improvement
- Cybersecurity education
- Cybersecurity certification.

This overview of the proposed measures is presented in the rest of this section.

8.1 Legislative measures

The list of proposed legislative measures is listed in the table below. These measures will allow the EnC CPs to make have aligned legislation and be able to better identify and secure their CIs.

Table 14: Proposed legislative measures, costs and impact

Proposed measures and acts	Expected outcomes	Economic cost	Human resource cost	Impact on EnC CP
Proposal for legal framework/identification of CI end ES and proposals for energy sector companies with CI and/or ES	Identified CI and ES. CI and ECI protection contact points and communication lines are established. There will be a need of constant monitoring and control of CI and ES by organising 7/24 SOC on behalf of TSOs and/or DSOs. Improved security of supplies and overall better energy delivery to customers as potential of cyber incidents lowers.	For TSOs and DSOs with CI and/or ES there is a cyber security investment impact as some of the controls/systems must be upgraded and/or expanded. The budgetary expansion for security investment should be around 5% for systems/processes with medium risk and up to 15% for systems/ processes with high risks respective of overall investment.	TSOs and DSOs with CI and/or ES will need to employ/appoint chief information security officers and engage cybersecurity auditor(s). Organising a 7/24 SOC will significantly expand the need for more human resources as well.	HIGH

8.2 Organizational measures

The list of proposed organizational measures is listed in the table below. These measures will allow the EnC CPs to make the necessary changes in their existing or soon to be built organizations.

Table 15: Proposed organizational measures, costs and impact

Proposed measures and acts	Expected outcomes	Economic cost	Human resource cost	Impact on EnC CP
Proposed organisational changes for the NRA (internal knowledge of cybersecurity issues, information security audit capability in energy sector)	Operational legal framework: audit program, PPP program, CA cooperation program. The NRAs is by legal framework given the power to issue final and binding decisions that are not subject to outside (e.g. ministerial) scrutiny.	Impact in NRA budgetary spending on human resource and external experts.	NRA will need to employ cybersecurity auditor(s) and sectorial cyber experts for analysing licensee data.	MEDIUM
Proposed changes for national CA regarding forming ad maintaining energy specific CERT/CSIRT	Operational legal framework: working energy CSIRT and energy ISAC, cross border cooperation, EnC level cooperation, awareness programs, education scheme support. The	CA budgetary spending on putting up energy specific CSIRT and ISAC as well as operating an early warning system is costly. If ISAC, CSIRT and/or early warning are functioning properly it can save the value of energy investment in one country by stopping threats to become real incidents. This saving can only be measured if we have long historical track of energy cyber incident data and the cost of it. The EnC must also provide a budget for EnC CP E-ISAC and EnC CP E-CSIRT secretariat.	CA will need to expand their cybersecurity analyst capability to energy sector specific knowledge or to engage new workforce. In the same time, it will be in need of cybersecurity in energy content managers for supporting E-ISAC and/or awareness programs.	HIGH

8.3 Improved cooperation

The list of proposed measures which would result in closer cooperation and improved information and knowledge sharing between the key energy sector cybersecurity actors are listed in the table below.

Table 16: Proposed cooperation measures, costs and impact

Proposed measures and acts	Expected outcomes	Economic cost	Human resource cost	Impact on EnC CP
Proposals for cross-border cooperation and data exchange	MoU's will provide the needed framework for data exchange (especially risk/threat and incident data) the level of cooperation will grow as the level of trust will allow. This process is usually slow and by some estimation it will reach it's optimum in 10-15 years. On community level it means active moderating activities for EnC.	Joint awareness and simulations probes with cross-border partners will be put into energy CSIRT and ISAC yearly budgets as well as into budgets of SOC operators.	Not applicable as the cooperation and data exchange are basic features in organizing CSIRT, ISAC or SOC.	MEDIUM
Proposals for cross-border crisis management	Successful joint cross-border crisis management among EnC CPs. Limit the extent of cyber incidents and any cascading effects. Active moderation by the EnC.	Joint incident management with cross-border partners are resulting with significant lowering of the cost of the cyber incident.	Not applicable as the incident handling is a e basic features in organizing CSIRT or SOC.	HIGH
Proposal for PPP cooperation	Each EnC CP member state will put up it's own energy ISAC. The ISAC will serve to gather not only big TSOs and DSOs but also SMBs in energy sector. The impact is lower cross-sectorial cascading effect. If EnC CPs does not have or are in a phase of developing E-ISAC, EnC may offer its E-ISAC capabilities to be used. The EnC will also be a moderator between EnC CPs ISACs providing the so needed chain of trust element.	CA to fund ISAC platform and/or cooperate with EnC in creating one. The highest expected cost is expected to be ISAC platform content management. The overall budget impact is not significant.	ISAC platform programming capabilities and also content managers will be in need for EnC CPs Cas and Enc itself also.	LOW

8.4 Cybersecurity education

The list of proposed measures which are necessary to obtain an educated workforce in the key energy sector cybersecurity stakeholders are listed in the table below.

