CEER

Council of European Energy Regulators

Fostering energy markets, empowering **consumers**.

CEER Paper on Cybersecurity in the Clean Energy for All Europeans Package

Cybersecurity Work Stream

Ref: C20-CS-58-03
4 June 2020

Council of European Energy Regulators asbl
Cours Saint-Michel 30a, Box F – 1040 Brussels, Belgium
Arrondissement judiciaire de Bruxelles – RPM 0861.035.445

INFORMATION PAGE

Abstract

This document (C20-CS-58-03) presents how cybersecurity topics have been developed in the Clean Energy for All Europeans Package, going through act by act. This paper also provides information on the status and the roles of the different stakeholders in respect to those topics with a special focus on the role of the national regulatory authorities (NRAs) and of the Council of European Energy Regulators (CEER).

Target Audience

European Commission, energy suppliers, traders, gas/electricity customers, gas/electricity industry, consumer representative groups, network operators, Transmission System Operators (TSO), Distribution System Operators (DSO), Member States, academics, national regulatory authorities (NRAs) and other interested parties.

Keywords

Clean Energy Package (CEP); Cybersecurity; risk preparedness; operator of essential services; cyber-risks; smart meters; digitalisation; Energy Performance of Buildings Directive; Energy Efficiency Directive; Directive on common rules for the internal market for electricity; Regulation on the internal market for electricity; Regulation on risk-preparedness in the electricity sector.

If you have any queries relating to this paper, please contact:
CEER Secretariat
Tel. +32 (0)2 788 73 30
Email: brussels@ceer.eu

Related Documents

CEER Documents

- CEER Cybersecurity Benchmark, 18 December 2019, Ref: C19-CS-56-03.
- CEER Cybersecurity Report on Europe's Electricity and Gas Sectors, 26 October 2018, Ref: C18-CS-44-04.

External Documents

- SGTF EG2 Report on "Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management", June 2019.
- European Parliament and Council Regulation on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC, 5 June 2019, Ref: 2019/941/EU.
- European Parliament and Council Regulation on the internal market for electricity, 5 June 2019, Ref: 2019/943/EU.
- European Parliament and Council Directive on common rules for the internal market in electricity, 5 June 2019, Ref: 2019/944/EU.
- European Parliament and Council Regulation on the European Union Agency for Cybersecurity (ENISA) and on information and communications technology cybersecurity certification, 17 April 2019, Ref: 2019/881/EU (Cybersecurity Act).
- European Parliament and Council Directive on energy efficiency, 11 December 2018, Ref: 2018/2002/EU.
- SGTF EG2 Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems V2, September 2018.
- European Parliament and Council Directive on energy performance of buildings, 30 May 2018, Ref: 2018/844/EU.
- ISO/IEC Standard on Information technology - Security techniques - Information security controls for the energy utility industry, October 2017, Ref: ISO/IEC 27019:2017
- SGTF EG2 Best Available Techniques Reference document for the cyber-security and privacy of the 10 minimum functional requirements of the Smart Metering Systems, 7 November 2016.
- European Parliament and Council Directive concerning measures for a high common level of security of network and information systems across the Union, 6 July 2016, Ref: 2016/1148/EU.
- SGTF EG2 Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems V1, March 2014.
- ISO/IEC Standard on Information technology - Security techniques - Information security management systems - Requirements, October 2013, Ref: ISO/IEC 27001:2013.
- ISO/IEC Standard on Information technology - Security techniques - Code of practice for information security controls, October 2013, Ref: ISO/IEC 27002:2013
- Commission Recommendation on preparations for the roll-out of smart metering systems, 9 March 2012, Ref: 2012/148/EU.
- European Parliament and Council Directive concerning common rules for the internal market in electricity, 13 July 2009, Ref: 2009/72/EC.

Table of Contents

List of Figures

EXECUTIVE SUMMARY

Background

The Clean Energy for All Europeans Package (CEP) is a comprehensive legal package that aims to enhance and further implement the energy union strategy which was adopted in 2015. Based on Commission proposals published in November 2016, the CEP was published in the Official Journal in three waves, first around mid-2018, the second around the end 2018 and the third and last in mid-2019.

