Report on Cyber Security Information Sharing in the Energy Sector

FINAL

VERSION 1.1

PUBLIC

NOVEMBER 2016

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

ENISA

Contact

For contacting the authors please use cert-relations@enisa.europa.eu.
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

The authors would like to thank the following experts who took the time to be interviewed, and whose opinions and views have informed many of the findings and suggestions of this report:

- Aurélio Blanquet, European Energy - Information Sharing & Analysis Centre (EE-ISAC)
- Stefano Bracco, Agency for the Cooperation of Energy Regulators (ACER)
- Belisario Contreras, Organization of American States (OAS)
- Emmanuel Dauvin, Sibelga
- Sandro Etalle, Eindhoven University of Technology (TUE), The Netherlands
- Georgios Giannopoulos, Joint Research Centre (JRC) - European Commission
- Igor Nai Fovino - Joint Research Centre (JRC) - European Commission
- Alejandro Pinto González, formerly Directorate General for Communications Networks, Content & Technology (DG CONNECT) - European Commission
- Ferenc Suba, Cybersecurity Solutions Ltd., Hungary
- Per Atle Vagle, Statoil

Special thanks goes to the following subject matter experts who, in addition to providing their insights, performed a peer review of the report:

- Mircea Grigoras, CERT-RO, Romania
- Philipp Irschik, Council of European Energy Regulators (CEER)
- Marcelo Masera, Joint Research Centre (JRC) - European Commission
- Anjos Nijk, European Network for Cyber Security (ENCS)

The authors would like also to thank the members of the ENISA mailing list of European national and governmental CSIRTs for their help during the data collection phase and acknowledge the contribution of the experts from National Cyber Security Centre (NCSC), The Netherlands.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN: 978-92-9204-177-9, doi: 10.2824/960067

Corrigendum Notice

Footnote 1 updated.

Cover page image from http://www.shutterstock.com - Image ID: 212609554 - Copyright: Incomible

Table of Contents

Executive Summary

The internet has broken down barriers between countries and citizens, allowing sharing of information across the globe. Today networks and information systems underpin services, which support the functioning of our society and economy. Cyber security is increasingly becoming a key priority in light of the crucial role played by information and communications in economic and societal development. The energy sector and the services it provides is a prime example of the importance of cyber resilience and security, alongside other sectors, such as finance, transport and health. This is underpinned by efficient cooperation and information sharing among energy sector stakeholders - including ISACs (Information Sharing and Analysis Centres) and CSIRTs (Computer Security and Incident Response Teams) active in the energy sector, EU level public bodies, and national regulatory authorities - which enable them to better address risks, vulnerabilities and threats.

The need for high levels of cyber security in Europe is evidenced by recent statistics. "According to a recent survey[1], at least 80% of European companies have experienced at least one cybersecurity incident over the last year and the number of security incidents across all industries worldwide rose by 38% in 2015" (European Commission, 2016). More specifically, the energy sector is highly dependent on secure network and information systems. Major gas and electricity companies suffer increased numbers of cyber-attacks motivated by commercial and criminal intent. Symantec noted that an average of 74 attacks per day were launched in the world between 2012 and 2013 and that 16% of these attacks targeted the energy sector (Symantec, 2014), illustrating the need for an efficient sharing of cyber security information in the energy sector. The recent cyber-attacks against power plants in Ukraine (ICS-CERT, 2016) shown that information sharing is "key in the identification of a coordinated attack and directing appropriate response actions" (E-ISAC and SANS, 2016).

The purpose of this report is to understand and learn the development of CSIRTs, ISACs, as well as relevant initiatives on information sharing on cyber security incidents in the energy sector by focusing on the subsectors identified in the NIS Directive (European Parliament and Council, 2016) - namely electricity, oil and gas - complemented by the nuclear and alternative fuels subsectors.

The findings of this report are:

- **Trust is a key component of information sharing**, this being confirmed and emphasised by the experts interviewed for this report.
- Participants in information sharing initiatives are more committed and willing to contribute with information when their organisation backs them. Nevertheless, **time, resources and knowledge are some of the constraints faced by the participants** that might hinder information sharing.
- Only a few energy sector specialists have the in-depth understanding of both **the complexities of the energy systems and of cyber security**. In **lack of specialist knowledge**, service continuity and security cannot be adequately ensured.
- **Energy security issues are often addressed only at the Member State level** (i.e. with a national focus only) without taking into account the complexity of the interdependence of Member States in multiple aspects of the energy area, including cyber security.
- The **legal and policy context is complex and fragmented.** Moreover, **energy relevant legislation does not address in detail cyber security** and more specifically information sharing.
- **Possible legal constrains** might result in difficulties to share information on cyber incidents.

[1] In the document referenced a link to this survey is provided. For more information, see p. 52 (reference to European Commission, 2016).