Table 17: Proposed education measures, costs and impact

Proposed measures and acts	Expected outcomes	Economic cost	Human resource cost	Impact on EnC CP
Proposals for implementing energy specific cybersecurity educational/awareness schemes	In each country there will be an educational model for cyber security management professionals in energy sector. In a case that the number of professionals does not reach the required number in the country there is always a possibility of regional cooperation between regional educational institutions. The EnC secretariat will be actively involved in organizing these activities.	Cost of organizing educational programs. Awareness program costs are usually negligible budget elements.	The educational institutions must provide instructors with capability in energy cybersecurity domain.	LOW

8.5 Cybersecurity certification

The list of proposed measures which are necessary to obtain a certified organisations and expert workforce in the key energy sector cybersecurity stakeholders are listed in the table below.

Table 18: Proposed certification measures, costs and impact

Proposed measures and acts	Expected outcomes	Economic cost	Human resource cost	Impact on EnC CP
Proposals for implementing energy specific cybersecurity expert certification schemes	In each country there will be a certification model for cyber security management professionals in energy sector. In a transition period, international certifications like CISA, CISM and CISSP are applied. The EnC secretariat will be actively involved in organizing these activities.	Cost of organizing personal certification.	The certification bodies of educational institutions and/or other local organisations must provide certification capability in energy cybersecurity domain. There is a possibility to optimize this by organizing regional certification bodies.	LOW
Proposals for energy systems/process certification schemes	In each country there will be an ISO compliant process certification model for certifying information security management systems in energy sector. On community level it means unifying certification to comply with EU regulation. In time when system certification model from ENISA will be available a separate analysis must be done for system impact by each country. EnC CP CSIRT secretariat will be actively engaged in making recommendation as well as providing EU certification expertise from ENISA.	ISO certification and system/process policy compliance costs at TSO's and DSO's with CI and/or ES. ISO process policy compliance costs at DSO's with no CI and/or ES. EnC CP E-CSIRT secretariat will have costs in organizing certification events and registering certified parties as well as making (if needed) mapping tables from and to ENISA specifications.	There will be a need for engaging ISO specialists (lead implementer, lead auditor etc.) at TSOs and DSOs. EnC will also be in need for highly skilled cyber security experts (CISA, CISM, CISSP, ISO27LA etc.)	MEDIUM

9 Roadmap with timing for the implementation of the proposed provisions and measures

Roadmap for the implementation of proposed measures has been developed based on the assessment of implementation impacts and having regards to the assessed status of CPs legislative frameworks and risk landscape. Implementation roadmap is proposed from the expert team and should not be viewed as an agreed final program of the Energy Community.

Proposed implementation roadmap has two main streams:

- Energy Community related activities and
- Contracting Parties activities.

It should be noted that adaptation and encompassment of EU cybersecurity legislation into the EnC acquis is more or less a prerequisite to align and foster activities on the Contracting Parties implementation roadmap.

In addition, timely support during the implementation of Contracting Parties roadmap provided as workshops, education events, coordination activities and technical assistance on the EnC level will have significant impact on timely and effective achievement of expected results.

9.1 Energy Community Roadmap

In the table below the implementations roadmap for Energy Community is given, including the proposed provisions and measures, expected results, fulfilment end date and projected sponsor.