The CEP lays down, amongst many other topics, provisions on cybersecurity for electricity. It tackles cybersecurity for smart meters, the obligation(s), especially of the System Operators (SO), to take adequate cybersecurity measures into consideration when performing their duties and in providing their services.

Objectives and Contents of the Document

This report details to what extent cybersecurity topics are developed in the legal acts that constitute the CEP (act by act). It further analyses the status of implementation and the roles of the involved stakeholders in respect to those topics with a special focus on national regulatory authorities (NRAs) and CEER.

Beyond that, this document gives some indications and advices on how those topics can be addressed by NRAs and CEER.

Brief Summary of the Conclusions

Cybersecurity is probably one of the hottest and still most underestimated topics of our modern society.

The wide use of the Internet and the continuous growth (both in speed and in the audience) of mobile communication technologies, has had an impact on the grid operator's infrastructure and processes. The way to deliver energy to a customer (regardless whether she/he/it is a standard or protected customer, a large industrial or small household) requires the grid to be adapted to meet the needs of a distributed network. Digitalisation and networks are of key importance to make sure that our electricity and gas networks remain safe from harm, be it caused by intentional or accidental attacks, and that the energy is delivered efficiently to the end-customers.

This document illustrates the legal and regulatory framework that actors in the energy markets should take into consideration; it does not make any claim to be exhaustive and complete but should be understood as a list of minimum standards and guidelines that TSOs and DSOs must become familiar with in the near future in order to operate in a market that embeds more and more aspects of digitalisation.

1 Introduction

The Clean Energy for all Europeans Package (CEP) consists of eight legislative acts of which five are directly and explicitly dealing with different cybersecurity topics. Those that deal with cybersecurity are the following:

- Energy Performance of Buildings Directive (EU) 2018/844[1]
- Energy Efficiency Directive (EU) 2018/2002[2]
- Directive on common rules for the internal market for electricity (EU) 2019/944[3]
- Regulation on the internal market for electricity (EU) 2019/943[4]
- Regulation on risk-preparedness in the electricity sector (EU) 2019/941[5]

Those acts modify or repeal legislative acts which did not explicitly deal with the "cyber" topic. It must be understood that cybersecurity was not the only reason to repeal some of the already existing acts, but it has been a source of concern.

On this point, the CEP marks a turning point in the way the European Commission (EC) deals with the subject of cybersecurity and integrates it into legislative acts dealing with energy. The use of more general acts (as an example, the General Data Protection Regulation does not contain any specific rules for the different sectors, but leaves it to companies to apply the principles provided) was replaced by the use of secondary legislation to which the EC will delegate the power to implement technical aspects of a more general nature. This spread of cybersecurity in multiple acts comes with additional problems; it can allocate the responsibilities among a number of actors, making it difficult to understand who has to act. One main objective of this report is to identify every cyber topic in the CEP and who is the stakeholder responsible in every case.

[1] European Parliament and Council Directive on energy performance of buildings, 30 May 2018, Ref: 2018/844/EU
[2] European Parliament and Council Directive on energy efficiency, 11 December 2018, Ref: 2018/2002/EU
[3] European Parliament and Council Directive on common rules for the internal market in electricity, 5 June 2019, Ref: 2019/944/EU
[4] European Parliament and Council Regulation on the internal market for electricity, 5 June 2019, Ref: 2019/943/EU
[5] European Parliament and Council Regulation on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC, 5 June 2019, Ref: 2019/941/EU

2 Energy Performance of Buildings Directive

The revised Energy Performance of Buildings Directive (EU) 2018/844[6] was the first of the eight legislative acts in the CEP to be adopted. It entered into force on 9 July 2018. EU countries have to transpose the new elements of the directive into national law by March 2020 (20 months after the adoption). This directive includes measures that will accelerate the rate of building renovation towards more energy efficient systems and strengthen the energy performance of new buildings, making them smarter.

2.1 Cybersecurity in the Energy Performance of Buildings Directive

This smartness that shall ideally derive from the application of new systems and the renovation of the buildings may become a cyber-risk, so attention was paid in the directive to that topic.

