ENERGY EXPERT CYBER SECURITY PLATFORM

Cyber Security in the Energy Sector

Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector

EECSP Report
February 2017

The mission of the EECSP-Expert Group is to provide guidance to the Commission on policy and regulatory directions at European level, addressing the energy sector key points including infrastructural issues, security of supply, smart grids technologies and nuclear.

Contents

1. Introduction 5
1.1 European Cyber Security Framework 5
1.2 Context 5
1.3 Acknowledgements 6
1.4 Disclaimer 6
2. Acronyms and Abbreviations 7
3. Executive Summary 9
4. EECSP – Mission and Approach 12
4.1 Analysis Approach 12
5. Cyber Security in the Energy Sector 14
5.1 Subsectors: Electricity, Oil and Gas and Nuclear Energy 14
5.2 The Energy Sector – Changes in the Infrastructure 15
5.3 The Energy Sector – Changes in the Market 16
5.4 The Energy Sector – Changes in Cyber Security 17
5.4.1 Grid Stability in a Cross-Border Interconnected Energy Network 18
5.4.2 Protection Concepts Reflecting Current Threats and Risks 19
5.4.3 Handling of Cyber Attacks within the EU 20
5.4.4 Effects by Cyber Attacks not Fully Considered in the Design Rules of an existing Power Grid or Nuclear Facility 22
5.4.5 Introduction of New Highly Interconnected Technologies and Services 23
5.4.6 Outsourcing of Infrastructures and Services 24
5.4.7 Integrity of Components Used in Energy Systems 24
5.4.8 Increased Interdependency among Market Players 25
5.4.9 Availability of Human Resources and Their Competences 25
5.4.10 Constraints Imposed by Cyber Security Measures in Contrast to Real-Time/Availability Requirements 25
5.5 Conclusion of Challenges in the Energy Sector 26
6. A Sectoral Approach for the Energy Sector 27
6.1 Identification of Strategic Areas for the Energy Sector 27
6.1.1 European Threat and Risk Landscape and Treatment 27
6.1.2 Identification of Operators of Essential Service 28
6.1.3 Cyber Response Framework 28
6.1.4 Crisis Management 29
6.1.5 European Cyber Security Maturity Framework 29

6.1.6 Supply Chain Integrity Framework for Components 30
6.1.7 Capacity and Competence Build-Up 30
6.1.8 Best Practice and Information Exchange 30
6.1.9 Foster International Collaboration 31
6.1.10 Awareness Campaign from Top-Level of EU Institutions 31
6.1.11 Overview of the Strategic Areas 31
6.2 Reflection of Strategic Areas to the Energy Subsectors 32
6.3 Strategic Framework for the Energy Sector 35
7. Policies and Regulations of the European Union 37
7.1 Digital Single Market (DSM) Strategy 37
7.2 Contractual Public Private Partnership (cPPP) 37
7.3 EU Cyber Security Strategy 38
7.4 European Agenda on Security 38
7.5 Directive on Security of Network and Information Systems (NIS) 39
7.6 European Programme for Critical Infrastructure Protection (EPCIP) Directive & European Critical Infrastructure (ECI) Directive 41
7.7 Security of Supply (SOS) Directive 42
7.8 Clean Energy for all Europeans – Commission Proposal 20th Nov. 2016 43
7.9 Security of Gas Supply Regulation 43
7.10 EURATOM 43
7.11 The General Data Protection Regulation (GDPR) 44
7.11.1 Data Protection Impact Assessment (DPIA) Template 45
7.12 National Cyber Security Strategies 45
7.13 Summary on Policies and Regulations 46
8. Gaps in Policy and Legislation 48
8.1 European Threat and Risk Landscape and Treatment 48
8.2 Identification of Operators of Essential Services 51
8.3 Cyber Response Framework 52
8.4 Crisis Management 53
8.5 European Cyber Security Maturity Framework 54
8.6 Supply Chain Integrity Framework for Components 55
8.7 Capacity and Competence Build-Up 56
8.8 Best Practice and Information Exchange 56
8.9 Foster International Collaboration 57

8.10 Awareness Campaign from Top-Level of EU Institutions 58
8.11 Consolidation of Gaps and Mapping to Subsectors and Nuclear Energy 58
9 Recommendation on Actions for the European Commission 64
9.1 Set-Up an Effective Threat and Risk Management System 64
9.2 Set-Up an Effective Cyber Response Framework 66
9.3 Continuously Improve Cyber Resilience 67
9.4 Build-Up the Required Capacity and Competences 67
9.5 Mapping of Recommended Actions to the Identified Gaps 69
9.6 Remarks on Recommendations 69
10. Conclusion 71
11. Annex 72
11.1 Annex A-1: Energy Expert Cyber Security Platform - Expert Group 72
11.2 Annex A-2: Editorial Team 74

1. Introduction

1.1 European Cyber Security Framework

The digitalisation of industry, including energy, is at the core of all major Commission initiatives such as the Digital Single Market, the Energy Union package and the Single Market strategy. These initiatives aim to create the right framework conditions to accompany the transformation of our markets, processes, actors and to provide consumer benefits in this digitalisation trend.

One of the major challenges accompanying this trend is the need to ensure appropriate cyber security for operators, market participants and consumers. In this respect, the European Agenda on Security 2015-2020[1] adopted in April 2015 and the Digital Single Market Communication[2] of 6 May 2015 stress the need for a common approach to address cyber threats across Europe, building on the existing Cyber Security Strategy of the European Union launched in 2013[3].

In December 2015, the European Parliament and the Council reached an agreement on the Commission's proposed measures for security of network and information systems (NIS Directive)[4] and on the data protection reform[5]. These measures established a modern and harmonised protection framework across the EU. The Directive on security of Network and Information Systems (NIS) is the first piece of European-wide legislation on cyber security. Its provisions aim to make the online environment more trustworthy and therefore support the smooth functioning of the EU Digital Single Market. The General Data Protection Regulation[6] is an essential step to strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the Digital Single Market. These two legislations, adopted in the second half of 2016, create a new framework for handling cyber security and data protection in the EU.

1.2 Context

The Commission under the lead of DG Energy is preparing a strategy on cyber security for the whole energy sector to reinforce and to complement the implementation of Directive on security of Network and Information Systems (NIS) at energy sector level and also to foster synergies between the Energy Union and the Digital Single Market agenda.

In this respect, the Energy Expert Cyber Security Platform (EECSP) - Expert Group started work in December 2015. This document reflects the work of this Expert Group towards the development of

[1] COM(2015) 185 final

[2] COM (2015) 192 final (pp. 13, 20) and the accompanying SWD (2015) 100 final (pp. 47-51).

[3] The Strategy of the European Union set up in 2013 a public-private cross-sectoral platform on security of Network and Information Systems (NIS Platform) to contribute to Commission recommendations on good cyber security practices, in particular on risk management, information sharing and incident notification.

[4] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ; and Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

[6] Regulation (EU) 2016/679

an energy cyber security strategy by analysis of respective cyber security challenges and existing policy papers with the aim to recommend actions for consideration by the European Commission.

Chapter 3 provides an executive summary highlighting the key analysis results and recommended actions. The approach and methodology to derive these recommendations from the EECSP-Expert Group is described in detail in chapter 4. Chapter 5 gives a detailed view on the challenges in the energy sector as viewed by the EECSP-Expert Group. These has lead to a set of strategic areas that need to be addressed by the energy sector; the strategic ares are described in chapter 6. Chapter 7 summarizes the existing policy landscape in cyber security for the energy sector at European Union level. These policy papers were analysed in the context of the strategic areas identified in order to identify gaps in the existing policy which are provided in chapter 8. A set of recommended actions to be considered by the European Commission are shown in chapter 9.

1.3 Acknowledgements

This report has been prepared by the Energy Expert Cyber Security Platform (EECSP) - Expert Group and is a product of intensive work and discussions among the experts from December 2015 until December 2016. Special thanks are due to all the experts (see Annex A-1) who have contributed in the course of this work and especially to the Editorial Team (see Annex A-2).

1.4 Disclaimer

2. Acronyms and Abbreviations

The following acronyms and abbreviations are used in the report:

- **CERT** Computer Emergency Response Team
- **CIA** Confidentiality, Integrity and Availability
- **CIIP** Critical Information Infrastructure Protection
- **CIWIN** Critical Infrastructure Warning Information Network
- **CPPNM** Convention of Physical Protection of Nuclear Material
- **cPPP** Contractual Public Private Partnership
- **CSDP** Common Security and Defence Policy
- **CSIRT** Computer Security Incident Response Team
- **DoE** Department of Energy (US)
- **DPIA** Data Protection Impact Assessment
- **DSM** Digital Single Market
- **DSO** Distribution System Operator
- **EAEC** European Atomic Energy Community
- **EC** European Commission
- **ECI** European Critical Infrastructure
- **EC3** European Cybercrime Centre (EUROPOL)
- **EDA** European Defence Agency
- **EECSP** Energy Expert Cyber Security Platform
- **EP** European Parliament
- **EPCIP** European Programme for Critical Infrastructure Protection
- **ES-C2M2** Electricity Subsector Cybersecurity Capability Maturity Model
- **EU** European Union
- **GDP** Gross domestic product
- **GDPR** General Data Protection Regulation
- **IAEA** International Atomic Energy Agency
- **ICT** Information and Communication Technology
- **IEC** International Electrotechnical Commission
- **IoT** Internet of Things
- **IPCR** Integrated Political Crisis Response
- **IPPAS** International Physical Protection Advisory Service
- **ISAC** Information Sharing and Analysis Center
- **IT** Information Technology
- **LNG** Liquefied Natural Gas
- **NATO** North Atlantic Treaty Organization
- **NCA** National Competent Authority
- **NIS** Network Information Security
- **NRA** National Regulatory Authority
- **NMAC** Nuclear Material Accounting and Control
- **NTI** Nuclear Threat Initiative

- **ONG-C2M2** Oil and Natural Gas Cybersecurity Capability Maturity Model
- **OSCE** Organisation for Security and Co-operation in Europe
- **OSP** Operator Security Plan
- **OT** Operational Technology
- **PLC** Programmable Logic Controller
- **RTU** Remote Terminal Unit
- **SCADA** Supervisory Control And Data Acquisition
- **SoS** Security of Supply
- **TSO** Transmission System Operator

3. Executive Summary

With the adoption of the Directive on security of Network and Information Systems (NIS)[7] and the General Data Protection Regulation (GDPR)[8] in 2016, the European Commission with its Member States is implementing the baseline for cyber security. This will support the EU Digital Single Market whilst protecting the interests of the European society and the functioning of essential services for the European citizens.

The framework of NIS Directive and GDPR represent a cross-sectoral approach, where no differentiation is made between sectors, but where the level of obligation is dependent only on the criticality of services provided. The Energy Expert Cyber Security Platform (EECSP) has been given the task by DG Energy to analyse whether the energy sector is sufficiently covered by existing legislation or if there is a need for more action to achieve an effective cyber security. The key questions for the energy sector are: Is energy different from any other sector in respect to cyber security? What are the challenges in the energy sector to be addressed? What are recommended actions to be taken in respect of cyber security once the NIS Directive and GDPR are fully implemented?

In trying to answer these three questions, the EECSP-Expert Group has identified ten cyber security challenges for the energy sector and nuclear energy. These are considered relevant in order to meet two high-level objectives which form the basis of the analysis in this report:

- Secure energy systems that are providing essential services to the European society.
- Protect the data in the energy systems and the privacy of the European citizen.

These two high-level objectives are important as they are defining the goal of what should be achieved by stakeholders in the energy sector (electricity including nuclear energy, oil, and gas).

In order to address those questions, the EECSP-Expert Group has identified the cyber security challenges and strategic areas in the energy sector where a sectoral approach is needed. An analysis of these strategic areas concerning coverage in EU policies and regulations has identified 39 gaps not covered by existing legislations. These gaps must be closed in order to achieve a sufficient level of assurance of cyber security in the energy sector. This has led to detailed recommended actions for the European Commission.

While the group believes that most subsectors of the energy sector already have some measures in place, this must be supported by a formalized and effective *threat and risk management system*. On this strategic priority, the main actions the EECSP-Expert Group would advise to **pursue a harmonized, structured and comprehensive way to identify operators of essential services for the energy sector at EU level**. This shall be supplemented by a **structured risk analysis and risk treatment plan specific for the highly interdependent European energy sector**. Finally, it may be enriched and completed by the establishment of two parallel frameworks: one that aims to establish acceptable and efficient governance, at the of which is **regional cooperation on cyber security topics** and the other, to allow the **controlled and secure disclosure of vulnerabilities and incidents**

[7] Directive (EU) 2016/1148
[8] Regulation (EU) 2016/679

affecting the energy sector in its crucial role which helps to meet the need for effective communication.

The second strategic priority is to establish an *effective cyber response framework* which will enable a fast and coherent response in case of an emergency linked to cyber security. To achieve the advised strategic priority would include work to **define and implement a cyber response and coordination framework** specifically focused on the energy sector and which may take into consideration the central role of energy in a digital society. At the same time action should be taken to ensure the **implementation and the strengthening of regional cooperation for efficient handling of cyber emergencies when energy is involved and affected**.

A third strategic priority is focused on the organisational readiness and protection of the energy sector by addressing the need to *improve cyber* resilience in the energy sector. To reach this goal, the EECSP-Expert Group suggests establishing a **European cyber security maturity framework** designed specifically for the energy sector. This must be undertaken in parallel with the establishment of a **cPPP for supply chain integrity** to allow public institutions and energy industry to discuss viable solutions to the unresolved issue of assuring integrity in a complex and continuously evolving supply chain. In addition, Europe has to **foster internal coordination and pursue international cooperation**, as this is the best way to involve the EU actors in cyber security for energy, as well as, a way to strengthen international alliances. The ultimate goal is to learn from others and to provide knowledge to those who want to cooperate across the international landscape.

As a last priority, the EECSP-Expert Group recommends addressing the problem of having resources available with the right skills. In this context, Europe should add the strategic priority to *build-up the adequate capacity and competences* in cyber security for the energy sector. The lack of specialized resources, and the lack of specific skills can be addressed by the creation of human and technical capacity to address cyber security in the energy sector: **building competences** that are today insufficiently available, and **providing knowledge**, to those willing to address cyber security in the energy sector, **promoting research** where it is not sufficient in terms of quantity and quality, may create the right conditions to provide an answer to this last strategic priority in the near future.

In conclusion, there is no easy way to answer to those questions: the NIS Directive is seen as a baseline applicable to cyber security for critical infrastructures with a focus on measures such as the implementation of CSIRTs within the Member States and cooperation via a CSIRT network. It is clear that any additional regulation and legislation should be built upon the frameworks established by the NIS Directive and GDPR, and should complement them as much as possible. The proposed actions may be of inspiration for future activities and legislative proposals that the European Commission may put forward. The EECSP-Expert Group would welcome and advise the use of the regional cooperation model (see chapter 9.1) for the implementation of the proposed actions, as it is seen as a promising model with a strong chance of success by taking advantage of the already existing cooperation. In this regard, further need on coordination and guidance by the European Commission and specifically EURATOM for the case of nuclear energy is recommended and proposed in this report.

Table 1 summarizes the strategic priorities linked to the strategic areas and the areas of actions, which are explained in detail later in this report.

Strategic Priorities		Strategic Areas	Areas of Actions
I	Set-up an effective threat and risk management system	European threat and risk landscape and treatment	(1) Identification of operators of essential services for the energy sector at EU level. (2) Risk analysis and treatment. (3) Framework of rules for a regional cooperation. (4) EU framework for vulnerabilities disclosure for the energy sector.
		Identification of operators of essential services	
		Best practice and information exchange	
		Foster international collaboration	
II	Set-up an effective cyber response framework	Cyber response framework	(5) Define and implement cyber response framework and coordination. (6) Implement and strengthen the regional cooperation for emergency handling
		Crisis management	
III	Continuously improve cyber resilience	European cyber security maturity framework	(7) Establish a European cyber security maturity framework for energy. (8) Establish a cPPP for supply chain integrity (9) Foster European and international collaboration
		Supply chain integrity framework for components	
		Best practice and information exchange	
		Awareness campaign from top level EU institutions	
IV	Build-up the required capacity and competences	Capacity & competence build-up	(10) Capacity and competence build-up.

Table 1: Overview table on strategic priorities, areas and recommended actions

Finally, a key success factor in achieving these goals is the ability and willingness of different stakeholders to cooperate and collaborate in this effort. We operate in a complex and diversified sector, where roles and responsibilities may unexpectedly change as a result of the ongoing smart evolution of the energy sector, which looks to a secure digital world as a crucial element for its own existence and its further evolution.

4. EECSP – Mission and Approach

The mission of the EECSP-Expert Group is to provide guidance to the European Commission on policy and regulatory directions at European level, addressing the energy sector key points including infrastructural issues, security of supply, smart grids technologies and nuclear.

The energy sector is defined by the European Commission[9] as the sector build by the three subsectors: electricity[10], oil and gas. The scope of the work, for this report, is the energy sector including nuclear energy. Nuclear energy[11] in this report means the civil nuclear energy fuel cycle[12] as part of Member States' operators of essential services according to the Directive (EU) 2016/1148.

The EECSP-Expert Group has analysed the challenges in the energy sector with the target to identify strategic areas where a sectoral approach for the energy sector is needed. The identified areas are then used for an analysis on existing policies and regulations in order to derive recommendations for the European Commission. The following section will describe in more detail the approach used for the analysis.

4.1 Analysis Approach

In line with the mission of the EECSP-Expert Group and based on the expertise of 14 international cyber security experts from the IT, telecommunications, electricity and nuclear sector, the following approach and steps were performed, see Figure 1:

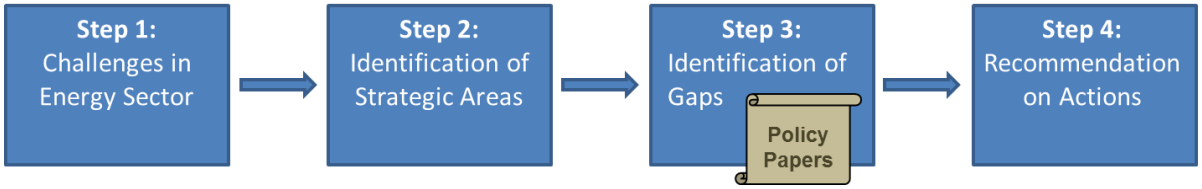

Figure 1: Overview of analysis approach

[9] NIS Directive, Annex II: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013PC0048&from=EN

[10] Included in the analysis work is electricity generation that is not explicitly included/excluded by the definition of the subsector. See chapter 7.5 for more details on the definition of operators of essential services.