Table 19: Roadmap with implementation timing for standard CPs

Proposed provisions and measures	Expected results	Fulfilment End date	Project sponsor
Adapt and encompass EU cybersecurity legislation into the EnC acquis	EnC acquis aligned with EU cybersecurity legislation and good practice	*6 months*	CyberCG
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*	CyberCG
Establish Cyber CG activities monitoring improvements process	Develop and implement monitoring and improvement process	*6 months*	CyberCG
	Regular progress reporting	*Quarterly*	ECS
Support to CPs in the implementation of legislative requirements	Organisation of awareness campaigns, capacity building and training activities	*24 months*	CyberCG
Sharing and coordination of essential cybersecurity information and activities between CPs	EnC CSIRT	*24 moths*	**E-CSIRT** working group
	EnC ISAC	*12 months*	CyberCG
	Cybersecurity incidents early warning communication system	*12 months*	CyberCG
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*	CyberCG, ECS

Based on the risk analysis carried out for this report we identified three distinctly different groups of Energy Community Contracting Parties:

- **Standard CPs** might lack a set of cybersecurity capabilities, but are not implementing high profile, regional energy projects, or are not in immediate and constant danger of cyberattacks originating from nation state actors.
- **Sensitive CPs** implement high-profile, regional energy projects and therefore need additional measures to be implemented in a shortened timeline.
- **High Risk CPs** are in urgent need to implement additional measures towards obtaining an adequate level of cybersecurity and cyber resilience.

The remaining parts of this section contain proposed roadmaps for all three country types for the implementation of the proposed, additional security controls.

Note that this roadmap is only recommendation from the expert team, not agreed as final program of the EnC. Also note that additional considerations should be taken by ECS and adjustments / comments shall be provided before the final version of the roadmap is approved. The proposal of the roadmap / timing

(when approved by ECS) should become the ECS proposal to the EnC CPs, subject to coordination between the EnC CPs and eventual adoption within the CyberCG activities. On policy level for the EnC and in the context of a general evolution of this Cybersecurity Study we are recommending a forming of a follow-up procedure to follow yearly update of the developments.

9.2 Standard CP Roadmap

The Standard Roadmap CPs do not implement high-profile, regional or international energy projects and are not under imminent and constant cyberattack from nation state actors with cyber intelligence capabilities and technical expertise. The following CPs are in this group: Albania, Bosnia and Herzegovina, Kosovo* and North Macedonia.

Table 20: Roadmap with implementation timing for standard CPs

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
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

9.3 Sensitive CP Roadmap

The Sensitive Roadmap CPs implement high-profile, regional or international energy projects of strategic importance for the EU. They are not under imminent and constant cyberattack from nation state actors with excellent cyber intelligence capabilities and technical expertise. The following CPs are in this group: Republic of Serbia (especially gas transport to EU and storage capacity development project in focus), Georgia (EU electricity integration project in focus), Montenegro (gas transport to EU project in focus) and Moldova (EU electricity integration project in focus).

Table 21: Roadmap with implementation timing for Sensitive CPs

Proposed provisions and measures	Expected results	Fulfllment End date	Project sponsor
Addressing gaps between national and EU legislation and standards	National legislation aligned with amended EnC acquis	within 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	within 18 months	CA
	OSP plans developed for EnCCI and OES	within 24 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 12 months	CA
	Early warning cooperation program regarding energy in national CSIRT	within 12 months	CA
Cross-border cooperation and data exchange	Cooperation MoUs with neighbouring countries regarding cybersecurity matters in energy sector, data exchange, incident cooperation	within 12 months	CA
Cross-border crisis management	Cooperation MoUs with neighbouring countries regarding incident cooperation, forming a joint task force	within 12 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 18 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 18 months	TSO/DSO/Vendor
Proposal for PPP cooperation	Operational national energy e-ISAC	within 128 months	CA and NRA

9.4 High Risk CP Roadmap

The High Risk Roadmap CPs implement high-profile, regional or international energy projects of strategic importance for the EU and/or are under imminent and constant cyberattack from nation state actors with the highest cyber intelligence capabilities and technical expertise. These countries require the highest level of expansion in cybersecurity capabilities in the shortest possible period. The following CPs are in this group: Ukraine.

Table 22: Roadmap with implementation timing for High Risk CPs

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	*within 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 6 months*	CA
	CI and ES designation	*within 12 months*	CA
	OSP plans developed for EnCCI and OES	*within 18 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 6 months*	CA
	Early warning cooperation program regarding energy in national CSIRT	*within 12 months*	CA
Cross-border cooperation and data exchange	Cooperation MoUs with neighbouring countries regarding cybersecurity matters in energy sector, data exchange, incident cooperation	*within 12 months*	CA
Cross-border crisis management	Cooperation MoUs with neighbouring countries regarding incident cooperation, forming a joint task force	*within 12 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 18 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 18 months*	TSO/DSO/Vendor
Proposal for PPP cooperation	Operational national energy e-ISAC	*within 12 months*	CA and NRA

Index

List of figures

List of tables

PAGE INTENTIONALLY LEFT BLANK