To that end, Annex IA states that building a smart readiness indicator calculation methodology shall take into account the principles of occupant ownership, data protection, privacy and security, in compliance with relevant EU data protection and privacy laws as well as best available techniques for cybersecurity.

To this extent, a reference was made to a document that the European Commission developed that contains clear instructions on the selection of technologies and techniques available on the European market to respond to this need.

2.2 Role of stakeholders

The National Regulatory Authorities (NRAs) or CEER do not have any explicit role to play with that methodology as the European Commission shall establish it through a delegated act.

Nevertheless, it is likely that NRAs may nominate experts to take part in the discussion and be consulted by the European Commission before the adoption of this delegated act.

[6] European Parliament and Council Directive on energy performance of buildings, 30 May 2018, Ref: 2018/844/EU

3 Energy Efficiency Directive

The revised Energy Efficiency Directive (EU) 2018/2002[7] was part of the second wave of the legislative acts in the CEP to be adopted by the end of 2018. It entered into force as of 24 December 2018. EU countries have to transpose the new elements of the directive into national law between June 2020 and October 2020. This directive includes measures that will set an energy efficiency target of 32.5% by 2030[8], with a possible upward revision in 2023.

3.1 Cybersecurity in the Energy Efficiency Directive

To reach such an energy efficiency objective, actions including smart metering, billing and consumption information for heating, cooling and domestic hot water should be developed in real time.

The information gathered for this purpose should be transferred and processed according to cybersecurity standards and according to the existing rules for privacy and data protection, especially in respect of the personal information that belongs to the consumers. In addition, the national laws of each Member State are applicable.

3.2 Role of stakeholders

No explicit role is provided for NRAs or CEER, unless they are in charge of heating, cooling and domestic hot water topics. However, Regulatory Authorities covering multiple utilities are a minority in the EU.[9]

Nevertheless, NRAs may be consulted as the obligations that may derive from the implementation of this directive may prove to be close to those already existing for smart metering in the Directive on common rules for the internal market in electricity. A coherent application of the standards may create an environment where all regulators (energy-related or simply working on other matters) may share the same approach toward cybersecurity matters.

[7] European Parliament and Council Directive on energy efficiency, 11 December 2018, Ref: 2018/2002/EU
[8] The energy efficiency target is defined as the intended reductions in energy over a specified time frame that have been defined in a SMART manner. To this extent the EU aims to reach a reduction of 32.5% of energy till 2030 through different actions. This value did not take into consideration the BREXIT, and the target may be revised.
[9] See the CEER Report on National Models of Cooperation among Different Sectoral Regulators in the Context of Consumer Law Enforcement, 29 April 2020, which has a listing of regulators with responsibilities beyond electricity and gas.

4 Directive on common rules for the internal market in electricity

This new electricity directive (EU) 2019/944[10], which repeals the Electricity Directive (2009/72/EC)[11] of the 3rd Energy Package, is aimed to adapt existing market rules to the new market realities.

Furthermore, in this new directive, the consumer is put at the centre of the clean energy transition and thus plays a crucial role. The new rules enable the active participation of consumers whilst putting in place a strong framework for consumer protection. One of the key elements of this active participation is smart metering systems and the information they can bring, together with the benefits they can produce for the consumers and for entire communities.

4.1 Cybersecurity in the Directive on common rules for the internal market in electricity

Some articles of this directive explicitly focus on cybersecurity obligations to be established on data management processes of transmission and distribution system operators and on cybersecurity aspects of smart metering platforms.

4.1.1 Functionalities of smart metering systems

In particular, the directive states that the security of the smart metering systems and data communication shall comply with all relevant EU security rules, having due regard for the best available techniques for ensuring the highest level of cybersecurity protection while bearing in mind the costs and the principle of proportionality.

4.1.2 Data management

The directive also states that Member States and system operators (setting a role for both transmission and distribution operators) are responsible for data management, including for assuring the cybersecurity of data flows.