[11] Nuclear energy has to be considered as highly regulated and internationally harmonized in the fields of safety and safeguards by legally binding instruments. In general, nuclear security remains to be Member State's responsibility. EURATOM has actually no mandate to regulate nuclear security and the IAEA has neither. But the IAEA relies now on the 2005 Amendment of the Convention of Physical Protection of Nuclear Material (CPPNM, https://www.iaea.org/publications/documents/conventions/convention-physical-protection-nuclear-material) which entered into force on 8th May 2016. This does not automatically imply that the IAEA guidance documents on cyber security legally binding but most IAEA member states include this in their national guidance and regulation. This report follows the view of the IAEA by categorizing cyber security as part of nuclear security. Having in mind that the CPPNM Amendment was adopted in 2005 and addresses physical protection, it could not have been considered new types of cyber risks and necessary principles deriving from them. This report instead, focusing on gaps and future actions on NIS, addresses new developments and risks in the field of cyber in energy, including nuclear.

[12] Nuclear fuel cycle includes the stages from Uranium mining/extraction to conversion, enrichment, fuel fabrication, use of the fuel in reactors, interim storage of the spent fuel, reprocessing and final waste disposal.

Step 1: Cyber security in the energy sector

The starting point of the analysis has been a description of challenges in the energy sector that need to be addressed. In order to derive the challenges in the energy sector, high-level objectives have been agreed, which are expected to be common targets among all stakeholders in the energy sector. Today's energy infrastructure and market have been reflected against these high-level objectives and challenges have been derived accordingly. The challenges described are based on an operational view point, i.e. they reflect challenges in daily operation but do not necessarily imply that support from a governmental authority is required to overcome these challenges as some may be solved with other means. The analysis and the results are presented in chapter 5.

Step 2: A sectoral approach for the energy sector

To address the challenges found in step 1, strategic areas have been agreed by the EECSP experts. These are areas where the EECSP experts do not believe that the industry itself can independently resolve the issues and therefore recommend support and actions from the European Commission. The strategic areas are reflected to the respective subsectors electricity, gas, oil and nuclear energy and categorized into strategic priorities in order to provide a cyber security strategy framework for the energy sector in the EU. The findings of this analysis are presented in chapter 6.

Step 3: Gaps in Policy and Legislation

A variety of policies and legislation exist in the EU addressing cyber security and digitalisation for the energy sector that are relevant for the analysis performed. Chapter 7 provides an overview on the major policy and legislation papers. EECSP experts have analysed respective policy papers on coverage of the identified strategic areas. The comparison between the identified areas and the existing policies and regulations reveal the gaps in the scenario of the existing policies and regulations with the target set to meet the high-level objectives as agreed in step 1 of this analysis approach. The analysis and results are presented in chapter 8.

Step 4: Recommendation for the European Commission

Based on the gaps found in step 3, the EECSP experts have defined recommendations on actions, see chapter 9, for the European Commission to close the gaps in a sectoral approach for the energy sector.

5. Cyber Security in the Energy Sector

Critical infrastructures provide essential services that underpin the smooth functioning of a modern society and serve as the backbone for the economic activities. These critical infrastructures include the energy, telecommunication, finance, health, and transport sectors. The energy infrastructure is arguably among one of the most complex and critical infrastructures as these other sectors depend upon it to deliver their essential services. Therefore, unavailability in supply of energy has a high potential impact on economy and proper functioning of the civil society that can last longer than the time of the incident itself. A potential disruption for a long period of time could affect the society, industry and trade with a high risk of impact on the gross domestic product (GDP)[13]. However, it must be noted that such level of threat has not yet materialized within the European Union.

The criticality of the energy sector and the possible high impact on economy and society in case of a wide disruption caused by potential cyber incidents and attacks are well understood and agreed among stakeholders[14,15]. As a consequence, two high-level objectives have been defined as a common ground among the EECSP-Expert Group and used as a base for the analysis in this report:

High-level objectives

- Secure energy systems that are providing essential services to the European society.
- Protect the data in the energy systems and the privacy of the European citizen.

These high-level objectives are common among stakeholders as they reflect the need to protect the energy systems and the data needed to efficiently operate those systems or needed to support flexibility use cases for the European citizens.

5.1 Subsectors: Electricity, Oil and Gas and Nuclear Energy

Challenges can be applied to all subsectors, namely electricity, oil and gas and the nuclear energy. However, the criticality differs from subsector to subsector. For the purpose of this analysis, challenges which are not considered critical by the EECSP experts have not been linked to the respective subsector. The following criteria have been taken under consideration:

- Importance for the European society and potential economic impact.
- Potential national or cross-border impact related to the 'weakest link problem'.
- Prospects of respective level to address the challenges.
- Real-time and dependence on availability requirements.

Importance for the European society and potential economic impact

The potential impact on the society and economy defines the importance of the challenges. For example, a challenge that can result in a blackout spanning several regions or a high density population or industrial area should be treated differently than a challenge where the impact is limited to a single rural area.

[13] Emerging Risk Report – 2015, Business Blackout, Lloyd's and the University of Cambridge Centre for Risk Studies

[14] See for example recital (2) of NIS Directive: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013PC0048&from=EN

[15] World Energy Council Perspectives – The road to resilience, 2016, page 7: ‚Cyber-attacks in the energy sector have an impact not only on the sector itself, but on the wider economy and the whole fabric of a state'

Potential national or cross-border impact related to the 'weakest link problem'

The energy grid is interconnected. A challenge is not limited to an operator or a Member State anymore in case of transboundary impacts. A well-known issue in cyber security is the weakest link-problem that indicates that an interconnected system is just as robust as the weakest part of it. Therefore, challenges with a potential national or cross-border impact have to be analysed and rated differently. Furthermore, even challenges causing only a regional direct impact might have collateral adverse effects on other Member States.

Prospects of respective level to address the challenges

A challenge might be solved on organisational, national or EU level. This criterion considers the capabilities of respective level to handle or solve a challenge.

Real-time and dependence on availability requirements

Real-time and availability criteria indicate the expected reaction time in case a challenge causes an impact. This might range from milliseconds (e.g. nuclear energy and electricity) to days in other subsectors. In this context, criticality is defined by the available response time to react to an incident.

Taking these criteria into consideration, it is obvious, that there will not be a 'one size fits all' recommendation for all subsectors, and that not all challenges needs to be addressed on the same level for all subsectors. It can be pointed out that the potential impact of the subsector oil and gas in regard of these challenges are rather national than European. In those cases, where countries, which are heavily depending on oil or gas for the electricity energy production, running out of supply, the time available to respond would still allow a controlled disconnection of these areas in order to keep the rest of the grid running stable e.g. by activation of alternative supply sources. Even in such extreme situation, the EECSP experts believe that each Member State would be able to get such situation under control. Therefore, criticality and potential impact indicates that for the oil and gas subsector, limited support from EU level is required at this stage from a technical view point.

Looking at the electricity subsector and nuclear energy, the picture looks different: high potential impact on economy, criticality for the European society, cross-border and weakest link problem, strong real-time and availability requirements. Most challenges will have limited chances to be solved on national or operator level.

5.2 The Energy Sector – Changes in the Infrastructure

Digital technologies are playing an increasingly important role in the energy sector. A smarter energy system can perform power generation, transmission, network management and market related tasks with better precision and faster response times than a human-dependent system, thereby optimising energy management, prioritizing usage, and setting policies for quick response to outages.

Energy control systems include a hierarchy of interconnected physical and electronic sensing, monitoring, and control devices, mostly acting in real-time and typically connected to a central supervisory station or a control centre. Control systems encompass supervisory control and data acquisition (SCADA) systems used to monitoring and control operations that in case of energy transport and distribution networks are widely dispersed. Distributed control systems (DCS) are used for single facilities or small geographical areas. Control systems are connected to remote

components such as remote terminal units (RTU) and programmable logic controllers (PLC) that monitor system data and initiate programmed control activities in response to input data and alerts. SCADA systems collect, display and store information from remotely located data collection transducers, sensors, control equipments, devices and automated functions. They form part of the process control systems that are used to manage in real-time, for example, the transmission and distribution of electricity or transmission and distribution along gas pipelines.

In generation systems, the processes of producing energy have to be controlled. Burning of oil, coal or gas and also nuclear fission processes generate heat which is used to run turbines. These turbines produce energy and the whole production process is controlled by analog and/or digital systems which are connected to a main control room where people monitor the processes. Renewable resources (wind, solar, hydro) are systems which are highly interconnected with each other and their energy production is controlled by central stations that considers the natural intermittent behaviour of renewable resources such as wind and solar.

Currently, the energy sector consists of both legacy and next generation technologies. New technologies are introducing new intelligent components (e.g. electricity or gas meters, digital valves or pumps) to the energy infrastructure that communicate in more advanced ways (two-way wired and wireless communications) than in the past. These new components are typically based on information and communication technology (ICT) that can be interconnected to local networks. Typically, 'analog' components are replaced by new digital systems as spare parts are not available anymore or obsolete.

Ensuring resilience of the energy supply systems against cyber risks and threats are becoming increasingly important as wide-spread use of ICT and data communication is becoming the foundation for the functioning of infrastructures underlying the energy systems.

The increased efficiency in supply services comes with a price: increased exposure to cyber incidents and attacks. In a cross-sector manner, these threats apply to all - generation, transmission, distribution and process technologies, and to energy market services. The digitalisation of the energy sector also raises the question of how to face the risks and threats of cyber incidents and attacks affecting personal data and strategic energy infrastructure data, which are sometimes crucial for the security of the energy supply.

5.3 The Energy Sector – Changes in the Market

The energy market is changing tremendously. With the increasing shift towards renewable energy and the introduction of digitalisation technologies, new generations of market players appeared using applications with a high degree of integration between demand and supply, e.g. virtual power plants. European citizens are becoming energy producers that can be managed virtually by new operators through the cloud. New market players emerged, such as aggregators and third parties managing demand and supply with a scale of many users. On the other side, demand response is used by utility planners and operators as resource options for balancing supply and demand on the grids. Such programs can lower the cost of electricity in wholesale markets, and as a consequence, lead to lower retail rates. Demand response programs are an increasingly valuable resource options for capacity expansion in grid modernisation.

With a changing generation mix, grid stability increasingly requires real time control. Renewable resources have an intermittent behaviour by nature. Flexibility and a possible short-time demand increase might require production of electric power itself with e.g. turbogas systems. This reflects the interdependency of electricity and gas networks as a building block to support grid stability.

Additionally, the broad deployment of renewable resources leads to a more dynamic pricing of electricity products. Changes in the energy market by dynamic pricing and new market players, e.g., aggregators controlling new flexible loads (e.g. electric vehicle charging, demand response), are offering new options for energy supply. This changing market environment is enabled with more digital interaction among market participants. With the active role of the consumer in the energy demand and supply by the use of renewable technology such as photovoltaic or storage, new technology applications and business models are reshaping the energy market and providing availability of new low variable cost opportunities for the market.

5.4 The Energy Sector – Changes in Cyber Security

The focus of cyber security in the energy sector is to support the reliability and resilience even in the event of a cyber attack. Unlike IT systems, a control system in the energy sector that is under attack cannot be easily disconnected from the network as this could potentially result in safety issues, brownouts or even blackouts.

In cyber security, three commonly accepted protection goals are defined: Confidentiality, Integrity and Availability (CIA). In the energy sector, the highest priority objective depends on the industry specific applications. For example, in generation and transmission, availability and integrity are the most important. Altered or delayed data could result in misconfiguration of a device that eventually could impact system reliability. For the advanced metering infrastructure, confidentiality of customer personal data is the most critical. In nuclear, cyber security, named as computer security, is part of the nuclear security[16]. The protection goals of computer security are preventing cyber acts that could directly or indirectly lead to unauthorized removal of nuclear or other radioactive material, sabotage against nuclear material or nuclear facilities or theft of nuclear sensitive information.

The Ukraine power grid attack[17] in 2015 demonstrated the potential impact of cyber attacks to the electricity subsector. With the growing use of digital devices and more advanced communications, the overall cyber risk has increased. For example, as substations are modernized, the new equipment is digital, rather than analog. These new devices include commercially available operating systems, protocols, and applications that provide a larger attack surface. This in combination with interconnectivity increase the complexity of addressing respective cyber risks and gives opportunities to potential adversary on cyber attacks. More examples on attacks on the energy sector can be found in a report of the World Energy Council[18] with examples in various subsectors of

[16] The prevention and detection of and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities. (IAEA GOV/2005/50)

[17] Analysis of the Cyber Attack on the Ukrainian Power Grid**,** Defense Use Case, March 18, 2016, SANS ICS and E-ISAC.

[18] World Energy Council Perspectives – The road to resilience, 2016

the energy sector. Examples for the nuclear domain can be found in reports from NTI[19] and Chatham House[20].

Threat agents are ranging from state actors to non-state actors, script-kiddies, disgruntled employees, experienced hackers and hacker groups, organized crime, hacktivists and terrorists. There are also non-malicious cyber security events, such as user/administrator errors or technical faults[21], which looks the same or may eventually have the same effect as a coordinated attack. Regardless of the source of a cyber security incident, the potential impact to the energy sector is similar, e.g. brownout, blackout, or misconfiguration of control systems.

With the ongoing changes of the energy sector as described in chapter 5.2 and 5.3, cyber security has to keep pace with increasingly sophisticated cyber threats.

Challenges in cyber security specific to the energy sector found by the EECSP experts are the following:

1. Grid stability in a cross-border interconnected energy network.
2. Protection concepts reflecting current threats and risks.
3. Handling of cyber attacks within the EU.
4. Effects by cyber attacks not fully considered in the design rules of an existing power grid or nuclear facility.
5. Introduction of new highly interconnected technologies and services.
6. Outsourcing of infrastructures and services.
7. Integrity of components used in energy systems.
8. Increased interdependency among market players.
9. Availability of human resources and their competences.
10. Constraints imposed by cyber security measures in contrast to real-time/availability requirements.

The challenges are described in more detail in the following sections.

5.4.1 Grid Stability in a Cross-Border Interconnected Energy Network

This challenge is relevant for the subsector electricity, gas and nuclear energy. It is not considered relevant for oil, based on the criteria defined in chapter 5.1. The potential cross-border impact for the oil subsector is low and the real-time and availability requirements can be considered negligible. Potential incidents can be typically treated on organisational or national level.

The electricity grid and gas transport pipelines are strongly interconnected across Europe[22,23]. Energy reliability at the European level relies on trans-European connectivity. A failure in one energy system can have a potential cascading effect across regions as shown in a major European blackout in 2006

[19] http://www.nti.org/analysis/reports/cyber-security-nuclear-facilities-national-approaches/

[20] https://www.chathamhouse.org/about/structure/international-security-department/cyber-and-nuclear-security-project; https://www.chathamhouse.org/publication/cyber-security-civil-nuclear-facilities-understanding-risks

[21] In 2013, a misleading control command in an Austrian power grid has led to broadcast that flooded the communication network and has a similar look as an 'internal' DDoS attack.

[22] ENTSO-E Transmission System Map, https://www.entsoe.eu/map/Pages/default.aspx

[23] ENTSO-G System Map, http://www.entsog.eu/maps/transmission-capacity-map/2016

caused by a planned disconnection of a transmission line[24]. The inter-connectivity in Europe is not limited to EU Member States, as Non-EU countries such as Norway and Switzerland are connected to the European electricity network, too.

Reliability of the energy system depends also on natural gas facilities. The natural gas plays a key role in the EU's energy mix and gains importance as back-up fuel for variable electricity generation. Whereas the impact on the network stability in electricity is without delay transmitted across the energy grid, the potential impact from gas does not have these time constraints and is therefore less critical and rather regional. The presence of gas storage and LNG facilities makes a potential impact from gas even less likely.

Another aspect in the interconnected energy grid is the 'weakest link' problem, i.e. due to the potential cascading impact across regions, network operators with a low maturity in cyber security bear a higher potential risk on causing a cascading blackout than operators with a high maturity in cyber security.

By taking this interconnected energy network in a broader sense, power generation systems are to be considered, too. When for example countries such as UK depending on the gas supplied by Norway[25] or UK and Italy on the power provided by the French power generation plants[26,27], therefore, these subsectors are as well getting into the focus of network stability.

5.4.2 Protection Concepts Reflecting Current Threats and Risks

This challenge is relevant for the whole energy sector.

Traditionally, the investment cycles in the energy sector are following the life span of primary equipment such as transformers or generators with a life span from 15 up to 40 years. Secondary equipment used for automation and control has a life span up to 15 years.

Until recently, information and communications technology (ICT) were typically seen as supporting technologies for reliability of power systems. However, these technologies are increasingly becoming more critical to gurantee a desired level of reliability and resilience for the energy sector. The integration of ICT in energy sector systems is used for information exchange and automation since decades, but their usage has increased dramatically in recent years. ICT allows utilities to manage systems more interactively and therefore the new and existing (aging) infrastructure can be used more efficiently. While integrating ICT components is essential to modernize the energy sector and to realize its benefits, the same networked technologies add complexity and also introduce new inter-dependencies and potential vulnerabilities. New devices are subject to the same vulnerabilities as general purpose ICT devices, which typically have a shorter life span than the devices used by utilities.

[24] 2006 European blackout, https://en.wikipedia.org/wiki/2006_European_blackout

[25] In 2015, Norwegian gas imports were 61 per cent of total gas import: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/540923/Chapter_4_web.pdf

[26] Statistics on UK import on power: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/357534/Imports__exports_and_transfers_of_electricity.pdf

[27] Derived from TERNA report 2013(import on power from France) and nuclear power production in France (http://www.world-nuclear.org/information-library/country-profiles/countries-a-f/france.aspx)

Typically, protection concepts are prepared at the time of procurement of a system which may take under consideration the risks and threats known at this point in time. Threat and risks are evolving and those legacy systems and devices used in the network do not necessarily comply with up-to-date operational and/or security standards. This reflects one key challenge in energy systems today. Additionally, cyber security in a multi-vendor environment requires interoperability where components should rely on the same set of security standards and requirements used, but these requirements of course vary depending on the operational context.