- Information security **standards tailored to the specificities of the energy sector are used** to support the implementation of security controls **but** they are **not enforced**.
- The **quality of the shared information** is not always at the required level, for example due to inconsistent use of the applicable taxonomy.
- Participants in the initiatives have **conflicting interests**, ranging from business development and commercial relationship-forging, as opposed to actual information sharing.
- There is a **need to create public-private partnerships** when sharing information.
- Information is shared between **heterogeneous players** who come from different regulatory environments or cultures, different maturity levels for cyber security management and different subsectors, making the exchange of information more challenging.
- **Smaller** energy companies do not have the needed **size** to build information security risk management capabilities, which **might limit their participation to sharing initiatives**.
- Many companies in the sector give **more importance to the safety of their physical infrastructure** than to the security of their computer, process systems and data.
- **Few good practices** have been identified on the subject, and the current information sharing initiatives lack visibility within companies in the energy sector.

Core recommendations include:

1. Energy sector companies (high-level management and IT management) should adequately **invest in cyber security and cyber security information sharing.**
2. **High-level (top) management and IT management** of energy sector companies should be **more involved in cyber security issues**. ENISA and information sharing initiatives' facilitators should develop material and provide opportunities to **disseminate the message that the involvement of management of energy companies in cyber security issues is essential**.
3. One of the ISACs or information sharing initiatives' facilitators/moderators, if needed with the support of ENISA, should **compile and keep updated a map** of all energy ISACs, CSIRTs (public or private) and existing information sharing initiatives. In addition, the members of an ISAC or an information sharing initiatives should **promote** their **initiative externally** in order to have all the relevant actors' part of it.
4. EU and national policy makers, lawmakers and regulators should **continue working together toward a legal framework as clear and as harmonised as possible** to share information on cyber incidents. ENISA could support them by injecting expertise.
5. Facilitators and members of an ISAC or of information sharing initiatives should **promote the use of already existing definitions and of a common taxonomy for sharing information about incidents,** and should **enhance the information flow internally and with other ISACs and information sharing initiatives**.
6. Members of ISACs/information sharing initiatives and information sharing initiatives' facilitators should **ensure trust** among the members by following good practices and by using tools to build and maintain it.
7. Energy sector companies, information sharing initiatives' facilitators and members of ISACs and information sharing initiatives in the energy sector should **leverage on the cyber security work performed in other sectors** such as the financial and the chemical sectors and apply lessons learned from these sectors.
8. Standard developing organisations, energy companies, and facilitators of sharing initiatives should **further develop and enable adoption of standards on information and cyber security management in the energy sector**. ENISA could support this process by identifying gaps and proposing possible solutions.

1. Introduction

This introductory chapter provides information about the report itself, including its purpose, background, objectives and scope, as well as intended target audience, key concepts and definitions employed.

1.1 Purpose

The purpose of this report is to understand and learn from the key developments of CSIRTs, ISACs, as well as relevant initiatives on information sharing on cyber security incidents in the energy sector. In particular, this report covers a number of subsectors of the energy sector, as follows: electricity, oil, gas, nuclear and alternative fuels.

Although this report focuses on information sharing on cyber security incidents, it also contains some considerations - derived from the data collected - about information sharing on cyber security in general (e.g. sharing of good practices and lessons learned) in the energy sector.

1.2 Background of the Report

The ENISA Work Programme for 2016 includes Strategic Objective 4 (SO4) "To enhance cooperation both between the Member States of the European Union and between related network and information security communities" (ENISA, 2016). SO4 covers aspects of cooperation between the EU Member States (MSs) and the EU and between related NIS communities where ENISA could play a role to enhance NIS cooperation.

Work package (WPK) 4.2 "Network and information security community building" under SO4 has a key goal of "build[ing] upon the good experience ENISA has acquired in supporting different operational communities, such as CSIRTs, law enforcement communities, European FI-ISAC, A-ISAC, CSIRT network provided for by the NIS Directive [European Parliament and Council, 2016] to enhance mutually satisfactory ways to collaborate". This comprises the following objectives:

- Support incident response community building and information exchange;
- Contribute to the existing communities' efforts in incident response field;
- Enable continuous trust and collaboration building for communities through regular events;
- Provide Information to key stakeholders on NIS policy developments.

One of the deliverables foreseen in WPK 4.2 is Deliverable 5: "D5: Review on new operational communities' development (A-ISAC, etc.)". This report, focused on the energy sector, has been prepared as the implementation of this deliverable.

1.3 Report Objectives and Scope

1.3.1 Report Objectives

The main objectives of this report are:

- Identification of the existing CSIRTs, ISACs and European information sharing initiatives in the energy sector;
- Analysis of problems and shortcomings that initiatives within this sector are facing when sharing information on cyber security incidents;
- Identification of good practices that are suitable for the energy sector (including incentives to create and maintain CSIRTs, ISACs and other initiatives);

- Formulation of suitable recommendations on information sharing on cyber security incidents in the energy sector that address the identified problems and shortcomings.

1.3.2 Report Scope

The geographical scope of this report consists of EU Member States as well as the EFTA countries[2]. As the territory of these countries are taken into account, this means that the maritime territory is also part of the report scope in order to include, for instance, deep sea drilling activities.

The key subsectors in scope of this report include indeed:

- electricity
- oil
- gas
- nuclear
- alternative fuels

While the subsectors electricity, oil and gas were specifically highlighted in the Annex II of the NIS Directive (European Parliament and Council, 2016), the scope of this report is broader and includes the nuclear and alternative fuels subsectors as well.