4.2 Role of NRA

NRAs are often in charge of assessing costs and evaluating the benefits of all related projects. Such assessments should take into consideration the methodology for cost-benefit analyses as well as the best available techniques for cybersecurity with regard to the Commission Recommendation 2012/148/EU[12]. In this respect it shall be understood that the best available techniques do not offer economic indexes that would help in the process of assessing the cost-benefit analysis for the regulators, without having an in-depth knowledge of the matters involved.

[10] European Parliament and Council Directive on common rules for the internal market in electricity, 5 June 2019, Ref: 2019/944/EU
[11] European Parliament and Council Directive concerning common rules for the internal market in electricity, 13 July 2009, Ref: 2009/72/EC
[12] Commission Recommendation on preparations for the roll-out of smart metering systems, 9 March 2012, Ref: 2012/148/EU

4.3 Role of CEER

CEER represented NRAs in Smart Grid Task Force (SGTF) Expert Group 2 (EG2), which issued Data Protection Impact Assessment (DPIA) Templates V1[13] and then a V2[14] (for data protection), together with a Best Available Techniques reference document (BRef)[15] (for cybersecurity). Having this in mind we can state that regulators participated and contributed in the definition of best available techniques for cybersecurity expected for smart metering systems.

4.4 Role of other stakeholders

The distribution system operators, as metering system operators in most Member States, have to implement the best available techniques for the metering purposes. It must be noted that, with the objective to further improve the efficiency of the grid and with the aim to reduce costs, new actors are appearing on the energy landscape, and in particular, companies operating Advanced Metering Systems on behalf of the Distribution System Operator(s). While they are very often just system integrators specialised in Advanced Metering Platforms, and with reduced knowledge on cybersecurity compliance issues, their role in the operations linked to the grid is essential. Therefore, they should respect the same rules as imposed on the Distribution System Operators in respect to smart metering. In this respect, the presence of new actors shall be constantly monitored by the regulators in order to assess and to assign the responsibilities at the right level.

[13] SGTF EG2 Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems V1, March 2014
[14] SGTF EG2 Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems V2, September 2018
[15] SGTF EG2 Best Available Techniques Reference document for the cyber-security and privacy of the 10 minimum functional requirements of the Smart Metering Systems, 7 November 2016

5 Regulation on the internal market for electricity

This new regulation (EU) 2019/943[16] seeks to establish a modern design for the EU electricity market, adapted to the new realities of the market, i.e. more flexible, more market-oriented, better placed to integrate a greater share of renewables in line with the Directive on common rules for the internal market in electricity, and open to new waves of digitalisation that may eventually further develop the markets.

5.1 Cybersecurity in the Regulation on the internal market for electricity

5.1.1 Cybersecurity network code

This regulation aims to establish a network code dealing with sector-specific rules for cybersecurity covering aspects such as automation and data flows related to cross-border electricity flows, common minimum cybersecurity requirements applicable to all actors for the electricity markets, planning of future developments, monitoring of the implementation of all measures, reporting obligations in addition to the existing (if needed and if duly justified) and crisis management in the event that cyber risks materialise.

5.1.2 ENTSO-E's and the EU DSO entity's explicit role

The regulation states that the EU DSO entity shall support and ENTSO-E shall promote cybersecurity and data protection. The establishment of the first entity is then a crucial step to progress in this direction.

5.2 Role of CEER

CEER represented NRAs in SGTF EG2, which issued a report on recommendations for the implementation of a cybersecurity network code[17]. This report, described in Annex 2 of this paper, should thus be the basis for the European Commission to define the topics and the priorities that contribute to the process for the creation of a network code. CEER also provided input to the European Commission's 2020 public consultation to establish the priority list of network codes[18], which included consultation on an electricity cybersecurity network code.

5.3 Role of NRAs

NRAs, within the ACER Board of Regulators, draft the Framework Guideline which serve as basis document to the Network Code.