Protection concepts have to cover various security capabilities of assets in a changing threat environment. Additionally, the widely used legacy (old) technologies in the network may not have an equivalent version on the market or may not be upgradable to meet state-of-the-art security requirements. Furthermore, 24/7 operations without maintenance windows due to high availability requirements on energy supply might lead to known vulnerabilities in legacy devices that are not always patched or mitigated. Outdated systems and proprietary technologies give additional concerns about the protection reflecting current risks and threats. This challenge affects generation, transmission and distribution and is present in all energy subsectors.

In nuclear energy, critical safety and security systems (for physical protection for example) used in nuclear facilities are isolated from internet and from IT networks. They are further protected by cyber security and physical security plans that are required by their respective national regulator[28]. In addition, nuclear power plants are designed to shut down safely should their systems detect a disturbance (for example a disturbance on the electricity grid). Even the nuclear sector is highly regulated and constantly inspected, not every country has already detailed regulations specifically for cyber security in nuclear facilities[29] in place.

5.4.3 Handling of Cyber Attacks within the EU

This challenge is relevant for the whole energy sector.

Cyber attacks do not respect geographical borders and an EU or nation-wide attack can have an EU-wide impact, see chapter 5.4.1. When talking about the handling of cyber attacks in the EU, one has to take into consideration several aspects:

- The capabilities to identify, detect, respond and recover from a cyber attack.
- The threat agents: state and non-state actors such as insider, script-kiddies, experienced hacker, hacker-groups, organized crime, hacktivists and terrorists.
- The different level of a handling: Operator, Member States, EU, diplomacy or military.
- Crisis management capabilities.
- Cyber response capabilities.
- Investigation of cyber attack capabilities and attribution of those attacks.

[28] Nuclear-relevant cyber threats are evaluated by Member States regulators via corresponding regulations that are typically based on experience built-up and shared by decades of work by the International Atomic Energy Agency (IAEA), a Vienna-based UN organisation. The IAEA has published computer security guidances and has included computer security as one of the areas of review in its inspection program for nuclear security named IPPAS.

[29] Cyber Security at Nuclear Facilities: National Approaches, Institute for Security and Safety, June 2015

An operator has to focus on his operational environment, to protect his systems, detect potential attacks and respond and recover on respective incidents. As shown in the Ukraine power grid attack[30], the attack has been undetected for a long period of time and only discovered after the strike by the attackers. With evolving threats, the capabilities to respond and recover on cyber incidents are getting more important.

An operator is typically not in a position to classify the threat agent without the support of the intelligence of a Nation State. Respective capabilities to identify, detect and respond are required on national level to support operators in case of sophisticated attacks. For coordinated attacks from non-state and/or state actors, a response structure for EU and Member States on cyber level as well as a coordinated response across EU and Member States (federal approach) might be appropriate.

As pointed out before, the threat and risk landscape is evolving while the number of potential vulnerabilities (most of times undetected) is increasing. Today, an early exchange of information about threats, risks and incidents specific to energy operations rarely exists. Information exchange arrangements with trustful relationships between multi-stakeholders are not sufficiently established between public and private sector as well as academia. Stakeholders playing a role in cyber security for energy will benefit of an in-time dissemination of critical and non-critical information.

Handling a serious cyber attack and responding adequately is a challenge as in most parts of EU rapid cyber response teams might not be available or well prepared to support the energy sector during or after a cyber attack on-site. Tasking a CSIRT with identifying the attacker and helping an operator remotely does not ensure that the operator's operational processes can survive over time. When an advanced cyber attack continues over a long period, as happened in Germany in 2012[31], the operator might need practical help, cyber response capabilities or diplomatic support to stop the attack to temporary mitigate the impact of the cyber attack. A coordination of all stakeholders cannot be assumed today.

Another important aspect on handling of cyber attacks in a Member State is crisis management. Crisis management depends strongly on communication capabilities for example between operators and governmental authorities. Ensuring that roles and responsibilities are clear and that communication is functioning in case of emergencies is therefore a critical part of a successful handling of crises.

Cyber response is a quite new topic addressing in extreme a case of an extensive cyber attack. Some legal frameworks[32] based on the Treaty of Lisbon exist at the EU level, which give the EU or its

[30] Analysis of the Cyber Attack on the Ukrainian Power Grid**,** Defense Use Case, March 18, 2016, SANS ICS and E-ISAC.

[31] The power operator 50Hertz has been attacked for 5 days with a DDoS that has affected Websites, external IT services and e-Mails; http://www.50hertz.com/Portals/3/Content/Dokumente/50Hertz/Finanzen/50Hertz-Geschaeftsbericht-2012.pdf

[32] Legislative Instruments for Collective Defence and Managing Crises:
http://eur-lex.europa.eu/summary/glossary/collective_defence.html
http://eur-lex.europa.eu/summary/glossary/european_security_defence_policy.html
http://eur-lex.europa.eu/summary/glossary/solidarity_clause.html
http://eur-lex.europa.eu/summary/glossary/mutual_defence.html
http://ec.europa.eu/echo/what/civil-protection/mechanism_en
https://eeas.europa.eu/topics/crisis-response_en

Member States a possibility to respond in crisis situations. However, these legal instruments have been set-up not considering potential extensive cyber attacks against the energy sector.

In the aftermath of an incident, the investigation takes place. Due to the priority in availability, the incident treatment in an operational environment differs from the treatment in a standard ICT environment. Even in case a system is clearly hacked, it will not be taken out of operation in order to allow evidence acquisition. Furthermore, if operation requires actions that may destroy or alter relevant information about the attack, operations will take the priority on the evidence acquisition process. Under this precondition, attribution of an attack is becoming more difficult due to the lack of information and/or evidentiary material.

As pointed out in this section, handling of cyber attacks and managing all the phases after a successful attack is a complex task among a variety of stakeholders and is one of the key challenges in cyber security which is relevant for the whole energy sector, including nuclear energy.

5.4.4 Effects by Cyber Attacks not Fully Considered in the Design Rules of an existing Power Grid or Nuclear Facility

This challenge is valid mainly for electricity subsector, including nuclear energy. It does not apply to oil and gas based on the criteria defined in chapter 5.1. The potential cross-border impact for the oil and gas subsector is lower and the real-time and availability requirements can be considered less critical, too.

The current energy sector has been designed and implemented to ensure the reliability of the sector, including redundancy and fall-back mechanisms to meet n-1 reliability criteria. It was never designed to withstand cyber attacks. This is valid for the whole electricity subsector, but it has to be noted that even power generation plants can be critical for the security of supply. However, it is expected that the n-1 reliability criteria will be effective in case only one power plant is going to stop working due to a cyber incident.

With standardized information and communication technology (ICT) components used in various systems and devices of an energy grid, vulnerabilities in one ICT components might cause common failures with a systemic impact on the grid. The design basis of the energy sector has not fully anticipated cyber security and can therefore not ensure the planned reliability in energy supply in case of specific events. However, it should be noted that the awareness in the sector is rising and that new installations and upgrades are typically considering cyber security with more adequate design rules.

In nuclear energy, a nuclear power plant has been designed and built to protect the environment against unintended release of nuclear material as well as against theft of nuclear material. Protection mechanisms as set in place in the past are mainly built against physical attacks and design rules that did not anticipate cyber security. EECSP experts have concerns that cyber security has not been fully anticipated in all Member States of the European Union as indicated by the NTI index[33].

[33] http://ntiindex.org/overview-highlights/cybersecurity/

5.4.5 Introduction of New Highly Interconnected Technologies and Services

This challenge is valid for the electricity subsector, but also affects the gas subsector in the sense, that the gas facilities getting increasingly automated and interconnected. The challenge does not apply to the oil subsector based on the criteria defined in chapter 5.1. The potential cross-border impact for the oil subsector is low and the real-time and availability requirements can be considered negligible. Potential incidents can be typically treated on organisational or national level. For nuclear energy, the challenge is not relevant, as for nuclear energy the use of new technologies is strictly controlled, verified and authorized by regulatory authorities before being introduced in a working environment.

The energy infrastructure is being modernized to increase energy and operational efficiency and reliability. The digitalisation in energy is driven by the growing use of renewable resources, storage, e-mobility, microgrids, distributed generation, etc. As a consequence, new grid technologies are introducing millions of novel, intelligent components to the energy sector that communicate in much more advanced ways (two-way communications with wired and wireless communications) than in the past, see chapter 5.2. Devices, which are based on standardized components with common vulnerabilities and a high number of potential attack points, are constantly added to the energy networks.

With the increased digitalisation of the energy sector, technology advances and trends have emerged such as:

- Integration of Internet of Things (IoT) in devices. These devices, including home appliances such as refrigerators, washing machines, etc., which were previously stand-alone and not accessible from the Internet.
- Cloud Services with 24/7 operation that requires automated status reporting and response.
- Analytics to effectively manage digital devices using ‘big data’ technologies to process the data.
- Expanded telecommunication infrastructures and networks with increased usage of mobile devices and fostered deployment of new applications.
- New applications with close integration of demand and response such as virtual power plants, microgrids or cloud management services for solar, building and home automation.

The increased complexity of the energy networks is reflected in the way energy and energy related information and data are used, shared, processed and controlled as well as communicated. On the one side, in case the management of the energy grid is increasingly dependent on availability and integrity of data services, the risk of data breaches in the context of data relevant for the grid has to be well understood. On the other side, energy data used for energy services which are relevant for data privacy has to be considered as well. In this context, the challenge is the transition towards ‘digital’ utilities which are becoming increasingly data driven and where ‘big data’ analytics will become part of their primary processes. In this context, adding new technologies and services into a network requires a high attention on cyber security risks and on the competences in addressing such in a changing environment.

5.4.6 Outsourcing of Infrastructures and Services

This challenge is relevant for the subsector electricity, gas and nuclear energy. It is not considered relevant for oil, based on the criteria defined in chapter 5.1. The potential cross-border impact for the oil subsector is low and the real-time and availability requirements can be considered negligible. Potential incidents can be typically treated on organisational or national level.

Operational efficiency by the use of new services, see section 5.4.5, and the increased cost pressure by declining wholesale prices in energy has led to a growing demand on data services (e.g. cloud based) and dedicated telecommunication networks. By doing this, the high reliable energy sector is becoming dependent on other sectors with lower requirements on availability and integrity. For the energy sector, it is important to have clear defined levels on quality of service such as latency and real-time in place in order to support availability and the control of the energy services. Outsourcing of infrastructures and services requires appropriate consideration and rules to manage the risks.

As the protection and the robustness of these services often remains unclear, another aspect of outsourcing is the strategic aspect on national security in case critical infrastructure components and services are outsourced outside a country as this might impact sovereignty in case of conflicts.

In nuclear energy, because of the tremendous costs of a nuclear unit (5-10 bn EUR), new operational models came up for new built nuclear power plants. Vendors offer in between an outsourced build and run-model for nuclear power plants[34]. With that, remote access or control of operational functions might be implemented and is eventually in the hands of the vendor.

5.4.7 Integrity of Components Used in Energy Systems

This challenge is relevant for the subsector electricity, gas and nuclear energy. It is not considered relevant for oil based on the criteria defined in chapter 5.1. The potential cross-border impact for the oil subsector is low and the real-time and availability requirements can be considered negligible. Potential incidents can be typically treated on organisational or national level.

With the potential risk of sophisticated attacks, in particular from state actors, another relevant challenge is the protection against corrupted components which might have hidden functions or access (backdoor) capabilities included. Backdoors or hidden functions are extremely difficult to discover and might therefore be the source of a key challenge for the energy sector, particular for the electricity and gas subsector as well as for nuclear energy. As cyber warfare uses such kind of hidden functions, a state actor might use these functions in the near or far future to control critical components of power systems which may have different impacts on a specific subsector such as electricity or nuclear energy. The integrity of components does not only apply to software based systems but also to electronic hardware components.

The challenge[35] does not only comprise energy-related infrastructure building blocks but also the security components which should protect the energy sector. If these components are vulnerable,

[34] See Akkuyu NPP project, presented by a representative of the Turkish Atomic Energy Authority at a Meeting on Engineering and Design Aspects of Computer Security for I&C at NPPs 03 - 05 September 2012 Garching, Germany

[35] UN GGE Report: https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html

the energy sector is exposed. Reliable security does only exist if trustful components are used and a trustful supply chain exists. If a Member State is not able to verify ex-ante the security of its most impactful national assets, a third party might exploit it. Security in this sense includes evaluation of appropriate encryption technologies as well as other protection technologies and, of course, the capability to identify and detect malicious or undocumented/unpredicted activities in terms of these assets.

5.4.8 Increased Interdependency among Market Players

This challenge is mainly relevant for the electricity subsector. As described in chapter 5.3, the energy market has changed tremendously and lead to an interdependency among market players that is reflected for example in the dynamic pricing of energy. In the way, closed systems are open up to more market players, the overall energy network stability is not any longer a uni-directional issue mainly controlled by the TSOs. As a consequence, operators are increasingly using network automation technologies to keep the network stable. The risks on security of supply are increased accordingly and a potential operational disruption could be caused by directly (e.g. Distribution System Operator) or indirectly (e.g. Virtual Power Plant Operator) connected market players.

Another potential risk is that the decision making process might be influenced indirectly via the energy wholesale markets, which are increasingly used for low cost opportunities in order to optimize business results and to manage demand and supply based on weather conditions and weather forecasts. A disruption or fraud on the energy organised market places might impact the energy stability as planned capacity might not be available if the planning is based on wrong data or information. This challenge is mainly relevant for the electricity subsector as a subsector which increasingly relies on short term planning.

5.4.9 Availability of Human Resources and Their Competences

This challenge is relevant for the whole energy sector. The growing need to handle ICT competences in an OT environment has led to a market need on having resources with the right skills to manage cyber security. However, these resources are rare. Current education programs are focussing on either ICT engineers or on electrical engineers. A combination of both is typically build-up over years with training on the job within the industry. Specific academic programmes are missing. With the increasing digitalisation in the energy sector, this is one of the major challenges in the industry to overcome.

Resources with a broader set of skills, i.e. ICT engineering and information security skills and sector specific engineering skills are needed in all subsectors of the energy sector and in nuclear energy; therefore this challenge applies to all.

5.4.10 Constraints Imposed by Cyber Security Measures in Contrast to Real-Time/Availability Requirements.

This challenge is relevant for the subsector electricity, gas and nuclear energy. It is not considered relevant for oil based on the criteria defined in chapter 5.1. The potential cross-border impact for the oil subsector is low and the real-time and availability requirements can be considered negligible. Potential incidents can be typically treated on organisational or national level.

The electric grids, the process industry such as gas or the nuclear energy facilities have strong real-time and availability requirements to ensure the security of supply. This means that there is a strong

requirement for protection of assets and safety. Cyber security measures implemented or applied are not allowed to impact, e.g. delay, the operation on the grid or on a reactor. Compare section 5.4.3 on the topic of 'investigation', too.

As pointed out before, a control system in the energy sector that is under attack cannot be just disconnected from the network. Due to the fact that traditional cyber security measures are developed to support the needs for an information technology (IT) office environment, constraints to apply such measures in high-availability, real-time systems are not easily met. Therefore, there is a need to have security controls and measures available, which are optimized to the real-time and availability requirements as needed in the electricity and gas subsector and in nuclear energy.

This challenge is subject to further research and development.

5.5 Conclusion of Challenges in the Energy Sector

All of the challenges identified in chapter 5 are related to the electricity subsector, but not all are related to nuclear energy or to the oil and gas subsector as pointed out in respective sections of the challenges. Table 2 summarizes which subsector, including nuclear energy, is subject to which of the challenges:

No.	Challenge	Electricity	Oil	Gas	Nuclear
1	Grid stability in a cross-border interconnected energy network.	x		x	x
2	Protection concepts reflecting current threats and risks.	x	x	x	x
3	Handling of cyber attacks within the EU.	x	x	x	x
4	Effects by cyber attacks not fully considered in the design rules of an existing power grid or nuclear facility	x			x
5	Introduction of new highly interconnected technologies and services.	x		x	
6	Outsourcing of infrastructures and services.	x		x	x
7	Integrity of components used in energy systems.	x		x	x
8	Increased interdependency among market players.	x			
9	Availability of human resources and their competences.	x	x	x	x
10	Constraints imposed by cyber security measures in contrast to real-time/availability requirements.	x		x	x

Table 2: Challenges in the energy sector

However, the mapping does not make any statement that the nature and possible impact and risk are comparable among all subsectors and nuclear energy. This is again subsector specific and is considered in the next chapter.

6. A Sectoral Approach for the Energy Sector

A sectoral approach defines the level of interaction, where cyber security is addressed. The basis for the discussion within this chapter is the challenges identified by the EECSP experts in chapter 5.

Typically, challenges are addressed on various levels with various aspects along the stakeholders:

- European Commission and international organisations such as OSCE, NATO
- Member States of the European Union
- Operators, respective service providers and vendors including the related industry associations
- Operators of Non-EU Nation States which are connected to the EU energy grid incl. respective Nation States
- Operators of other sectors that services are used in the energy sector, e.g. telecommunication or IT

This chapter will identify strategic areas which address the challenges identified and will derive a framework with strategic priorities for the energy sector. However, please note that the strategic areas might be addressed differently for the respective energy subsectors, see chapter 5.1, and that not all strategic areas are relevant for all subsectors, see section 6.2.

Please note that this chapter will not refer to existing policy papers or legislation as this analysis is developed in chapter 8.

6.1 Identification of Strategic Areas for the Energy Sector

This section will point out strategic areas in order to address the challenges identified without going into the details of the challenges itself again as this has been done in chapter 5. The identified strategic areas of potential interventions in order to overcome the existing challenges are described as following:

6.1.1 European Threat and Risk Landscape and Treatment

European Union with its Member States should agree on a common threat and risk landscape with the goal to understand and address the threat and risks concerning the energy systems. This threat and risk landscape should be updated regularly and as a common base to protect the energy grid and the data protection rights of European citizens. As pointed out in chapter 5.4, the cyber security threats and risks for the energy grid is changing continuously. The energy grid is connected not just with the Member States of the European Union, but also with other connected operators and states such as Norway and Switzerland, which have to be considered and actively involved in the threat and risk landscape definition as well.

Additionally, European Union with its Member States should agree on how to address respective threats and risks (avoid, mitigate, transfer, accept) based on an actual and more global threat and risk landscape. Member States should also include the European threat and risk landscape into their respective threat and risk treatment processes. The target of a threat and risk treatment is to protect the energy sector from existing threats and risks.