[16] European Parliament and Council Regulation on the internal market for electricity, 5 June 2019, Ref: 2019/943/EU
[17] SGTF EG2 Report on "Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management", June 2019
[18] See https://ec.europa.eu/energy/consultations/consultation-establish-priority-list-network-codes_en

5.4 Role of other stakeholders

Beyond their explicit role, the EU DSO entity (at this point in time represented by the main DSO associations, without any shared legal entity) and ENTSO-E represented System Operators in SGTF EG2, are empowered to issue recommendations for the content of the cybersecurity network code.

The EU DSO entity and ENTSO-E have to prepare the network code under the framework guidelines defined by the European Union Agency for the Cooperation of Energy Regulators (ACER) and then to submit it to ACER for review.

6 Regulation on risk-preparedness in the electricity sector

The Regulation (EU) 2019/941[19] on risk-preparedness in the electricity sector requires that Member States, using common methods, identify all possible electricity crisis scenarios at national and regional levels. Member States must prepare risk preparedness plans based on these scenarios that cooperate and coordinate with neighbouring Member States.

6.1 Cybersecurity in the regulation on risk-preparedness in the electricity sector

This regulation complements the directive (EU) 2016/1148[20] by ensuring that cyber-incidents are properly identified as a risk, and that the measures are taken to address them in a timely manner, as well as that they are properly reflected in the risk-preparedness plans of the Operators and of their respective Member States and regions.

6.2 Role of NRAs and CEER

Each NRA, if it is the competent authority responsible for carrying out the tasks provided for in preparedness regulation, shall establish, after consulting stakeholders, a risk-preparedness plan that address risks that shall include cyber-incidents.

The plans should be developed having in mind electricity crisis scenarios, taking into account events such as cyber-incidents and cyber-attacks. In addition, the scenarios shall take into consideration the most common scenarios such as natural disasters and fuel shortages, to cite just a couple. An exhaustive list of the scenarios was defined by ENTSO-E and NRAs and they set out the measures necessary to prevent and to mitigate the impact such crisis.

Risk-preparedness plans have to be agreed by national authorities and at regional level in order to ensure that they are supported.

Plans should consist of two parts, setting out national measures and coordinated measures agreed among the NRAs in each region.

The risk-preparedness plan shall include the following information:

- Shall summarise the electricity crisis scenarios;
- Shall establish the responsibilities of the competent authorities involved in the management of the crisis;
- Shall describe the national measures to prevent and manage the crisis, should they materialise;
- Shall designate the role of a national crisis coordinator; and
- Shall describe the mechanisms used to share information about electricity crises within the state and at regional level.

The risk-preparedness plans should be updated regularly to ensure that the plans are effective and relevant.

[19] European Parliament and Council Regulation on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC, 5 June 2019, Ref: 2019/941/EU
[20] European Parliament and Council Directive concerning measures for a high common level of security of network and information systems across the Union, 6 July 2016, Ref: 2016/1148/EU

7 Conclusion

Every single actor in the energy business today relies on modern IT/OT equipment that are at the foundation of their processes. Equipment and processes are vulnerable to potential security failures that may be exploited, as all activity takes place over networks and with limited human interaction. Therefore, any active actor in the energy sector (from TSOs, DSOs to new emerging actors), is in a crucial position in implementing appropriate cybersecurity rules and standards. Especially if the actor plays a key role in the supply chain of energy, when a cyber-attack could have substantial impact on the functioning of the energy system and of the energy markets.

In an era where classic physical networks of grid operators are integrated with information flows and information technologies, it is of utmost importance that the energy markets and all its actors are prepared to deal with any security breach. No matter if a security vulnerability might be the cause of an erroneous configuration or the consequence of a malevolent external attack. Each professional actor in the energy business must be able to identify and neutralise or mitigate the effect of any cyber incident at any time.

The CEP has set a milestone for topics that had previously been postponed but that had to be addressed in order to provide solutions to current risks and that may help in the resolution of issues related to cybersecurity.

Through five legislative acts, the EU has set the priorities for providing solutions that address these issues:

- The CEP identified all actors that shall play a role in cybersecurity for the electricity sector;
- All actors have been provided with a responsibility and an assignee that shall take part in the work and in the discussions that will just start this new branch of the energy regulation field; and
- The EU has set a high priority on security for the “smart” part of the new grids, and on protecting the grid through good planning for crises that may emerge, and may become tangible risks.