Reasoning: As pointed out in challenge 5.4.1, the energy grid and systems in Europe are interconnected. Protection of such an interconnected network requires a risk and threat based approach that not just include known risks and incidents, but take into consideration as well threat intelligence in order to derive potential risks and threats for the energy grid and systems in Europe. A European threat and risk landscape and treatment is supporting the effort to protect the European Union by keeping up with the pace of changing threats and risks. A threat and risk landscape is therefore the base for the respective treatment and is a relevant strategic area addressing nearly all challenges found in chapter 5 as can be seen in the mapping of challenges and identified strategic areas in section 6.2.

6.1.2 Identification of Operators of Essential Service

According to the NIS Directive[36], Member States are requested to identify the operators of essential services. The European Union should support on the identification of the operators of essential services in order to harmonize the process among Member States and to address the weakest link problem in an interconnected energy grid. This becomes crucial when implementing a threat and risk treatment in the Member States, see previous strategic area, while avoiding the weakest link problem.

Reasoning: Besides the weakest link problem stated above, challenges 5.4.1 and 5.4.8 pointed out that the energy grid and systems are interconnected and the energy market is changing tremendously. The first challenge (5.4.1) implies the need that relevant operators are identified as operators of essential services who are addressed with the threat and risk treatment as pointed out in previous strategic area (European threat and risk landscape and treatment). The second challenge (5.4.8) takes into account the changing market environment what might need to consider new market players as operators of essential services, too.

6.1.3 Cyber Response Framework

Cyber attacks can be caused by various threat agents ranging from non-state to nation state actors as pointed out in chapter 5.4. Operators under attack are typically busy with re-establishing an acceptable level of protection for their systems, keeping them operational or bring them back to life. In case of extensive coordinated attacks, support from Member States or coordinated actions across Member States (federal or regional approach) might be required. This might involve organisations such as OSCE or NATO. The NATO agreements cover already cyber response within a respective unit[37]. Nevertheless, NATO Nation States and EU Member States do not correspond; as a consequence, some of the EU Member States are left out from the NATO cyber defence system. The EU need to consider countries not included in the NATO alliance (e.g. Austria), which are nevertheless connected with the European energy grid. This issue has been already recognized and has been started to be addressed in the Joint Framework to counter hybrid threats[38]. As pointed out

[36] NIS Directive: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013PC0048&from=EN

[37] Cyber Defence Policy Framework:
http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf
Six monthly reports on implementation:
- http://statewatch.org/news/2016/jul/eu-council-cyber-defence-implementation-report-9701-16.pdf
- http://data.consilium.europa.eu/doc/document/ST-13801-2015-INIT/en/pdf

[38] Joint Framework 2016/18: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018

in chapter 5.4.3, the handling of cyber attacks has many aspects to be covered. A cyber response framework would be required for example to classify attacks, define responsibilities and capabilities needed to protect against cyber attacks which must be tailored to threat profiles in order to be resolved on an appropriate institutional or organisational level. This should include diplomatic means to reduce tensions or stem conflicts such as OSCE Confidence Building Measures[39]. Coordination and information exchange mechanism between the attacked organisation, nation states, EU, NATO and OSCE. International alliances are required for an effective protection of the European energy grid.

Reasoning: Typically, the protection of an energy grid has various aspects, see challenge 5.4.3. Beside the active part of any organisation to identify, detect, protect, respond and recover from cyber attacks, there are attacks that go beyond the capability of a public or private organisation such as an energy system operator that require collaboration with allies, diplomatic or military. The relevance for such collaboration can be seen for example in the announced cooperation in cyber security between NATO and European Union[40]. This should be well defined in a cyber response framework.

6.1.4 Crisis Management

Blackout scenarios are discussed widely in the industry. A major long lasting blackout as seen typically by natural catastrophes has not been seen caused by cyber attacks yet. Nevertheless, the criticality of the energy grid and potential high impact on the society requires respective emergency plans and practice on cyber exercises available for handling of major blackouts as pointed out in chapter 5.4.3.

Reasoning: A well-established crisis management capability is a key responsibility of Member States. In case of major long-lasting black-outs, crisis management might get challenging as it typically relies on well-functioning communication technologies, which might not be available without energy as pointed out in the respective challenge 5.4.3.

6.1.5 European Cyber Security Maturity Framework

Protection of the energy grid is a collective responsibility of the respective operators and the Member States. However, the criticality and the interdependency of the grid require a harmonization of the protection of respective systems across the European Union. An appropriate tool to define and develop the protection level of an energy grid is the usage of a cyber security maturity framework, which should be defined at EU level and best based on international standards (e.g. ISO/IEC 27000 series). This would allow a flat assessment scheme against to which Member States and the EU can evaluate the maturity of security within the Member State and the EU and on which the overall resilience of the energy grid within the EU can be measured and assessed while avoiding a scattered view of the EU landscape. Examples of a maturity framework for the energy grid exist for example by the ES-C2M2[41] framework for electricity subsector or the ONG-C2M2 framework for the oil and gas subsector from the United States Department of Energy (DoE). An additional advantage of a maturity framework would be to enable and foster use of cyber insurance

[39] OSCE Confidence Building Measures: http://www.osce.org/cio/126475
[40] NATO and the European Union enhance cyber defence cooperation: http://www.nato.int/cps/en/natohq/news_127836.htm
[41] http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program

as one mechanism to cover potential damages by cyber attacks and by the achievement of a higher maturity level that may result in a lower insurance cost.

Reasoning: Several challenges can be addressed with a maturity framework. As already discussed in the strategic area 'European threat and risk landscape and treatment', there is a need to establish a common baseline for cyber security in order to avoid the weakest link problem (challenge 5.4.1 and 5.4.2). Additionally, the deployment of new technologies (challenge 5.4.5) and the usage of outsourcing (challenge: 5.4.6) requires a maturity within the respective organisations in order to address these challenges appropriately. Another point is challenge 5.4.8, which needs to take into consideration the increased interdependency among market players and therefore addresses the weakest link problem in an interconnected horizontal (energy grid and systems) and vertical (different market players and application) diversified energy sector.

6.1.6 Supply Chain Integrity Framework for Components

Hidden functions and undocumented access capabilities (backdoors) in components are one major concern in the energy sector which typically cannot be exhaustively identified by the most common certifications or standard penetration tests. In order to address this area, an EU supply chain integrity framework for components and suppliers is required.

Reasoning: As pointed out in challenge 5.4.7, the integrity of components used in critical infrastructures is difficult to assure and to gurantee. This is relevant for components with associated high potential impact as they are used in power grids or nuclear energy. However, measures to increase the level of trust are possible and should be defined with due care.

6.1.7 Capacity and Competence Build-Up

As pointed out in chapter 5.4.9, availability of human resources and their competences required for the energy sector are rare. Capacity and competence build-up can include the creation of a partner networks, training and skill certification programs, education with academic curricula's, promote specific grants and research programs covering energy and cyber security aspects as a core topic.

Reasoning: The energy sector is changing tremendously as pointed out in chapter 5. This requires capacity and competences, which are not sufficiently available in the market. A special focus point is therefore the build-up of respective capacity and competence in order to address the challenges 5.4.5, 5.4.9 and 5.4.10.

6.1.8 Best Practice and Information Exchange

Best practice and information sharing, e.g. via an energy Information Sharing and Analysis Centre (ISAC), can support the overall goal on a resilient energy network by increasing the knowledge on how to enable stakeholders to learn and apply best practices as well as helping in organisational preparedness while fostering trust and collaboration among all involved stakeholders.

Reasoning: The introduction of new technologies (challenge 5.4.5), the interdependency of market players (challenge 5.4.8) or the inter-connection of energy systems and networks (challenge 5.4.1) are building typical scenarios that can benefit from best practice sharing. This will help avoiding pitfalls by the exchange of experience. Furthermore, the exchange on sensitive information on

incidents such as information on cyber attacks can help operators to protect their network proactively (challenge 5.4.3). This can be done for example via an ISAC set-up[42].

6.1.9 Foster International Collaboration

Cyber security does not respect geographical borders and has an international essence. It requires international collaboration and alliances. Cooperation and alliances require the generation and sharing of added value information among partners. For an EU with 28 Member States, it is reasonable to have one interface towards international allies in order to build-up a reliable and strong network of partners to help protecting the European infrastructure.

Reasoning: In cases of cyber security incidents, a fast sharing of information can help to protect the energy sector; this is valid, too, in case of cyber attacks (challenge 5.4.3). The exchange of information with international organisations can support the overall goal to proactively protect the energy sector.

6.1.10 Awareness Campaign from Top-Level of EU Institutions

Awareness in cyber security is still lacking behind. Efficient treatment and cooperation among Member States and within the EU requires a good understanding what is at stake and why this needs to be a collaborative effort. In the same way, Member States have to understand the need for a joint effort in cyber security, the top-level of the EU institutions have to drive the effort to protect and to increase the resilience of the energy grid.

Reasoning: In order to emphasize and foster collaboration among Member States, a structured and focused awareness campaign could be used as the institutions of the EU do play a key role in cyber security particular when it comes to challenge 5.4.3.

6.1.11 Overview of the Strategic Areas

Table 3 summarizes the strategic areas:

No.	Identified Strategic Areas
1	European threat and risk landscape and treatment
2	Identification of operators of essential services
3	Cyber response framework
4	Crisis management
5	European cyber security maturity framework
6	Supply chain integrity framework for components
7	Capacity & competence build-up
8	Best practice and information exchange
9	Foster international collaboration
10	Awareness campaign from top level EU institutions

Table 3: Identified Strategic Areas of the energy sector

They are reflected in the following section 6.2 to the energy subsectors electricity, oil, gas and nuclear energy. In chapter 6.3, they are further categorized in order to derive a strategic framework and strategic priorities for the EU.

[42] Compare https://www.esisac.com, www.ee-isac.eu

6.2 Reflection of Strategic Areas to the Energy Subsectors

As stated in chapter 5.5 and in chapter 5.1, neither are all challenges relevant for each subsector and nuclear energy nor do all domains have the same criticality, impact, cross border and weakest link problem, real-time and availability requirements. This section will reflect the strategic areas to the subsectors electricity, oil, gas and nuclear energy in regards to the respective challenges from chapter 5.4, see Table 4:

No.	Challenges
1	Grid stability in a cross-border interconnected energy network.
2	Protection concepts reflecting current threats and risks.
3	Handling of cyber attacks within the EU.
4	Effects by cyber attacks not fully considered in the design rules of an existing power grid or nuclear facility.
5	Introduction of new highly interconnected technologies and services.
6	Outsourcing of infrastructures and services.
7	Integrity of components used in energy systems.
8	Increased interdependency among market players.
9	Availability of human resources and their competences.
10	Constraints imposed by cyber security measures in contrast to real-time/availability requirements.

Table 4: Challenges in the energy sector

In the following, a reflection of the strategic areas to the energy subsectors electricity, oil, gas and nuclear energy is provided.

Electricity subsector

Due to the nature of the electricity subsector, all criteria defined in chapter 5.1 are met with a high potential disruptive effect on the real economy and society. Taken into account the strong real-time and availability requirements, all challenges are relevant and all identified strategic areas apply to the electricity subsector:

Electricity Subsector		Challenges (see Table 4)									
No.	Identified Strategic Areas	1	2	3	4	5	6	7	8	9	10
1	European threat and risk landscape and treatment	x	x	x	x	x	x	x	x	x	
2	Identification of operators of essential services	x							x		
3	Cyber response framework			x							
4	Crisis management				x		x				x
5	European cyber security maturity framework	x	x			x	x		x		
6	Supply chain integrity framework for components							x			
7	Capacity & competence build-up					x				x	x
8	Best practice and information exchange	x		x		x			x		
9	Foster international collaboration			x							
10	Awareness campaign from top level EU institutions			x							

Table 5: Relevant strategic areas for the electricity subsector

In the electricity subsector, the criticality and interconnection of the energy grid and systems requires a support of EU level in all strategic areas.

Oil subsector

The oil subsector can be considered rather distributed without interconnection; in Europe oil pipelines are used for transport of oil, but alternative means of transport for oil, e.g. by road or rail, is possible, too. Therefore, the potential impact is rather regional and can be typically treated regionally by respective Member States. Even the potential impact is rather regional, a potential environmental impact has to be taken into consideration. Looking into the relevant challenges for oil, see chapter 5.5, three challenges are considered relevant for oil:

2. Protection concepts reflecting current threat and risks.
3. Handling of cyber attacks within the EU.
9. Availability of human resources and their competences.

The respective areas relevant for the oil subsector can be taken from Table 6:

Oil Subsector		Challenges (see Table 4)									
No.	**Identified Strategic Areas**	1	2	3	4	5	6	7	8	9	10
1	European threat and risk landscape and treatment		x	x						x	
2	Identification of operators of essential services										
3	Cyber response framework			x							
4	Crisis management										
5	European cyber security maturity framework		x								
6	Supply chain integrity framework for components										
7	Capacity & competence build-up									x	
8	Best practice and information exchange			x							
9	Foster international collaboration			x							
10	Awareness campaign from top level EU institutions			x							

Table 6: Relevant strategic areas for the oil subsector

Considering particular the potential regional impact compared to electricity and nuclear energy, a treatment of the strategic areas on a national level seems appropriate for the oil subsector. However, it should be agreed among Member States and respective industry associations, if the need on a support by the EU is seen for respective areas.

Gas subsector

The gas subsector has nearly the same challenges to be addressed as the electricity subsector. Relevant are the challenges:

1. Grid stability in a cross-border interconnected energy network.
2. Protection concepts reflecting current threats and risks.
3. Handling of cyber attacks within the EU.
5. Introduction of new highly interconnected technologies and services.
6. Outsourcing of infrastructures and services.
7. Integrity of components used in energy systems.
9. Availability of human resources and their competences.
10. Traditional cyber security measures conflicts with real-time and availability requirements.

Even not all challenges are relevant for the gas subsector, still all identified strategic areas are to be considered:

Gas Subsector		Challenges (see Table 4)									
No.	Identified Strategic Areas	1	2	3	4	5	6	7	8	9	10
1	European threat and risk landscape and treatment	x	x	x		x	x	x		x	
2	Identification of operators of essential services	x									
3	Cyber response framework			x							
4	Crisis management						x				x
5	European cyber security maturity framework	x	x			x	x				
6	Supply chain integrity framework for components							x			
7	Capacity & competence build-up					x				x	x
8	Best practice and information exchange	x		x		x					
9	Foster international collaboration			x							
10	Awareness campaign from top level EU institutions			x							

Table 7: Relevant strategic areas for the gas subsector

However, similar to oil, the potential impact on a cyber attack on a gas network is considered mainly as regional, except for the cases, where a country's energy supply depends strongly on the supply of power by gas delivered cross-border. Additionally, turbogas systems used as cogeneration power plants to overcome shorter instabilities in the power supply should be treated as critical systems for the energy grid, too. Besides those specific turbogas systems, it should be agreed with Member States and respective industry associations, if the need on a support by the EU is seen for respective areas.

Nuclear Energy

Due to the potential devastating impact of incidents with nuclear, a different view on nuclear has to be taken. Relevant challenges are:

1. Grid stability in a cross-border interconnected energy network.
2. Protection concepts reflecting current threats and risks.
3. Handling of cyber attacks within the EU.
4. Effects by cyber attacks not fully considered in the design rules of an existing power grid or nuclear facility.
6. Outsourcing of infrastructures and services.
7. Integrity of components used in energy systems.
9. Availability of human resources and their competences.
10. Traditional cyber security measures conflicts with real-time and availability requirements.

Even not all challenges are relevant for nuclear energy, still all identified strategic areas are to be considered:

Nuclear Energy		Challenges (see Table 4)									
No.	Identified Strategic Areas	1	2	3	4	5	6	7	8	9	10
1	European threat and risk landscape and treatment	x	x	x	x		x	x		x	
2	Identification of operators of essential services	x									
3	Cyber response framework			x							
4	Crisis management				x		x				x
5	European cyber security maturity framework	x	x				x				
6	Supply chain integrity framework for components							x			
7	Capacity & competence build-up									x	x
8	Best practice and information exchange	x		x							x

Nuclear Energy		Challenges (see Table 4)									
No.	Identified Strategic Areas	1	2	3	4	5	6	7	8	9	10
9	Foster international collaboration			x							
10	Awareness campaign from top level EU institutions			x							

Table 8: Relevant strategic areas for nuclear energy

In nuclear energy, a differentiation has to be done due to the fact that civil nuclear installations are controlled in different aspects by different national and international regulatory bodies.

6.3 Strategic Framework for the Energy Sector

In chapter 5, high-level objectives have been agreed that have eventually lead to the strategic areas for the energy sector in chapter 6.1. In order to bring the identified areas into context, i.e. providing a big picture, a further step can be taken by categorization of these areas. Doing this, strategic priorities can be directly derived:

I. Set-up an effective threat and risk management system (1, 2)
II. Set-up an effective cyber response framework (3,4,9)
III. Continuously improve cyber resilience (5, 6, 8, 9, 10)
IV. Build-up the required capacity and competences (7)

In the brackets of these strategic priorities, the corresponding strategic areas, see chapter 6.1.11 are listed.

As a result, the following European strategic framework for the energy sector can be outlined:

High-level objectives

- Secure energy systems that are providing essential services to the European society
- Protect the data in the energy systems and the privacy of the European citizen.

Strategic Priorities

I. Set-up an effective threat and risk management system

- EU-wide agreed threat and risk landscape for the energy sector.
- EU-wide agreed risk and threat treatment (avoid, mitigate, transfer, accept) based on an actual threat and risk landscape.
- Member States include and consider the European threat and risk landscape into their respective risk treatment processes.

II. Set-up an effective cyber response framework

- Cyber response framework to support protect and response mechanism on cyber attacks.
- Member States have crisis management capabilities in place to handle major blackouts scenarios deriving from cyber incidents and/or cyber attacks.
- Build-up and maintain international alliances and partnerships.

III. Continuously improves cyber resilience

- EU-wide agreed level of cyber security protection defined by a European cyber security maturity framework.
- Supply chain integrity framework for supplier and components.
- Collaboration among national and international entities.

- Increase the awareness on cyber security for the energy sector.

IV. Build-up the required capacity and competences

- Build-up of capacity and competences required to fulfil the protection, risk and threat treatment goals of the European Union.
- Sharing of information and best practice among relevant stakeholders in the energy sector.

This strategic framework is meant as an instrument that helps to bring the identified areas into the context of the overall objectives while providing a big picture without losing the content. However, the implementation details might differ for each subsector and should consider the risks in order to balance the implementation cost.

The strategic priorities are used furthermore to link the gaps and recommended actions in chapter 8 and chapter 9.