The work of cyberspace security in the energy markets shall be delegated to specialists that are better positioned to describe, define and implement rules that shall reduce the risk for society.

The need for protecting critical network environments has never been higher than today and those who wait for all cybersecurity rules to be firmly defined and published might become victims of attacks.

It is, therefore, essential that each TSO and DSO is first and foremost responsible for the security of its own equipment and must do everything possible to prevent any potential leakage of its information assets. Each actor must have an understanding of its role and of the risks it may generate in the wider context. The organisation, furthermore, must take any necessary action to prevent an incident occurring. Such preventive technical and procedural protection measures should be in line with official regulations and must, above all, be perfectly adapted to the very circumstances of the respective actor. Their EU representatives (EU DSO entity and ENTSO-E) should help to develop that awareness.

To conclude, even though NRAs do not have an explicit role in cybersecurity topics in the CEP, they can influence the way forward through their national power over financing and objectives definition and through CEER's participation in the network code process, in agreement with all the other National Competent Authorities that are empowered and responsible for the on-going process.

Annex 1 – List of Abbreviations

Term	Definition
ACER	Agency for Cooperation of Energy Regulators
BRef	Best Available Technics reference document
CEER	Council of European Energy Regulators
CEP	Clean energy for all Europeans package
CSIRT	Computer Security Incident Response Team
DG Ener	Directorate-general for energy
DPIA	Data protection impact assessment
DSO	Distribution system operator
ENISA	European Union Agency for Cybersecurity
ENTSO-E	European network of transmission system operators for electricity
GGP	Guidelines of Good Practice
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardisation
IT	Information Technology
MISP	Malware Information Sharing Platform
MS	Member States
NCA	National Competent Authority (following the NIS Directive)
NIS Directive	European Parliament and Council Directive concerning measures for a high common level of security of network and information systems across the Union, 6 July 2016, Ref: 2016/1148/EU
NRA	National Regulatory Authority
OES	Operator of essential services
OT	Operational technology
SGTF EG2	Smart Grid Task Force Expert Group 2
SO	System operator
EU DSO entity	European entity for distribution system operators
TSO	Transmission system operator

Annex 2 – Recommendations of SGTF EG2 to the EC for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management.

Energy systems are inarguably one of the most complex and most critical infrastructures of a modern digital society. They serve as the backbone for its economic activities, security and for consumers' daily life. It is therefore in the interest of the EU and its Member States (MS) to secure the energy infrastructure against cyber threats and risks.

In the EU, one of the key pieces of legislation in this regard is the NIS Directive[21] and its implementation at MS level is a key element. The NIS Directive provides a legislative basis for all sectors, including the energy sector. Specific obligations deriving from the NIS Directive that are already impacting the energy sector are:

1. The NIS Directive addresses a number of general needs in regard to cybersecurity for the energy sector. A specific CSIRT at MS level can be established;
2. The identification of operators of essential services (OES) including energy operators. Those energy operators identified as OES will have to implement appropriate security measures with principles that are general to all sectors; and
3. The OES will have the obligation to notify incidents to their relevant NCA.

The CEP allows sector-specific rules for cybersecurity aspects of cross-border electricity flows, on common minimum requirements, planning, monitoring, reporting and crisis management for the electricity subsector, also referred to as the Network Code on cybersecurity. This Network Code may address cybersecurity challenges and gaps of the electricity subsector, which were identified in an analysis done for the European Commission. The provisions of the Network Code scoped by energy-specific secondary legislation build upon already compulsory measures under the NIS Directive.

The proposed scope for the Network Code on cybersecurity is outlined in the following Figure 1. The Network Code on cybersecurity may address electricity transmission and distribution SOs, and as such the Network Code needs to consider electricity SOs with different capabilities and capacities. It is suggested that all operators should meet a baseline protection that includes the management of known security risks in respect to the essential services (e.g. ISO/IEC 27001:2013)[22] and a prescriptive approach to implement minimum security requirements in the operational infrastructure that could make good use of the certification tools offered by the EU Cybersecurity Act. Operators which are providing services essential for the well-functioning of the economies and societies are identified by respective MS as OES. Those Operators may be subject to advanced cybersecurity requirements reflecting the criticality of the services provided that include the protection of the current infrastructure and specific care in the risk management of their supply chain.