7. Policies and Regulations of the European Union

This chapter gives an overview on the key policies and regulations of the European Union which are analysed in chapter 8 concerning coverage on the strategic areas identified in chapter 6.

7.1 Digital Single Market (DSM) Strategy

The DSM Strategy (2015)[43] addresses the Protect and Respond functions. The strategy is general and references the energy sector in the context of critical infrastructures, alongside justice, health, and transport. The strategy discusses the importance of technical and interoperability standards, but is not specific except for references to the e-Privacy Directive[44] and the European Agenda on Security. Finally, the strategy stresses the importance of economic aspects of having a Digital Internal Single Market and includes several general references to cyber security. Specific references are to the NIS Directive and the Cyber Security Strategy of the European Union.

The DSM Strategy has two specific recommendations related to security:

- The Commission will initiate the establishment of a contractual Public-Private Partnership on cyber security (cPPP) in the area of technologies and solutions for online network security. (see chapter 7.2)
- The need to define missing technological standards that are essential for supporting the digitalisation of the industrial and services sectors (e.g., Internet of Things, cyber security, big data and cloud computing) and mandating standardisation bodies for fast delivery.

In the Digital Single Market Strategy for Europe, the European Commission adopted a Communication on 'Building a European Data Economy'[45], accompanied by a Staff Working Document on January 2017, where it looks at proven or potential blockages to the free movement of data and presents options to remove unjustified and or disproportionate data location restrictions in the EU. It also considers the barriers around access to and transfer of non-personal machine-generated data, data liability, as well as issues related to the portability of non-personal data, interoperability and standards.

7.2 Contractual Public Private Partnership (cPPP)

By mid-2016, the European Commission launched a new public-private partnership on cyber security that is intended to better equip Europe against cyber-attacks and to strengthen the competitiveness of the cyber security sector. The partnership will include cyber security market players, research centres, academia, and members from national, regional, and local public administrations. The aim of the partnership is to foster cooperation at early stages of the research and innovation process and to build cyber security solutions for various sectors, such as energy, health, transport and finance. The Commission will propose how to enhance cross-border cooperation in the case of a major cyber incident. Finally, the Commission will examine how to strengthen and streamline cyber security cooperation across different sectors of the economy, including in cyber security training and education.

[43] COM/2015/0192 final

[44] e-Privacy directive: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML
European Agenda on Security: http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

[45] COM(2017) 9 final and SWD(2017) 2 final

7.3 EU Cyber Security Strategy

The EU Cyber Security Strategy (2013)[46] provides an overview of the changing environment, particularly in cyberspace and the internet and the need for requirements in security. The strategy document references critical infrastructures including the energy sector and primarily addresses the Identify, Protect, and Respond functions.

The document includes the following five strategic priorities:

- Achieving cyber resilience.
- Drastically reducing cybercrime.
- Developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP).
- Develop the industrial and technological resources for cyber security.
- Establish a coherent international cyberspace policy for the European Union and promote core EU values.

The document focuses on:

- Compliance with the EU data protection laws applicable to personal data.
- The definition, analysis and remediation of vulnerabilities in ICT.
- Prevention, detection, and responding to cyber security incidents.
    - The reporting of incidents with a significant impact on continuity of core services.
- Management of risk by providers of electronic communications.
- EU level exchange of information and cyber incident exercises.

7.4 European Agenda on Security

The European Agenda on Security (2015)[47] implements Political Guidelines in the area of security prioritising terrorism, organized crime and cybercrime. The Agenda builds on the actions undertaken in the last years, thus ensuring consistent and continued action by replacing the previous Internal Security Strategy (2010-2014).

The agenda offers five key principles on which all actors involved have to work together:

- Ensure full compliance with fundamental rights;
- Guarantee more transparency, accountability and democratic control;
- Ensure better application and implementation of existing EU legal instruments;
- Provide a more joined-up inter-agency and a cross-sectoral approach;
- Bring together all internal and external dimensions of security.

The Communication fully acknowledges cybercrime as an ever-growing threat to citizens' fundamental rights and to the economy, as well, as to the development of a Digital Single Market. The Directive promotes better cooperation between law enforcement and cyber security authorities as well as the cooperation with the private sector. Among others, it sets an emphasis on ensuring the full implementation of existing policies on cyber security, reviewing obstacles to criminal

[46] JOIN(2013) 1 final

[47] European Agenda on Security: http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

investigations on cybercrime and on enhancing cyber capacity building action under external assistance instruments.

7.5 Directive on Security of Network and Information Systems (NIS)

The NIS Directive (2016)[48] is a key component of the overall strategy to prevent and respond to cyber disruptions and attacks. The Directive specifies measures with a view to achieving a high common level of security of networks and information systems within the EU so as to improve the functioning of the internal real and digital market.

The Directive:

- Obligates Member States to adopt a national NIS strategy.
- Creates a Cooperation Group to support and facilitate strategic cooperation regarding security of network and information systems and the exchange of information among Member States.
- Creates a CSIRTs ("Computer Security Incident Response Team") network to contribute to developing confidence and trust between Member States and to promote swift and effective operational cooperation.
- Establishes security and notification requirements for operators of essential services.
- Requires that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and information systems which they use in their operations.
- Obligates Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of networks and information systems.

The first "pillar" of the Directive is the capabilities, which requires each Member State to make sure they are well equipped to face cyber threats. The second pillar aims at increasing EU-wide cooperation, both at strategic (Cooperation Group of national authorities) and operational (CSIRT network) level. The third pillar, which is the most relevant for this analysis, refers to the security and notification requirements. According to the NIS Directive, "operators of essential services" will have to take appropriate security measures and to notify the national competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services.

With regard to the operators of essential services, the energy sector falls within the scope of the Directive. Gas, oil and electricity supplies are essential services covered by the NIS Directive; Annex II of the NIS Directive describes the subsectors and types of entities addressed.

For the electricity subsector, ‘electricity undertakings as defined in clause (35) of Article 2 of Directive 2009/72/EC[49] of the European Parliament and of the Council, which carry out the function of ‘supply’ as defined in clause (19) of Article 2 of that Directive’ are included. Regarding Directive 2009/72/EC, to these electricity undertakings count ‘any natural or legal person carrying out at least one of the following functions: generation, transmission, distribution, supply, or purchase of electricity, which is responsible for the commercial, technical or maintenance tasks related to those functions, but does not include final customers.’ This electricity undertaking shall carry out the

[48] Directive (EU) 2016/1148
[49] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

function of supply, meaning 'the sale, including resale, of electricity to customers'. Thus point 1 letter (a) of Annex II refers to electricity undertakings that carry out the supply function, therefore 'suppliers' as defined by Directive 2009/72/EC. For the electricity sector, distribution system operators[50] and transmission system operators[51] fall as well under the definition of operators of essential services as shown in point 1 (b) and 1 (c). The coverage of electricity generation is not explicit included and gives room for interpretation.

For the subsector oil, operators of oil transmission pipelines and operators of oil production, refining and treatment facilities, storage and transmission fall under the definition of operators of essential services.

For the subsector gas, supply undertakings[52], distribution system operators[53], transmission system operators[54], storage system operators[55], LNG system operators[56], natural gas undertakings[57] and operators of natural gas refining and treatment facilities fall under the definition of operators of essential services.

The specific operators of essential services that fall within the scope of the Directive will be identified by the Member States based on the following criteria:

- The entity provides a service which is essential for the maintenance of critical societal/economic activities;
- The provision of that service depends on network and information systems; and

[50] 'distribution system operator' means a natural or legal person responsible for operating, ensuring the maintenance of and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems and for ensuring the long-term ability of the system to meet reasonable demands for the distribution of electricity- Directive 2009/72/EC

[51] 'transmission system operator' means a natural or legal person responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity- Directive2009/72/EC

[52] 'supply undertaking' means any natural or legal person who carries out the function of supply – Directive 2009/73/EC Article 2 (8)

[53] 'distribution system operator' means a natural or legal person who carries out the function of distribution and is responsible for operating, ensuring the maintenance of, and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution of gas; - Directive 2009/73/EC Article 2(6)

[54] 'transmission system operator' means a natural or legal person who carries out the function of transmission and is responsible for operating, ensuring the maintenance of, and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transport of gas; Directive 2009/73/EC Article 2 (4)

[55] 'storage system operator' means a natural or legal person who carries out the function of storage and is responsible for operating a storage facility; 2009/73/EC Article 2 (10)

[56] 'LNG system operator' means a natural or legal person who carries out the function of liquefaction of natural gas, or the importation, offloading, and re-gasification of LNG and is responsible for operating a LNG facility; Directive 2009/73/EC Article 2 (12)

[57] 'natural gas undertaking' means a natural or legal person carrying out at least one of the following functions: production, transmission, distribution, supply, purchase or storage of natural gas, including LNG, which is responsible for the commercial, technical and/or maintenance tasks related to those functions, but shall not include final customers; Directive 2009/73/EC Article 2 (1)

- A NIS incident would have significant disruptive effects on the provision of the essential service.

With regard to security requirements, Member States will have to ensure that Operators of Essential Services (ESOs) adopt security requirements to:

- Manage risks: Companies will have to put in place organisational and technical measures that are appropriate and proportionate to the risk.
- Ensure security of network and information systems: The measures should ensure a level of NIS security appropriate to the risks.
- Handle incidents: The measures should prevent and minimize the impact of incidents on the IT systems used to provide the services.

It is left to Member States to define these specific measures.

Guidance on technical and organisational matters can be provided at the EU level, in particular via the Cooperation Group mentioned above.

The NIS Directive primarily addresses the Identify and Respond functions. The Directive focuses on: business continuity, risk assessment and management, incident reporting and response.

7.6 European Programme for Critical Infrastructure Protection (EPCIP) Directive & European Critical Infrastructure (ECI) Directive

In December 2006, the Commission adopted the Communication on a European Programme for Critical Infrastructure Protection (EPCIP)[58], which set out an overall framework for critical infrastructure protection activities at EU level.

The threats to which the programme aims to respond are not confined to cyber security or terrorism alone, but also include criminal activities, natural disasters and other causes of accidents. The programme thus seeks to provide an all-hazard, cross-sectoral approach to the protection of critical infrastructures.

A key pillar of this program is the 2008 Directive on European Critical Infrastructures[59] (2008/114/EC), which established a procedure for identifying and designating European Critical Infrastructures (ECI) and a common approach for assessing the need to improve their protection. This Directive has a sectoral scope and applies only to the energy and transport sectors.

Main provisions of the Directive:

- Member States must go through a process of identifying potential European Critical Infrastructures (ECIs)
- Member States should use a series of criteria to identify the potential ECIs. The cross-cutting criteria take into account possible casualties and economic and social effects, while the sectoral criteria consider the specificities of each ECI sector.
- Member States must ensure that an operator security plan (OSP) or an equivalent measure is in place for each designated ECI.
- Within a year from designating an ECI in the subsectors, Member States are to conduct an assessment of the threats relating to it. In addition, Member States are to report to the

[58] EPCIP: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:l33260
[59] ECI Directive: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

Commission every two years on the risks, threats and vulnerabilities that the different ECI sectors are facing.

Taking into account developments since the adaption of the EPCIP Communication in 2006, the Commission adopted a 2013 Staff Working Document[60] on a new approach to the European Programme for Critical Infrastructure Protection. It sets out a revised and more practical implementation of activities under the three main work streams – prevention, preparedness and response. The new approach aims at building common tools and a common approach in the EU to critical infrastructure protection and resilience, taking better account of interdependencies.

7.7 Security of Supply (SOS) Directive

Directive 2005/89/EC of the European Parliament and of the Council of 18 January 2006 concerns measures to safeguard security of electricity supply and infrastructure investment. These measures are to ensure the proper functioning of the internal market for electricity and to ensure:

a) An adequate level of generation capacity;
b) An adequate balance between supply and demand; and
c) An appropriate level of interconnection between Member States for the development of the internal market.

The Directive establishes a framework within which Member States are to define transparent, stable and non-discriminatory policies on security of electricity supply compatible with the requirements of a competitive internal market for electricity.

Main provisions of the SOS Directive:

- Member States shall ensure a high level of security of electricity supply by taking the necessary measures to facilitate a stable investment climate and by defining the roles and responsibilities of competent authorities, including regulatory authorities where relevant, and all relevant market actors and publishing information thereon.
- Member States or the competent authorities shall ensure that transmission system operators set the minimum operational rules and obligations on network security.
- Member States shall take appropriate measures to maintain a balance between the demand for electricity and the availability of generation capacity.
- Member States shall establish a regulatory framework that:
    - Provides investment signals for both the transmission and distribution system network operators to develop their networks in order to meet foreseeable demand from the market; and
    - Facilitates maintenance and, where necessary, renewal of the existing networks.

Although this Directive focuses on electricity and transmission systems, the establishment and implementation of the regulatory framework and facilitation of the investments are left to the Member States.

[60] Commission Staff Working Document: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/docs/swd_2013_318_on_epcip_en.pdf

7.8 Clean Energy for all Europeans – Commission Proposal 20th Nov. 2016

The Commission's 'Clean Energy for All Europeans' proposals were adapted 30 November 2016. The proposals cover energy efficiency, renewable energy, the design of the electricity market, security of electricity supply and governance rules for the Energy Union. In addition the proposals acknowledge the importance of cyber security for the energy sector and the need to secure risk preparedness and crisis management. It proposes an obligation to assess rare and extreme risks via appropriate measures (via the risk preparedness proposal). It also proposes further technical rules (i.e. a Network Code) on cyber-security to be adopted in the future.

7.9 Security of Gas Supply Regulation

Regulation (EU) No 994/2010 aims at demonstrating to gas customers that all the necessary measures are being taken to ensure their continuous supply, particularly in case of difficult climatic conditions and in the event of disruption.

The Regulation establishes provisions aimed at safeguarding the security of gas supply by ensuring the proper and continuous functioning of the internal market in natural gas (gas), by allowing for exceptional measures to be implemented when the market can no longer deliver the required gas supplies and by providing for a clear definition and attribution of responsibilities among natural gas undertakings, the Member States and the Union regarding both preventive action and the reaction to concrete disruptions of supply.

Each Member State shall establish at a national level a Preventive Action Plan and an Emergency Plan. The Preventive Action Plan shall contain the measures needed to remove or mitigate the risks identified based on the performed risk assessment. The Emergency Plan shall contain the measure to be taken to remove or mitigate the impact of a gas supply disruption.

In February 2016, the Commission proposed an update to its Security of Gas Supply Regulation. Cyber security – as a source of risk – is part of the template for the risk assessment (Article 6, Annex IX).

7.10 EURATOM

The European Atomic Energy Community (EAEC or EURATOM) is an international organisation that is governed by the European Union's institutions. The legal framework of the work of the EURATOM is based on the EURATOM Treaty as signed on 25th March 1957. The objective of EURATOM is to establish EU-wide conditions in relation to a responsible use of nuclear energy, i.e. for safeguards to avoid misuse of nuclear materials, nuclear safety, radioactive waste management and spent fuel, radiation protection, decommissioning of nuclear facilities.

For example regarding safeguards, EURATOM is full supranational regulator, i.e. it supervises all the nuclear operators in all EU Member States and provides thus also assurance that physical protection measures work properly by avoiding any unauthorized access to nuclear material and to detect a potential insider threat.

As highlighted by the jointly agreed EU Security Agenda[61], law enforcement and other key authorities need to be better prepared for security risks related to the vulnerability of critical infrastructure and to design and enforce preventive measures in a coordinated manner across

[61] https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security_en

borders. They should also support and actively participate in research on future technological and capability needs.

While the EURATOM Treaty contains no explicit provisions addressing nuclear security or physical protection, provisions in the preamble and in Article 2 have been interpreted as also covering the subject. In its Ruling 1/78 of 1978, the Court of Justice of the EU found that the EURATOM Community shares competence with the Member States in the area of physical protection of nuclear material, and should therefore become a Party to the Convention on the Physical Protection of Nuclear Materials (CPPNM)[62] which was being negotiated at the time. While leaving room for interpretation on the extent of the Community's competences in this area, the Court clearly recognised that involvement of the Community in decision-making on measures of physical protection was essential in order to implement our recognised responsibilities on safeguards, supply policy and ownership of nuclear materials. In spite of the Court's ruling and the Community's subsequent accession to the CPPNM, the Community has to date not proposed any secondary legislation specifically addressing e.g. physical protection in the scope of nuclear security[63] as defined in chapter 5.4.

7.11 The General Data Protection Regulation (GDPR)

The GDPR (2016)[64] specifies rules relating to the protection of individuals with regard to the processing of personal data by automated means and rules relating to the free movement of personal data.

The regulation updates and modernises the principles of the 1995 Data Protection Directive to guarantee privacy rights. It focuses on: reinforcing individuals' rights, strengthening the EU internal market, ensuring stronger enforcement of the rules, streamlining international transfers of personal data and setting global data protection standards.

The changes will give people more control over their personal data and make it easier to access it. They are designed to make sure that people's personal information is protected – no matter where it is sent, processed or stored – even outside the EU, as may often be the case on the internet.

Measures towards providing stronger individual's rights

- It introduces an explicit 'right to be forgotten' in cases where data have been made public (e.g. online).
- Easier access to one's data: Individuals will have more information on how their data is processed and this information should be available in a clear and understandable way. A right to data portability will ease the transmission of personal data between service providers.
- It reinforces the notion of consent. Whenever consent is required for data processing, it will have to be given explicitly, rather than be assumed.
- The powers of supervisory authorities are strengthened with higher fines and legal remedies.

[62] See e.g.: https://www.iaea.org/Publications/Documents/Conventions/cppnm_status.pdf
[63] 'Nuclear security' denotes here the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities.
[64] Regulation (EU) 2016/679

Measures setting forth new obligations to enhance the accountability of data controllers

- Notification of personal data breaches.
- Obligation to perform data protection impact assessments in certain specific cases.
- It requires data controllers to keep the documentation regarding their processing activities.
- Requires data controllers to designate a data protection officer.

It introduces explicitly the principles of accountability, data protection by design and by default.

7.11.1 Data Protection Impact Assessment (DPIA) Template

Related to smart grids, the European Commission collaborated with the EC Smart Grid Task Force to develop a Data Protection Impact Assessment Template for smart grid and smart metering systems (Recommendation 2014/724/EC). The requirement to perform data protection impact assessments is included in the GDPR and listed above. The objective is to guarantee protection of personal data throughout the EU.

The Template is an evaluation and decision-making tool that helps entities planning or executing investments in smart grids to identify and anticipate risks to data protection, privacy, and security and will help industry identify data protection risks in smart grid developments from the start. The DPIA test phase was initiated in 2014 and will continue for two years.