[21] European Parliament and Council Directive concerning measures for a high common level of security of network and information systems across the Union, 6 July 2016, Ref: 2016/1148/EU

[22] ISO/IEC Standard on Information technology - Security techniques - Information security management systems - Requirements, October 2013, Ref: ISO/IEC 27001:2013

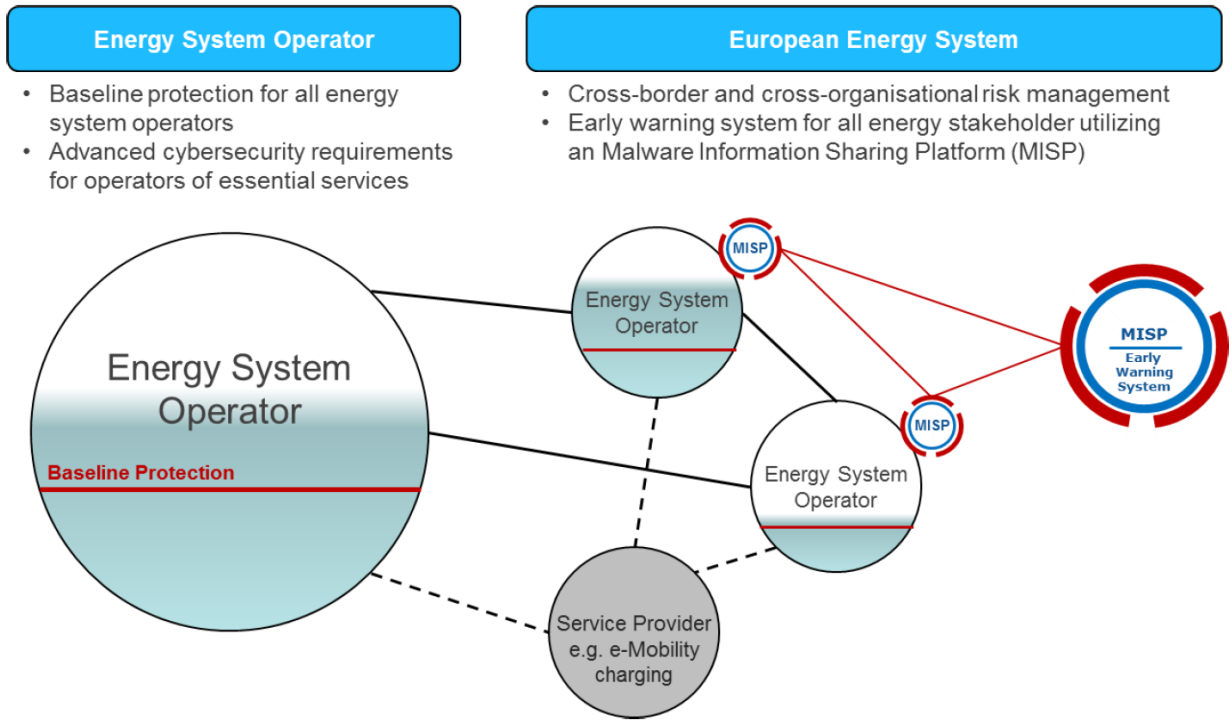

Figure 1 – Scope of the Network Code on Cybersecurity
(source SGTF EG2)

The European energy system is interconnected and interdependent. As an example, energy system operators have the need to interact directly or indirectly with other service providers such as e-mobility charging, photovoltaics or smart homes. Understanding and mitigating cyber risks that can cascade throughout this interconnected and interdependent network may go beyond the scope of individual energy system operators. Such cross-border and cross-organisational risks are recommended to be addressed by ENTSO-E and the EU-DSO entity as organisations which can encompass a broader range of expertise into the analysis. They may also offer the possibility to formulate cybersecurity recommendation to stakeholders that cannot directly be addressed by a Network Code.

The objective of the recommended Network Code on cybersecurity should not only address current cybersecurity risks, but support energy SOs in order to mitigate and protect their cyberspace against future threats and risks. Taking into consideration the fast and unpredictable evolution of cyber threats, this can only be properly addressed with an early warning system. This may be built on the already-existing infrastructure and communication systems provided by the implementation of the NIS Directive in the MS. A so-called Malware Information Sharing Platform (MISP) is recommended to be established and supported by the MS for collaboration and cooperation across public and private organisations, MS and other international allies and partners. OSE are recommended to actively participate in such early warning system.

Further supportive elements recommended are sector-specific guidance for operators on the implementation of crisis management and on the security of the supply chain, and a tool to support mature organisations to steer cybersecurity implementation by assessing the actual status of implementation.

All the recommended actions are based on principles to address cybersecurity in a holistic and risk-based approach that offers operators freedom in the implementation in order to address organisation-specific operational needs. Additionally, harmonisation requirements are provided that allow the achievement of a minimum protection level across Europe.

The recommendation outlined in the SGTF EG2 report can be summarised as follows:

Baseline Protection for Energy SOs

- Set-up of an Information Security Management System (ISO/IEC 27001:2013) with consideration of ISO/IEC 27002:2013[23] and ISO/IEC 27019:2017[24]; and
- Minimum security requirements protecting the EU Energy System (using the EU Cybersecurity Act[25]).

Advanced Cybersecurity Implementation for Energy System Operators of Essential Services

- Protection of current infrastructure;
- Supply chain risk management process;
- Protection against cross-border and cross-organisational risks through proper analysis and risk treatment; and
- Active participation in an early warning system.

Supportive Elements and Tools

- Sector-specific guidance on crisis management for operators;
- Sector-specific guidance on supply chain security for operators; and
- Energy cybersecurity maturity framework (a tool to assess maturity and to steer cybersecurity implementation).

Cybersecurity is not a one-time action plan, but a continuous effort that requires different stakeholders to cooperate and collaborate to achieve a resilient energy infrastructure. The recommendations provided in the SGTF EG2 report support this effort by providing direction and guidance.

[23] ISO/IEC Standard on Information technology - Security techniques - Code of practice for information security controls, October 2013, Ref: ISO/IEC 27002:2013

[24] ISO/IEC Standard on Information technology - Security techniques - Information security controls for the energy utility industry, October 2017, Ref: ISO/IEC 27019:2017

[25] European Parliament and Council Regulation on the European Union Agency for Cybersecurity (ENISA) and on information and communications technology cybersecurity certification, 17 April 2019, Ref: 2019/881/EU (EU Cybersecurity Act)

Annex 3 – About CEER

The Council of European Energy Regulators (CEER) is the voice of Europe's national energy regulators. CEER's members and observers comprise 39 national energy regulatory authorities (NRAs) from across Europe.

CEER is legally established as a not-for-profit association under Belgian law, with a small Secretariat based in Brussels to assist the organisation.

CEER supports its NRA members/observers in their responsibilities, sharing experience and developing regulatory capacity and best practices. It does so by facilitating expert working group meetings, hosting workshops and events, supporting the development and publication of regulatory papers, and through an in-house Training Academy. Through CEER, European NRAs cooperate and develop common position papers, advice and forward-thinking recommendations to improve the electricity and gas markets for the benefit of consumers and businesses.

In terms of policy, CEER actively promotes an investment friendly, harmonised regulatory environment and the consistent application of existing EU legislation. A key objective of CEER is to facilitate the creation of a single, competitive, efficient and sustainable Internal Energy Market in Europe that works in the consumer interest.

Specifically, CEER deals with a range of energy regulatory issues including wholesale and retail markets; consumer issues; distribution networks; smart grids; flexibility; sustainability; and international cooperation.

CEER wishes to thank in particular the following regulatory experts for their work in preparing this report: Stefano Bracco; Frédéric-Michael Foeteler; Pierrick Muller; Roman Picard.

More information is available at www.ceer.eu.