The GDPR focuses on the protection and processing of personal data, and does not address the critical infrastructures. The GDPR primarily addresses the Identify and Protect functions. The document focuses on the protection of personal data, including processing, usage, storage, and accuracy. The document does not reference cyber security, critical infrastructures, or the energy sector.

7.12 National Cyber Security Strategies

Member States have national cyber security strategies[65] defined which are evolving under the light of the NIS Directive. The EECSP experts have reviewed over 50 strategies from Member States and other Nation States such as Switzerland and USA. The national cyber security strategies are typically high-level, top-down approaches to cyber security that establish a range of national objectives and priorities. Each strategy provides a strategic framework for a nation's approach to cyber security. Following are general comments that are applicable to the majority of the strategies:

- All countries provided a general security strategy and some included a cyber security strategy. The national approach to cyber security is typically at a high strategic level.
- All strategies have the following points in common:
  - Assess increasing risks associated with the use of new technologies
  - Lay out a vision for a secure cyberspace.
  - Protect national sovereignty in cyberspace.
  - Promote a culture of trust and cooperation between public and private stakeholders.
- Implementation is scheduled from 2008 to 2020.
- Public awareness, education, and citizen participation are emphasized.
- Increased cooperation is needed between the public sector and stakeholders from the private sector.

[65] EU 28 - National Cyber Security Strategies map: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

- There is an emphasis on national and international cooperation and collaboration.
- Risk assessment and management are stressed, particularly in relationship with the new technologies and the resulting threat environment.
- There are few qualified experts in the cyber security field.

In general, the strategies do not include specific requirements, best practices, or specific measures for the energy sector although there are many references to critical infrastructures. Furthermore, most of the strategies do not provide detailed information about how the strategic goals and visions should be achieved or put into practice.

7.13 Summary on Policies and Regulations

This chapter has given an overview on existing policy papers and legislation of the European Union who are available at the level of the European Commission. Existing policy papers and legislation of Member States have not taken into consideration as the task of the EECSP-Expert Group has been to focus on European level. Furthermore, a comprehensive analysis of Member States strategies, polices and legislation would be an exhaustive exercise that is beyond the capacity of the EECSP-Expert Group.

The policies and legislation described in this chapter can be grouped into following clusters:

Strategy papers:

- EU Cyber Security Strategy (section 7.3)
- Digital Single Market Strategy (section 7.1)

Legislation with focus on cyber security for critical infrastructure operators:

- Directive on security of Network and Information Systems (NIS) (section 7.5)
- European Programme for Critical Infrastructure Protection (EPCIP) Directive (section 7.6)
- Contractual Public-Private Partnership (section 7.2)

Legislation with focus on security of supply:

- Security of Supply (SoS) Directive (section 7.7)
- Security of Gas Supply Regulation (section 7.9)

Legislation and documents with focus on data protection and privacy:

- General Data Protection Regulation (GDPR) (section 7.11)
    - Data Protection Impact Assessment (DPIA) Template (section 7.11.1)

The European Commission proposals 2016:

- The European commission proposal on new rules for EU gas supply security
- 'Clean Energy for All Europeans' package

The strategy papers are cross-domain and therefore do not address the particular challenges of the energy sector or nuclear energy.

Legislation papers with focus on cyber security for critical infrastructure operators do consider the security of network and information systems for operators of essential services. For example, the NIS Directive and the EPCIP Directive do not differentiate security provisions among sectors. This is as well the case for the cPPP which targets as well across sectors. However, legislation papers such

as Security of (Gas) Supply do address the energy sector in particular, but does not focus on cyber security.

Today, cyber security for the civil nuclear energy fuel cycle is not explicitly addressed by legislation of the EU (i.e. EURATOM). The obligation is with the respective Member States. However, as stated in chapter 7.10, EURATOM indeed does share competence with the Member States in the area of physical protection of nuclear material and has in general a mandate for decision-making on measures of physical protection (including cyber security) for nuclear facilities in scope.

As no regulation for cyber security in nuclear energy currently exist at EU level, Member States often simply follow in their national approaches on computer security principles and methods developed by the IAEA, which offers a set of cyber security standards supplemented by the voluntary possibility of an advisory service (IPPAS[66]) of IAEA on State's request. However, not all EU Member States have already an effective legislation and regulation developed or implemented, as can, for example, be seen from the detailed evaluation of the Nuclear Threat Initiative (NTI) on security conditions[67,68,69].

Legislation papers with focus on data protection and privacy such as the GDPR Directive address the overall protection of European citizens and are therefore not sector-specific by nature.

[66] http://www-ns.iaea.org/security/ippas.asp
[67] http://ntiindex.org/overview-highlights/cybersecurity/
[68] http://www.ntiindex.org/sabotage-indicators/security-and-control-measures-2/
[69] http://ntiindex.org/wp-content/uploads/2016/03/2016-NTI-Index-Data-2016.03.25.zip

8. Gaps in Policy and Legislation

Chapter 7 has provided an overview on the existing policies and legislation of the European Union related to cyber security that is relevant for energy sector and nuclear energy. This chapter is going to compare the existing legislation in regards to the strategic areas identified in chapter 6. The focus of the analysis will be on the NIS Directive (chapter 7.5) and the GDPR Directive (chapter 7.11). However, other documents such as described in chapter 7 are considered in the analysis. Documents that includes strategies, policies and legislations, regulations, communication papers and action plans, frameworks and programs; the respective documents are referenced accordingly in the analysis work and the key documents are described in more detail in chapter 7.

The analysis is structured according to the strategic areas as derived in chapter 6:

No.	Identified Strategic Areas
1	European threat and risk landscape and treatment
2	Identification of operators of essential services
3	Cyber response framework
4	Crisis management
5	European cyber security maturity framework
6	Supply chain integrity framework for components
7	Capacity & competence build-up
8	Best practice and information exchange
9	Foster international collaboration
10	Awareness campaign from top level EU institutions

Table 9: Identified Strategic Areas

Each strategic area is analysed by looking into the following categories:

- Set-up: Evaluation if the existing set-up is supporting the strategic areas.
- Methodology: Evaluation if the methodology and processes defined in legislation and regulations are sufficient to support the strategic areas.
- Content: Evaluation if the content is sufficiently defined to fulfil the needs of the strategic areas. Content can mean available standards, definitions or guidelines. For example, in case of incident reporting, it looks, if it is clearly defined which information has to be reported.

8.1 European Threat and Risk Landscape and Treatment

The key points of this strategic area, see 6.1 for more details, are:

1. EU and Member States agree on a common threat and risk landscape.
2. Actively involve connected operators and Non-EU Member States such as Norway and Switzerland.
3. EU and Member States agree on how to address respective threats and risks (avoid, mitigate, transfer, and accept).
4. Member States and relevant Non-EU Member States include the European threat and risk landscape into their respective threat and risk treatment process.

The key legislation in this regard revolves around the ECIs Directive[70] and the NIS Directive. The former defines the energy sector and sets the basic arrangements for the exchange of information relevant for a risk and threat landscape between Member States and the Commission while the latter builds the base for a threat and risk landscape and treatment by implementing national CSIRTs and establishing reporting and information exchange capabilities between CSIRTs.

According to the NIS Directive, Member States have to identify operators of essential services who are obliged to report incidents to respective CSIRT of the Member States. Information exchanges among Member States are established on following channels:

- Within a CSIRT network, where participation is not limited to the CSIRTs of the Member States.
- With connected Member States in case of incidents that affects those.
- With the NIS Cooperation Group that targets harmonization of approaches and share best practices

ENISA is acting as an advisor to the Cooperation Group and Member States and provides the secretariat to the CSIRT network; it actively supports the cooperation among CSIRTs. A potential international collaboration with the Cooperation Group is stated in article 13 of the NIS Directive. The following figure gives an overview on the NIS Directive.

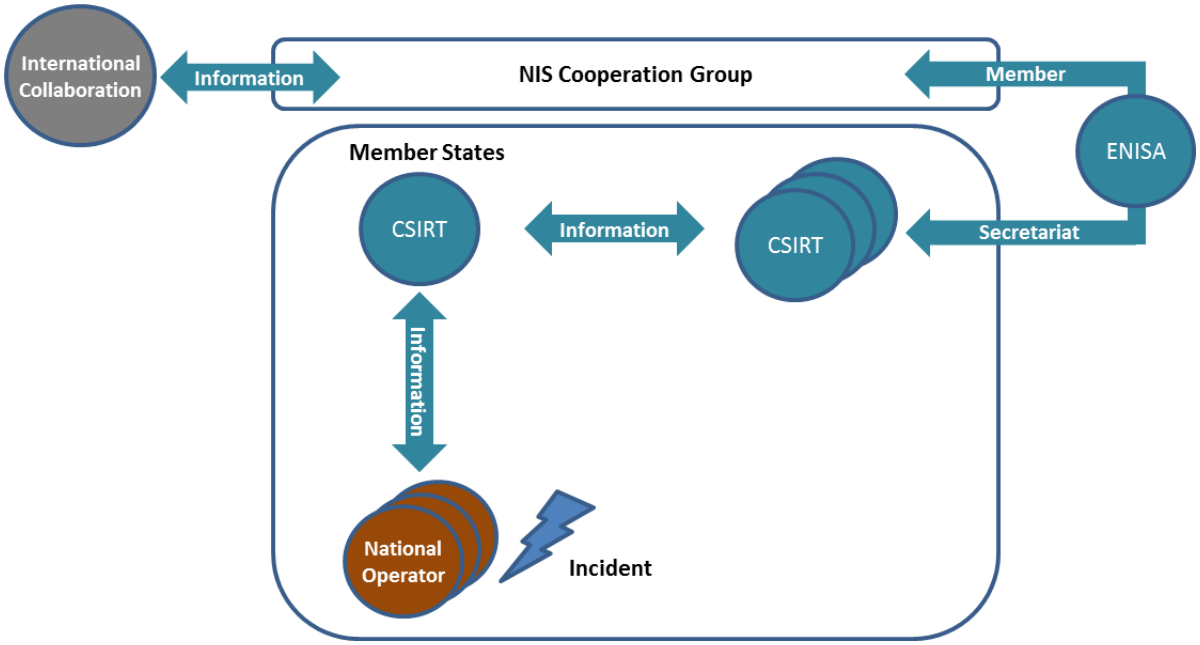

Figure 2: Overview on the NIS Directive

The NIS Directive responds in such to the action plan of the European Parliament on addressing cyber security at EU level[71]: 'Suggests that the Commission propose binding measures via the EU cyber incident contingency plan for better coordination at EU level of the technical and steering

[70] Directive on European Critical Infrastructure (ECIs):
Link: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:jl0013&from=EN

[71] Critical Information Infrastructure Protection (CIIP) Action Plan:
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2012-0237+0+DOC+PDF+V0//EN

functions of the national and governmental CERTs.', but do not fully anticipate the European Agenda on Security[72]: 'The EU must be able to react to unexpected events, seize new opportunities and anticipate and adapt to future trends and security risks.'. The NIS Directive provides a mechanism to report incidents, where a harmonization among Member States could be achieved either via the Cooperation Group (Article 11) or via further guidance of the European Commission (e.g. article 16 (9)). CSIRTs might provide early warnings as this is one of the tasks described in Annex I (2-ii). However, the NIS Directive does not take into consideration future trends and security risks that would be required to get to a common threat and risk landscape. A landscape, which use is already foreseen and put as an action plan in the European Programme for Critical Infrastructure Protection (EPCIP) by setting-up a Critical Infrastructure Warning information Network (CIWIN)[73].

Following gaps are identified by EECSP experts concerning set-up:

- CSIRT network is an 'open' network among CSIRTs, article 12 (2). This network does not meet the requirement for a closed ('trusted') group on CSIRTs to work on such a threat and risk landscape.
- Foster and enable close cooperation with law enforcement, intelligence services and counter-intelligence services and defence services are needed to provide such a landscape. The current directive defines cooperation with law enforcement mainly as a treatment of criminal acts (article 8 (6)). However, a pro-active approach is mentioned in the recital clause of the Directive.
- Electricity generation is not explicitly included in the NIS-Directive, therefore opens the field for interpretation by Member States.
- Nuclear energy is not explicitly included in the NIS-Directive, therefore opens the field for interpretation by Member States. Additionally, it does not cover the nuclear fuel-cycle. However, it must be noted, that nuclear energy is a very sensitive area that might requires a parallel set-up for potential activities such as incident reporting and information exchange.
- Connected non-EU Nation States have to be considered and involved. They are not part of the NIS Directive. Only the SOS Directive[74] considers 3rd party countries in the context of security of supply.
- Current set-up as defined in the NIS directive has a liaison character with the EU as secretary and advisory role. An operational role on EU level is missing.

Following gaps are identified by EECSP experts concerning methodology:

- The NIS Directive does not request domain specific expertise in the Cooperation Group and CSIRT set-up. This might be an issue as not all CSIRT procedures can be applied to the energy sector. For example, in nuclear energy, the access to a nuclear plant facility is strongly restricted as compared to non-nuclear power generation facilities. In the energy sector, the usage of devices for forensic purpose is not always possible or for operational reason not considered.

[72] European Agenda on Security: http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

[73] European Program for Critical Infrastructure Protection (EPCIP): http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al33260

[74] Security of Supply (SoS) Directive: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al27016

- The NIS Directive (article 7 (1-f)) requests Member States to identify cyber risks in their national strategy and article 14 (1) requests Member States to ensure that operators take appropriate technical and organisational measures. Not considered are threats, risks which require measures on national level and an agreed landscape and treatment.
- The ECIs Directive[75] (article 7) requests a reporting of risks, threats and vulnerabilities to the European Commission every two years, whereas the NIS Directive (article 10) requests Member States to provide a summary report on incidents to the Cooperation Group only. Based on the ECIs Directive, provisions of a threat and risk landscape are given as energy is explicitly mentioned as critical infrastructure. This is not appropriately reflected in the NIS Directive and requires further clarifications.
- The link between the information being exchanged in the context of the ECI Directive and the data which is envisaged to be communicated in the context of the NIS Directive has not been defined yet.
- The GDPR regulation[76] requires a reporting to the European Data Protection Board. As a consequence, the same incident might be reported twice to different authorities. The establishment of an unique reporting obligation has not been considered yet.

Following gaps are identified by EECSP experts concerning content:

- The information sharing on threats, risks and vulnerabilities is not well defined and lacking a common applicable classification scheme. An issue already identified in the ECIs Directive.
- No systematic and frequent exchange of actionable information relevant to Indicators of Compromise (IOCs) and Indicators of Attacks (IOAs) is defined.

8.2 Identification of Operators of Essential Services

The key point of this strategic area, see 6.1 for more details, is:

1. EU support on the identification of the operators of essential services in order to harmonize the process among Member States and to address the weakest link problem.

The key legislations in this regards are the NIS Directive and the Directive on European Critical Infrastructure (ECIs)[77]. The NIS Directive (article 5) requests Member States to identify operators of essential services according to the criteria pointed out in article 5 (2) and the sectors and subsectors as listed in Annex II. The criteria are listed as services which are critical for the well-functioning of the society and economy, services where the provision depends on networks and information systems and where an incident would have a significant disruptive effect. The ECIs Directive requests Member States to identify critical infrastructure operators based on causalities criteria, economic effects and public effects (article 3-2 a-c) with focus on energy and transport sector (article 3-3 and

[75] Directive on European Critical Infrastructure (ECIs), item (15) on page 2:
Link: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:jl0013&from=EN.
[76] General Data Protection Regulation (GDPR) – *Proposal*
Link: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
[77] Directive on European Critical Infrastructure (ECIs):
http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:jl0013&from=EN

Annex I). An exercise, which has been already encouraged by the European Program for Critical Infrastructure Protection (EPCIP)[78].

Following gaps are identified by EECSP experts concerning methodology:

- A harmonization of criteria for the identification of operators of essential services is not available. On one side, there might be a need to harmonize across the mentioned Directives, on the other side, the NIS Directive only partly address a harmonization by article 23 with the request to the Commission to report on the consistency of the approach taken by Member States. Furthermore, an exchange on best practices is requested by the Cooperation Group (article 11 3-l). A consistent set of commonly accepted criteria for the identification of the energy essential operators is missing.
- Electricity generation is not explicitly included in the NIS-Directive, therefore opens the field for interpretation by Member States.
- Nuclear energy is not explicitly included in the NIS-Directive, therefore opens the field for interpretation by Member States. Additionally, it does not cover the nuclear fuel-cycle. However, it must be noted, that nuclear energy is a very sensitive area that might requires a parallel set-up for potential activities such as incident reporting and information exchange.
- The NIS Directive, article 14, requests Member States to ensure operators of essential services to implement appropriate measures to manage the risks. This might lead to the point where a further differentiation and classification of essentiality could be considered to define different level of implementation depending on the criticality of an operator of essential services.

8.3 Cyber Response Framework

The key points of this strategic area, see 6.1 for more details, are:

1. A Cyber response framework that includes a classification of attacks, definition of responsibilities and capabilities needed to respond adequately on different levels of sophistication of cyber attacks.
2. Support from Member States or tighter coordination across Member States.
3. Seek for support from diplomacy (e.g. OSCE) and/or military (e.g. NATO).
4. All EU Member States to be included (as these do not correspond to NATO Nation States).
5. International alliances.
6. Coordination and information exchange between the attacked organisation, Member States, Nation States, EU, OSCE, NATO and international alliances and coordinated response mechanisms.

A potential cyber response framework could be based on existing legislative instruments[79] for a collective response. They are based on EU's Common Security and Defence Policy (CSDP) and are

[78] European Program for Critical Infrastructure Protection (EPCIP): http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al33260

supported by the Lisbon Treaty. The Critical Information Infrastructure Protection (CIIP) Action Plan[80] has already pointed out the need of a clear definition and differentiation of responsibilities as well as of a robust international cooperation mechanism. Additionally, the Joint Framework to counter hybrid threats[81] recognizes that EU Member States are not necessarily included in the NATO alliance.

Following gaps are identified by EECSP experts concerning set-up:

- European institutions and Member States have not acknowledged the need on a cyber response framework yet and have not agreed on a set-up supporting the goal to protect and defend European Union's energy sector.
- A coordinating role is missing at the European level.
- Non-EU Nation States directly connected to the energy network of the European Union are currently not sufficiently considered.

Following gaps are identified by EECSP experts concerning methodology:

- A EU-wide accepted cyber response framework is missing that should include the necessary processes in case of cyber attacks and promote cyber defence exercises such as the NATO Locked Shield exercise.
- Existing agreements establishing international alliances do not explicitly include treatment of cyber attacks.

Following gaps are identified by EECSP experts concerning content:

- A clear classification of attacks, definition of responsibilities and roles and an inventory of needed essential capabilities is missing.

8.4 Crisis Management

The key point of this strategic area, see 6.1 for more details, is:

1. Emergency plans and cyber exercises.

Various legislative instruments are in place for crisis management such as the mutual support clause[82], the civil protection mechanism[83] or the integrated political crisis response arrangements (IPCR). Additionally, the need on emergency plans is supported by several strategies and communication papers of the European Commission. The cyber security strategy[84] from the European Commission points out the importance of crisis management response mechanisms. A

[79] Legislative Instruments for Collective Defence and Managing Crises:
http://eur-lex.europa.eu/summary/glossary/collective_defence.html
http://eur-lex.europa.eu/summary/glossary/european_security_defence_policy.html
http://eur-lex.europa.eu/summary/glossary/solidarity_clause.html
http://eur-lex.europa.eu/summary/glossary/mutual_defence.html
http://ec.europa.eu/echo/what/civil-protection/mechanism_en
https://eeas.europa.eu/topics/crisis-response_en

[80] Critical Information Infrastructure Protection (CIIP) Action Plan:
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2012-0237+0+DOC+PDF+V0//EN

[81] Joint Framework 2016/18: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018

[82] Treaty of the functioning of the European Union, Article 222

[83] Treaty of the functioning of the European Union, Article 196

[84] Cybersecurity Strategy for the European Union, chapter 3.2:
http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

more efficient and coherent EU response on crisis management including joint field exercises is requested by the EU Agenda on Security[85]. This is pointed out by the internal security strategy communication[86], too, which asks for a joint, solidary approach in crisis management. Another example is the Directive on European Critical Infrastructure[87] which does request organisational measures on crisis management. None of the policy papers addresses crisis management caused by cyber incidents and attacks in detail. However, Europe supports Member States in terms of cyber security exercises, which are on request conducted by ENISA and the European Defence Agency (EDA). Contingency plans are encouraged by the European Program for Critical Infrastructure Protection (EPCIP)[88]. The importance of contingency plans and exercises in this regards on national and pan-European level are pointed out by the Critical Information Infrastructure Protection (CIIP) Action Plan[89].

Following gaps are identified by EECSP experts concerning set-up:

- In Europe, an EU on-going action (ERCC[90] – Emergency Response Coordination Centre under the European Commission – DG ECHO) exists that acts as an emergency response coordination centre, but a coordination role for cyber security is not included in its activities and missing within the European Union.
- The required capacity for handling of cyber security incidents in the context of crisis management needs to be reviewed in regards to a defined framework, see gap below.

Following gaps are identified by EECSP experts concerning methodology:

- Existing frameworks for crisis management typically do not address cyber security incidents and attacks and might not work when there is a major, long-lasting and wide-spread blackout, i.e. frameworks for crisis management within Member States and for a coordinated approach are missing.
- Exercises are crucial to proof the functioning of a framework, e.g. an exercise on a blackout scenario can lead to out-of-control situations when no communication between the operational teams is possible. Cyber exercises in the energy sector are not sufficiently advertised, considered and attended.

8.5 European Cyber Security Maturity Framework

The key points of this strategic area, see 6.1 for more details, are:

1. Harmonization of the protection level across the European Union.

[85] European Agenda on Security, chapter 2.2: http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

[86] Internal Security Strategy for the European Union, chapter 1: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0673&from=EN

[87] Directive on European Critical Infrastructure (ECIs), Annex II: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:jl0013&from=EN

[88] European Program for Critical Infrastructure Protection (EPCIP): http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al33260

[89] Critical Information Infrastructure Protection (CIIP) Action Plan: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2012-0237+0+DOC+PDF+V0//EN

[90] http://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en

2. Cyber security maturity framework as a tool to define a minimum level of security and as a tool to assess the overall protection level.

The need for harmonizing the resilience of the energy grid with a minimum level of security and high standards on data protection across Europe has been stated in the resolution of the European Parliament concerning critical infrastructure protection[91]. ENISA has the role of providing guidance and advising Member States, see EPCIP Directive[92]. The realization concerning data protection is done via the GDPR Regulation[93], see chapter 7.11 for more details. The NIS Directive[94] addresses the implementation of a minimum level of security by recommending the use of internationally accepted standards and specifications (article 19), but let the Member States define appropriate organisational and technical measures in a risk-based approach (article 14). Furthermore, the NIS Directive states in the recital clause (5) that the existing capabilities in the EU are not sufficiently developed and that the level of preparedness among the Member States led to a fragmented approach.

Following gaps are identified by EECSP experts concerning methodology:

- The NIS Directive is focussing on technical measures in implementation of security standards. Required capabilities needed in order to increase the resilience of the energy sector are not properly addressed.
- The harmonization of security implementation across the European Union is not sufficiently addressed as mainly the common base to rely on international standards and specifications is requested. As a consequence, the level of implementation is expected to be unequal across European Union.
- A minimum level of maturity has to be agreed when a maturity framework is available; see gap below.

Following gaps are identified by EECSP experts concerning content:

- A maturity framework is missing. Several parallel frameworks might be needed to take into consideration the specificities among the subsectors electricity, oil and gas and nuclear energy.

8.6 Supply Chain Integrity Framework for Components

The key point of this strategic area, see 6.1 for more details, is:

1. Supply chain integrity framework for components and suppliers.

This topic is not addressed by any EU policy paper known to the EECSP-Expert Group.

Following gaps are identified by EECSP experts concerning methodology:

[91] Critical Information Infrastructure Protection (CIIP) Action Plan, recital clause (I, K) and measures (5, 6): http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2012-0237+0+DOC+PDF+V0//EN

[92] European Program for Critical Infrastructure Protection (EPCIP) Directive: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Ajl0013

[93] General Data Protection Regulation (GDPR): http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[94] Directive on security of Network and Information Systems (NIS): http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN)

- A supply chain and integrity framework is not available today.

8.7 Capacity and Competence Build-Up

The key points of this strategic area, see 6.1 for more details, are:

1. Capacity and competence build-up for a mix of knowledge between the energy sector and cyber security.
2. Use or build-up of partner networks, training and skill certification programs, and education with academic curricula's, grants and programs.

The need of capacity and competences is outlined in nearly every policy paper analysed. For example, the EPCIP Directive[95] asks the Commission to launch a public pan-European education initiative and to promote cyber-security education and specialised training exercises in critical infrastructure protection. Information security trainings, curriculum for academic experts and specialised training exercises are recommended by the Critical Information Infrastructure Protection (CIIP) Action Plan[96]. The NIS Directive states in article 7 that Member States for adoption of a national strategy shall include an indication of the education, awareness-raising and training programmes as well as research and development plans in relation to the respective strategy. In the area of data protection, the GDPR regulation request in article 47 that cooperation's provide appropriate trainings to personnel that are having access to personal data. The effort on trainings is supported by the objectives in research, where cyber security is for example included in the Cyber Security Strategy for the European Union[97] by addressing the area of cyber security within the Horizon 2020 program and is part of the EU Agenda on Security[98], where training, research and innovation is supported.

Following gaps are identified by EECSP experts concerning set-up:

- A set-up supporting a systematic approach (see gap below) in order to build-up capacity and competences is missing.

Following gaps are identified by EECSP experts concerning methodology:

- There is no systematic approach to build-up capacity and competence.

8.8 Best Practice and Information Exchange

The key points of this strategic area, see 6.1 for more details, are:

1. Best practice and information sharing.
2. Fostering trust and collaboration among stakeholders.

Best practice sharing and information exchange aims to increase the overall resilience. The NIS Directive (article 11) has both, information and best practice sharing, described as key task for the

[95] European Program for Critical Infrastructure Protection (EPCIP) Directive, clause 28, 31: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Ajl0013

[96] Critical Information Infrastructure Protection (CIIP) Action Plan: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2012-0237+0+DOC+PDF+V0//EN

[97] Cybersecurity Strategy for the European Union: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

[98] European Agenda on Security: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

Cooperation Group. The Cyber Security Strategy of the European Union[99] sees the need to actively engage with the private sector for best practice sharing due the fact that most networks and information systems are privately owned and managed. In order to provide operators of critical infrastructure access to best practices and new technical developments on critical infrastructure protection, the ECI Directive[100] has asked the Commission for respective support. The European Program for Critical Infrastructure Protection (EPCIP)[101] ask for a multi-stakeholder dialogue on cyber security issues and encourages the Commission to make further efforts in this regards. A key problem in information exchange can be seen in the NIS Directive (article 12), where the exchange of sensitive information related to incidents is voluntary based on non-confidential information. As a consequence, one key task of the Cooperation Group (article 1) will be to build-up trust and confidence. An information hub is foreseen by the European Commission in order facilitate trust and cooperation among Member States[102]; however, the target and content are not yet clarified.

Following gaps are identified by EECSP experts concerning set-up:

- There is no EU supported pan-European trusted platform (e.g. ISAC) for exchanging actionable information around security incidents in the energy sector.

Following gaps are identified by EECSP experts concerning methodology:

- Trust building measures through the obligation of security clearance for Staff and Contractors involved, as in the case where EU Classified Information, could be considered as a prerequisite for sharing information among organisations such as CSIRT network and Cooperation Group. This will enable the possibility to share 'classified' relevant information, still respecting a 'need to know' principle and the existing legal frameworks. This must be supplemented by the use of specific certified communication means which may eventually provide a secure way to communicate the classified information, in line with the imposed security standards.

Following gaps are identified by EECSP experts concerning content:

- There are no common incident reporting criteria defined in the energy sector.

8.9 Foster International Collaboration

The key point of this strategic area, see 6.1 for more details, is:

1. International collaboration and alliances.

International collaboration and alliances are considered crucial for an effective cyber protection with collaboration and alliances with EU and Non-EU organisations as pointed out for example in the EU Agenda on Cyber Security[103] in the direction of cybercrime or in the Cyber Security Strategy[104] where

[99] Cybersecurity Strategy for the European Union, chapter 2.1: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
[100] Directive on European Critical Infrastructure (ECIs), article 8: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:jl0013&from=EN
[101] European Program for Critical Infrastructure Protection (EPCIP): http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al33260
[102] https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-410-EN-F1-1.PDF
[103] European Agenda on Security, chapter 1: http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

the collaboration among ENISA, Europol/EC3 and the European Defence Agency is recommended. International collaboration is seen as a core instrument by policy papers such as CIIP[105] an EPCIP[106]. In the context of the NIS Directive (article 13), the Cooperation Group can collaborate in some activities with third countries and international organisations.

Following gaps are identified by EECSP experts concerning methodology:

- The cooperation with EU and Non-EU countries and international organisations such as NATO and OSCE is not defined.

8.10 Awareness Campaign from Top-Level of EU Institutions

The key point of this strategic area, see 6.1 for more details, is:

1. Efficient treatment and cooperation among Member States.

Raising awareness is addressed by many policy papers such as Cyber Security Strategy[107] where it is stated as a common responsibility or the Cyber Security Strategy[108] mentioned as one instrument to promote a dialogue between stakeholders. The focus in the GDPR Directive (article 57) is the awareness rising in understanding of the risks, rules, safeguards and rights in relation to data processing. This is one task of the Cooperation Group as defined in the NIS Directive (Article 11).

Following gaps are identified by EECSP experts concerning methodology:

- As pointed out in the strategic area on international collaboration, the dialogue between stakeholders is crucial in order to achieve a more resilient Europe. Understanding the value of joint efforts among Member States, international alliances and in international collaboration requires awareness among stakeholders that should be facilitated and promoted by the top-level of EU institutions. A structured and comprehensive awareness program on cyber security for energy is missing and may be a starter to promote international collaboration.

8.11 Consolidation of Gaps and Mapping to Subsectors and Nuclear Energy

In chapter 6.3, four strategic priorities have been defined in order to categorize the strategic areas:

I. Set-up an effective threat and risk management system
II. Set-up an effective cyber response framework
III. Continuously improve cyber resilience
IV. Build-up the required capacity and competences

---

[104] Cybersecurity Strategy for the European Union, chapter 3.1: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

[105] Critical Information Infrastructure Protection (CIIP) Action Plan: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2012-0237+0+DOC+PDF+V0//EN

[106] European Program for Critical Infrastructure Protection (EPCIP): http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al33260

[107] Cybersecurity Strategy for the European Union, chapter 2.1: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

[108] European Agenda on Security, chapter 2.3: http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

The categorization is used to consolidate the gaps identified in the analysis in this chapter. Each gap has an indication for which subsector including nuclear energy it is relevant, but keep in mind that the potential impact differs for each subsector and nuclear energy.

Set-up an effective threat and risk management system

The following table summarizes the gaps that need to be addressed in order to meet the strategic priority to set-up an effective threat and risk management system:

Gap No.	Gap	Electricity	Oil	Gas	Nuclear
1	CSIRT network is an 'open' network among CERTs, article 12 (2). This network does not meet the requirement for a closed ('trusted') group on CSIRTs to work on such a threat and risk landscape.	x	x	x	x
2	Foster and enable close cooperation with law enforcement, intelligence services and counter-intelligence services and defence services are needed to provide such a landscape. The current directive defines cooperation with law enforcement mainly as a treatment of criminal acts (article 8 (6)). However, a pro-active approach is mentioned in the recital clause of the Directive.	x	x	x	x
3	Electricity generation is not explicitly included in the NIS-Directive, therefore opens the field for interpretation by Member States.	x			
4	Nuclear energy is not explicitly included in the NIS-Directive, therefore opens the field for interpretation by Member States. Additionally, it does not cover the nuclear fuel-cycle. However, it must be noted, that nuclear energy is a very sensitive area that might requires a parallel set-up for potential activities such as incident reporting and information exchange.				x
5	Connected Non-EU Nation States have to be considered and involved. They are not part of NIS Directive. Only the SOS Directive considers 3rd party countries in the context of security of supply.	x	x	x	x
6	Current set-up as defined in the NIS directive has a liaison character with the EU as secretary and advisory role. An operational role on EU level is missing.	x	x	x	x
7	The NIS Directive does not request domain specific expertise in the Cooperation Group and CSIRT set-up. This might be an issue as not all CSIRT procedures can be applied to the energy sector. For example, in nuclear energy, the access to a nuclear plant facility is strongly restricted as compared to non-nuclear power generation facilities. In the energy sector, the usage of devices for forensic purpose is not always possible or for operational reason not considered.	x	x	x	x

Gap No.	Gap	Electricity	Oil	Gas	Nuclear
8	The NIS Directive (article 7 (1-f)) requests Member States to identify cyber risks in their national strategy and article 14 (1) requests Member States to ensure that operators take appropriate technical and organisational measures. Not considered are threats, risks which require measures on national level and an agreed landscape and treatment.	x	x	x	x
9	The ECIs Directive[109] (article 7) requests a reporting of risks, threats and vulnerabilities to the European Commission every two years, whereas the NIS Directive (article 10) requests Member States to provide a summary report on incidents to the Cooperation Group only. Based on the ECIs Directive, provisions of a threat and risk landscape are given as energy is explicitly mentioned as critical infrastructure. This is not appropriately reflected in the NIS Directive and requires further clarifications.	x	x	x	x
10	The link between the information being exchanged in the context of the ECI Directive and the data which is envisaged to be communicated in the context of the NIS Directive has not been defined yet.	x	x	x	x
11	The GDPR regulation[110] requires a reporting to the European Data Protection Board. As a consequence, the same incident might be reported twice to different authorities. The establishment of an unique reporting obligation has not been considered yet.	x	x	x	x
12	The information sharing on threats, risks and vulnerabilities is not well defined and lacking a common applicable classification scheme. An issue already identified in the ECIs Directive.	x	x	x	x
13	No systematic and frequent exchange of actionable information relevant to Indicators of Compromise (IOCs) and Indicators of Attacks (IOAs) is defined.	x	x	x	x
14	A harmonization of criteria for the identification of operators of essential services is not available. On one side, there might be a need to harmonize across the mentioned Directives, on the other side, the NIS Directive only partly address a harmonization by article 23 with the request to the Commission to report on the consistency of the approach taken by Member States. Furthermore, an exchange on best practices is requested by the Cooperation Group (article 11 3-l). A consistent set of commonly accepted criteria for the identification of the energy essential operators is missing.	x	x	x	X
15	Electricity generation is not explicitly included in the NIS-Directive, therefore opens the field for interpretation by Member States. Note: Same gap as no. 3, but kept listed in order to avoid confusion as this gap relates to two strategic areas.	x			

[109] Directive on European Critical Infrastructure (ECIs), item (15) on page 2: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:jl0013&from=EN.

[110] General Data Protection Regulation (GDPR) – *Proposal* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Gap No.	Gap	Electricity	Oil	Gas	Nuclear
16	Nuclear energy is not explicitly included in the NIS-Directive, therefore opens the field for interpretation by Member States. Additionally, it does not cover the nuclear fuel-cycle. However, it must be noted, that nuclear energy is a very sensitive area that might requires a parallel set-up for potential activities such as incident reporting and information exchange. Note: Same gap as no. 4, but kept listed in order to avoid confusion as this gap relates to two strategic areas.				X
17	The NIS Directive, article 14, requests Member States to ensure operators of essential services to implement appropriate measures to manage the risks. This might lead to the point where a further differentiation and classification of essentiality could be considered to define different level of implementation depending on the criticality of an operator of essential services.	x		x	X
18	Trust building measures through the obligation of security clearance for Staff and Contractors involved, as in the case where EU Classified Information, could be considered as a prerequisite for sharing information among organisations such as CSIRT network and Cooperation Group. This will enable the possibility to share 'classified' relevant information, still respecting a 'need to know' principle and the existing legal frameworks. This must be supplemented by the use of specific certified communication means which may eventually provide a secure way to communicate the classified information, in line with the imposed security standards.	x	x	x	x
19	There are no common incident reporting criteria defined in the energy sector.	x	x	x	x
20	The cooperation with EU and Non-EU countries and international organisations such as NATO and OSCE is not defined.	x	x	x	x

Table 10: Identified gaps related to the strategic priority: (I) Set-up an effective threat and risk management system

Set-up an effective cyber response framework

The following table summarizes the gaps that need to be addressed in order to meet the strategic priority to set-up an effective cyber response framework:

Gap No.	Gap	Electricity	Oil	Gas	Nuclear
21	European institutions and Member States have not acknowledged the need on a cyber response framework yet and have not agreed on a set-up supporting the goal to protect and defend European Union's energy sector.	x	x	x	x
22	A coordinating role is missing at the European Level.	x	x	x	x
23	Non-EU Nation States directly connected to the energy network of the European Union are currently not sufficiently considered.	x	x	x	x

Gap No.	Gap	Electricity	Oil	Gas	Nuclear
24	A EU-wide accepted cyber response framework is missing that should include the necessary processes in case of cyber attacks and promote cyber defence exercises such as the NATO Locked Shield exercise.	x	x	x	x
25	Existing agreements establishing international alliances do not explicitly include treatment of cyber attacks.	x	x	x	x
26	A clear classification of attacks, definition of responsibilities and roles and an inventory of needed essential capabilities is missing.	x	x	x	x
27	In Europe, an EU on-going action (ERCC – Emergency Response Coordination Centre under the European Commission – DG ECHO) exists that acts as an emergency response coordination centre, but a coordination role for cyber security is not included in its activities and missing within the European Union.	x	x	x	x
28	The required capacity for handling of cyber security incidents in the context of crisis management needs to be reviewed in regards to a defined framework.	x		x	x
29	Existing frameworks for crisis management typically do not address cyber security incidents and attacks and might not work when there is a major, long-lasting and wide-spread blackout, i.e. frameworks for crisis management within Member States and for a coordinated approach are missing.	x		x	x
30	Exercises are crucial to proof the functioning of a framework, e.g. an exercise on a blackout scenario can lead to out-of-control situations when no communication between the operational teams is possible. Cyber exercises in the energy sector are not sufficiently advertised, considered and attended.	x	x	x	x

Table 11 Identified gaps related to the strategic priority: (II) Set-up an effective cyber response framework

Continuously improve cyber resilience

The following table summarizes the gaps that need to be addressed in order to meet the strategic priority to continuously improve cyber resilience:

Gap No.	Gap	Electricity	Oil	Gas	Nuclear
31	The NIS Directive is focussing on technical measures in implementation of security standards. Required capabilities needed in order to increase the resilience of the energy sector are not properly addressed.	x	x	x	x
32	The harmonization of security implementation across the European Union is not sufficiently addressed as mainly the common base to rely on international standards and specifications is requested. As a consequence, the level of implementation is expected to be unequal across European Union.	x	x	x	x
33	A minimum level of maturity has to be agreed when a maturity framework is available.	x	x	x	x

Gap No.	Gap	Electricity	Oil	Gas	Nuclear
34	A maturity framework is missing. Several parallel frameworks might be needed to take into consideration the specificities among the subsectors electricity, oil and gas and nuclear energy.	x	x	x	x
35	A supply chain and integrity framework is not available today.	x		x	x
36	There is no EU supported pan-European trusted platform (e.g. ISAC) for exchanging actionable information around security incidents in the energy sector.	x	x	x	x
37	As pointed out in the strategic area on international collaboration, the dialogue between stakeholders is crucial in order to achieve a more resilient Europe. Understanding the value of joint efforts among Member States, international alliances and in international collaboration requires awareness among stakeholders that should be facilitated and promoted by the top-level of EU institutions. A structured and comprehensive awareness program on cyber security for energy is missing and may be a starter to promote international collaboration.	x	x	x	x

Table 12: Identified gaps related to the strategic priority: (III) Continuously improve cyber resilience

Build-up the required capacity and competences

The following table summarizes the gaps that need to be addressed in order to meet the strategic priority to build-up the required capacity and competences:

Gap No.	Gap	Electricity	Oil	Gas	Nuclear
38	A set-up supporting a systematic approach (see gap below) in order to build-up capacity and competences is missing.	x	x	x	x
39	There is no systematic approach to build-up capacity and competence.	x	x	x	x

Table 13: Identified gaps related to the strategic priority: (IV) Build-up the required capacity and competences

The gaps identified are the basis for the recommendations on actions for the European Commission defined in the next chapter.

9 Recommendation on Actions for the European Commission

The thirty nine gaps identified in policy and legislation in chapter 8 have led to detailed recommendations for action by the European Commission. These actions are linked to the strategic priorities as defined in chapter 6.3:

I. Set-up an effective threat and risk management system.
II. Set-up an effective cyber response framework.
III. Continuously improve cyber resilience.
IV. Build-up the required capacity and competences.

This chapter will describe the recommended actions in detail for each strategic priority and provides an additional recommendation on the implementation timeline:

(S) Short Term: Until implementation of NIS Directive.
(M) Medium Term: Up to 5 years.
(L) Long Term: Beyond 5 years.

The intended outcome is to address the gaps identified in chapter 8; a mapping of the actions to the gaps are provided in chapter 9.5. Although not all findings identified in chapter 8 are relevant to all subsectors and nuclear energy, the consolidation of gaps and recommendation of actions can be applied to all domains as the few items, where a gap is not relevant, can be neglected.

9.1 Set-Up an Effective Threat and Risk Management System

The EECSP-Expert Group recommends action in 4 areas in order to address this strategic priority:

1. Identification of operators of essential services for the energy sector at EU level

The following actions are recommended:

1. Further to current provisions of Art. 5 of the NIS Directive, the European Commission, in cooperation with ACER and ENISA, shall recommend to the Member States and Cooperation Group a minimum set of criteria for the identification of operators of essential services in the energy sector. This shall include electricity generation. (S)
2. The European Commission in cooperation with EURATOM to give guidance to Member States on the elements of the nuclear fuel cycle which should be subject to the provisions of the NIS Directive (S).

2. Risk analysis and treatment

The following actions are recommended:

1. The European Commission should launch an analysis of possible cyber threat scenarios addressing the high-level objectives (see chapter 5) with their associated risks and to assess how to mitigate respective risks and associated mitigation costs. (S)
2. EURATOM to assess the status of the nuclear cyber security in Europe with the aim to ensure sufficient future cyber security readiness in nuclear energy across all Member States. (M)

3. Framework of rules for a regional cooperation

The EECSP experts recommends that the European Union follows an approach of regional cooperation within a common framework as already proposed and/or implemented in the energy sector for the regional cooperation on electricity[111] and the security of supply for gas[112]. Additionally, this is an already existing approach used by ACER[113] for some of its assigned tasks and it was indicated as the preferred approach for a set-up for TSOs based on the outcomes of Public Consultations[114]. The approach of regional cooperation should be used to build trust and to assure coordination in regards to cyber security within and among the already existing regions.

The regional cooperation has to build trust and coordination within and among EU energy regions using the already existing CSIRT network[115]. Furthermore, through the regional approach cooperation with EU neighbouring countries can be established and further developed and expanded.

The main tasks are to exchange information and identify minimum requirements for CSIRTs groups within and among regions to prevent, detect, respond and recover from cyber security incidents, in order to assure that security of supply is kept to an acceptable level in all energy related regions. The information exchange should be based upon rigourous risk assessment process tailored for the purpose, on the actual threat landscape and on known vulnerabilities, and should be based in a specific common ontology and on an agreed and shared classification schema and classification methodology.

As for nuclear energy a regional split would be meaningless, as a single region for EU can be considered more appropriate.

The following action is recommended:

1. The European Commission, in collaboration with the Member States, to establish a framework of rules for the regional cooperation of CSIRTs groups for energy. (M)
   The framework shall include rules for:
   a. The composition of CSIRTs teams in terms of minimum professional profiles in order to properly cover the energy field. (S)

---

[111] Regional Cooperation on Electricity:
https://ec.europa.eu/energy/en/commission-welcomes-reinforced-regional-cooperation

[112] Regional Cooperation in Securty of Gas Supply:
1) https://ec.europa.eu/energy/en/news/new-rules-boost-gas-supply-security-and-solidarity
2) https://ec.europa.eu/energy/sites/ener/files/documents/1_EN_ACT_part1_v10.pdf
3) South GRI: http://www.acer.europa.eu/en/Gas/Regional_%20Intiatives/South_GRI/Pages/default.aspx
4) South-East GRI: http://www.acer.europa.eu/en/Gas/Regional_%20Intiatives/South_South-East_GRI/Pages/default.aspx
5) North-West GRI: http://www.acer.europa.eu/en/Gas/Regional_%20Intiatives/North_West_GRI/Pages/default.aspx

[113] ACER on regional cooperation:
http://www.acer.europa.eu/en/Gas/Regional_%20Intiatives/Pages/default.aspx

[114] Public Consultation of the EC:
https://ec.europa.eu/energy/sites/ener/files/documents/First%20Results%20of%20Market%20Design%20Consultation.pdf

[115] NIS Directive: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013PC0048&from=EN

b. Regional rules for streamlining obligations for exchanging and processing information within the regional CSIRTs group and among the regions. The exchange of information related to incidents and vulnerabilities shall include indicators of compromise (IOCs) and Indicators of Attacks (IOAs). (S-M)
c. Developing trust in order to enhance and boost exchange of information among operators of other essential services, CSIRTs and the regional CSIRTs groups. (S-M)
d. Setting-up and maintaining a vulnerability, threat and risk regional landscape. (S)
e. Agreement on minimum protection profiles and security measures to put in place for the energy sector based on the risk and threat landscape at regional level. (M)
f. Assessment and recommendation of appropriate measures to Member States with a wider regional perspective, supplementing actions foreseen by existing EU and National regulations. (S-M)

4. EU framework for vulnerabilities disclosure for the energy sector

The following action is recommended:

1. A cPPP shall establish a common EU framework for vulnerabilities disclosure for the energy sector. The framework shall provide an ontology and a classification methodology for risks and vulnerabilities. (M)

9.2 Set-Up an Effective Cyber Response Framework

The EECSP-Expert Group has agreed on actions in 2 areas in order to address this strategic priority:

5. Define and implement a cyber response framework and coordination

The following action is recommended:

1. The European Commission, with assistance of ACER and ENISA, to propose to Member States a responsible body or bodies (e.g. regional CSIRT Cooperation Groups, see chapter 9.1) to set up a cyber response framework for the energy sector without prejudice to the already existing frameworks at international and national level. (S) The responsible body or bodies shall:
    a. Establish a cyber response framework that includes a classification of attacks, processes and escalation schemes, definition of responsibilities and capabilities needed to respond adequately on different levels of cyber-attacks. (M-L)
    b. Define and Implement cyber response coordination in cooperation with Member States, diplomacy (e.g. OSCE) and/or military (e.g. NATO). (S-M)
    c. Monitor and report on the implementation of the cyber response framework. (L)
    d. Cooperate with international alliances. (L)

6. Implement and strengthen the regional cooperation for emergency handling

The following action is recommended:

1. Each regional CSIRT Cooperation Group (see chapter 9.1) shall
    a. Act as a coordinating body in case of an emergency at regional level. (M)
    b. Intensively cooperate with the Emergency Response Coordination Centre (ERCC) at regional level.(M)

c. On regular basis, and/or prior or post a crisis phase, shall assess and make recommendations of emergency plans of Member States regarding their suitability and sustainability for major, long-lasting and wide-spread blackouts. (M-L)
d. Supervise and provide guidance to regular emergency exercises (with the aim to test the event of a cyber-incident and/or a deliberate cyber-attack) of Member States. This shall be planned and executed in cooperation with the Commission and with the support of EDA, ACER and ENISA. (S-M)

9.3 Continuously Improve Cyber Resilience

The EECSP-Expert Group would recommend actions in 3 areas in order to address this strategic priority:

7. Establish a European cyber security maturity framework for energy

The following action is recommended:

1. The Commission to analyse the needs, scope and coverage of a proposal for a secondary regulation for Europe wide definition of capabilities to ensuring a minimum level of cyber resilience maturity for the energy sector. (S)

8. Establish a cPPP for supply chain integrity

The following action is recommended:

1. The Commission to establish supply chain integrity framework for components and suppliers, used in processes handled by operators of essential services for energy, via a contractual public private-partnership (cPPP). (M)

9. Foster European and international collaboration

The following action is recommended:

1. The Commission should launch a forum with Member States, National Regulatory Authorities and/or National Competent Authorities (NRAs/NCAs) and stakeholders to promote awareness and foster confidence in freely and securely exchanging best practices, case studies (e.g. incidents), detected threats and potential new risks. It shall report to the NIS Cooperation Group. (S). This forum should be also a platform to foster and seek for international collaboration in the energy/ICT/security sectors. (M)

9.4 Build-Up the Required Capacity and Competences

The EECSP-Expert Group would recommend actions in one area in order to address this strategic priority:

10. Capacity and competence build-up

The following action is recommended:

1. The European Commission together with ACER and ENISA shall:
    a. Develop a systematic approach (certification program for specific technical curricula) to build up capacity and competences in cyber security in the energy sector. (M)
    b. Promote multi-level awareness programme (with top down approach) for the security in the energy sector.(S-M)

c. Support the build-up of a partner network for providing training, for establishing and operating certification programs and education with academic curricula. (M)

9.5 Mapping of Recommended Actions to the Identified Gaps

The recommended areas of actions are mapped to the gaps identified in chapter 8, to the strategic areas as identified in chapter 6 and linked to the strategic priorities as defined in chapter 6.3:

Strategic Priorities		Strategic Areas		Related Gaps	Areas of Actions
I	Set-up an effective threat and risk management system	1	European threat and risk landscape and treatment	1-13	(1) Identification of operators of essential services for the energy sector at EU level. (2) Risk analysis and treatment. (3) Framework of rules for a regional cooperation. (4) EU framework for vulnerabilities disclosure for the energy sector.
		2	Identification of operators of essential services	14-17	
		8	Best practice and information exchange	19	
		9	Foster international collaboration	20	
II	Set-up an effective cyber response framework	3	Cyber response framework	21-26	(5) Define and implement cyber response framework and coordination. (6) Implement and strengthen the regional cooperation for emergency handling
		4	Crisis management	27-30	
III	Continuously improve cyber resilience	5	European cyber security maturity framework	31-34	(7) Establish a European cyber security maturity framework for energy. (8) Establish a cPPP for supply chain integrity (9) Foster European and international collaboration
		6	Supply chain integrity framework for components	35	
		8	Best practice and information exchange	36	
		10	Awareness campaign from top level EU institutions	37	
IV	Build-up the required capacity and competences	7	Capacity & competence build-up	38-39	(10) Capacity and competence build-up.

Table 14: Overview table on strategic priorities, areas, related gaps and recommended actions

9.6 Remarks on Recommendations

While the recommendation on actions addresses the gaps identified by the EECSP experts, see chapter 8, a further discussion and alignment with respective stakeholders is recommended to fine-tune on the details to be established.

The analysis in this report has considered only European policy and legislation; existing regulation and legislation of Member States would have been beyond the capabilities of the EECSP-Expert

Group. It is recommended to clarify in advance that possible upcoming regulation and legislation does not contradict with existing international policy or national regulation and legislation (e.g. German IT security regulation for the energy sector[116]).

[116] http://www.gesetze-im-internet.de/bundesrecht/enwg_2005/gesamt.pdf, §11, 1a and 1b

10. Conclusion

As the report has pointed out the energy sector is undergoing substantial changes in infrastructure (chapter 5.2), in the structure of the markets (chapter 5.3) and in cyber security (chapter 5.4). With evolving cyber threats, our infrastructure is increasingly vulnerable for disruptive or destructive attacks. This report has proposed a strategic framework for the energy sector with the target to address the challenges found in the energy sector and in nuclear energy.

This strategic framework consists of 4 strategic priorities (chapter 6.3) which address key areas of threat and risk management (I), the cyber response in case of a cyber attack (II), the continuously improvement of cyber resilience (III) and the build-up of required capacities and competences (IV) for the energy sector. The overall objectives are to secure energy systems that are providing essential services to the European society and to protect the data in the energy systems and the privacy of the European citizens.

In order to meet current and future cyber security needs, the strategic priorities target organisational preparedness and maturity of organisations rather than demanding specific cyber security functionalities. This helps to address the dynamics in the energy sector and to anticipate and adapt to existing and emerging threats by the analysis and implementation of capabilities and appropriate in-time mitigation measures at EU, Nation and organisational level.

Key success factors to meet the overall objectives are the capabilities and competences of the people involved within the process and the ability of all the involved stakeholders to collaborate and cooperate across public and private organisations, Member States and international allies and partners. The recommendation for the European Commission given in this report (chapter 9) targets to provide the set-up and frameworks that allow an efficient, holistic and effective cyber security treatment in the European Union.

11. Annex

11.1 Annex A-1: Energy Expert Cyber Security Platform - Expert Group

The Energy Expert Cyber Security Platform (EECSP) has member[117] which are appointed either as individual expert or as expert representing a common interest, i.e. organisation. The following table provides the list of expert of the EECSP group:

Individual Experts:

Name of Expert
Stephan Beirer (Germany) GAI NetConsult GmbH
Giovanna Dondossola (Italy) RSE Research Company
Guido Gluschke (Germany) Institute of Security and Safety at the Brandenburg University of Applied Sciences
Annabelle Lee (United States of America) EPRI – Electric Power Research Institute
Rajesh Nair (Switzerland) Detecon (Switzerland) AG

Experts representing a common interest:

Name of Expert
Jean-Luc Trolle (France) EDF ENISS
Volker Distelrath (Germany) Siemens AG, Orgalime
Peter Kjær Hansen (Denmark) Dansk Energi, Eurelectric
Michael John (Germany) ENCS – European Network of Cyber Security
Jean-Pierre Mennella (France) GE, T&D Europe
Johan Rambi (Netherlands) Alliander EDSO/CEDEC
Armin Selhofer (Austria) Österreichs Energie GEODE

Former Members of the EECSP-Expert Group:

[117] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3341&NewSearch=1&NewSearch=1

Name of Expert
David Willacy (United Kingdom) National Grid, ENTSO-E
Philipp Irschik (Austria) E-Control, CEER

11.2 Annex A-2: Editorial Team

The Editorial Team is listed in the following table:

Experts	
Volker Distelrath	Editor & Editorial Team
Guido Gluschke	Editorial Team
Armin Selhofer	Editorial Team
European Commission & EU Agencies	
Manuel Sánchez-Jiménez	European Commission (DG ENER)
Michaela Kollau	European Commission (DG ENER)
Christian Kirchsteiger	European Commission (DG ENER – EURATOM)
Igor Nai-Fovino	European Commission (DG JRC)
Domenico Ferrara	European Commission (DG CNECT)
Stefano Bracco	Agency for the Cooperation of Energy Regulators (ACER)
Konstantinos Moulinos	Agency for Network and Information Security (ENISA)