The main segments of the different subsectors are taken into account in this report: for instance, as far as it concerns the electricity subsectors, generation, transmission and distribution, energy supply and power exchange platforms are considered. In the same way upstream, midstream and downstream segments are considered for the oil and gas subsectors.

1.4 Target Audience

The intended target audience for the report is primarily the national and governmental CSIRTs and other types of CSIRTs with activities and constituencies in the energy sector. Policy and lawmakers, notably the European Commission at the EU level, any public and private organisations with an interest in NIS, as well as other interested parties engaged in information sharing initiatives within the energy sector, including energy operators, are also intended audiences.

1.5 Key Concepts and Definitions

In the context of this report, the following definitions apply – see alphabetically[3]:

- **Computer Security and Incident Response Team (CSIRT)** or **Computer Emergency Response Team (CERT)** refer to "an organisation that studies computer and network security in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and to offer other information to help improve computer and network security". At present, "both terms (CERT and CSIRT) are used in a synonymous manner, with CSIRT being the more precise term" (ENISA, 2015 and ENISA, 2015a).

[2] "Norway and Switzerland were among the founding Member States of EFTA [European Free Trade Association] in 1960. Iceland joined EFTA in 1970, followed by Liechtenstein in 1991. Norway, Iceland (from 1994) and Liechtenstein (from 1995) are also parties to the European Economic Area (EEA) Agreement with the European Union, while Switzerland has signed a set of bilateral agreements with the EU" (EFTA, n.d.).
Please note that in the references 'n.d.' is used in the case when no date could be found for the cited sources.

[3] A majority of these definitions were also used in the 2015 ENISA report 'Cyber Security Information Sharing: An Overview of Regulatory and Non-Regulatory Approaches (ENISA, 2015a).

- **Computer system** refers to a system consisting of one or more computers and associated software that use common storage for all or part of a program and for all or part of the data necessary for the execution of the program. The computer system performs user-designated data manipulation, including arithmetic and logic operations.
- **Cyber risks** are defined as “the combination of the probability of an event within the realm of networked information systems and the consequences of this event on assets and reputation” (World Economic Forum, 2012).
- **Cyber safety** refers to a “condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event in the Cyberspace which could be considered non-desirable” (ISO, 2012).
- **Cyber security** refers to “the safeguards[4] and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure” and it “strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein” (European Commission, 2013). As highlighted in some previous ENISA work (ENISA, 2014a), in the academic context the “most widespread is the notion according to which cyber security is identified with information security, which refers to protection of information and information systems against being broken into, used, spread, or subjected to service interruptions, unauthorised changes, or destruction, with the aim of guaranteeing their confidentiality, integrity, and availability”. In a good practice context, cyber security refers to the “[p]reservation of confidentiality, integrity, and availability of information in the Cyberspace”.
- **Cyber threats** refers to “threats applying to assets related to information and communication technology. Such threats are materialized mostly in cyberspace, while some threats included are materialized in the physical world but affect information and cyber-assets” (ENISA, 2016c).
- **Cyber vulnerabilities** are susceptibilities or insufficient defences in the protection of an asset or group of assets and capacities from cyber threats (World Economic Forum, 2012).
- **Incident** is an event that has been assessed as having an actual or potentially adverse effect on the security or performance of a system (ENISA, n.d. [5]). Subcategories of incidents are information security (IT) incidents and cyber incidents. These terms are often used interchangeably.
- **Industrial control systems (ICS)** refer to supervisory control and data acquisition systems, distributed control systems, programmable logic controllers used in industrial facilities to monitor, control and supervise industrial processes. “ICS are typically used in industries such as electric, […] oil and natural gas, […], chemical and pharmaceutical”, and many more (NIST, 2011). It must be noted that “A cyber-incident impacting an industrial control system can have a significant negative impact not only on the organisation itself; it can also harm national security, cause injury or death of organisation employees or community members, damage equipment or the environment, or disrupt supply chains” (ENISA, 2013).
- **Information sharing** means “the exchange of a variety of network and information security related information such as risks, vulnerabilities, threats and internal security issues as well as good practice” (ENISA, 2010).
- **Information sharing initiative** means actions taken, in the form of activities or projects which support and solve challenges facing information sharing (ENISA, 2010).

[4] It must be noted that the term “safeguards” is used in this context with a different meaning than commonly used in the specific nuclear energy field where safeguards refer to activities to “verify that a State is living up to its international commitments not to use nuclear programmes for nuclear-weapons purposes” (IAEA, n.d(a)).

[5] ‘n.d.’ is used in the case when no date could be found for the cited sources.

- **Intra-sector information sharing** refers to communication of information between communities within the same sector (ISO, 2012a).
- **Information Sharing and Analysis Centres (ISACs)** are trusted entities established by critical infrastructure owners and operators to foster information sharing and good practices about physical and cyber threats and mitigation (National Council of ISACs, n.d.).
- **National and governmental CSIRTs** are "teams that serve the government of a country by helping to protect the critical information infrastructure. [National and governmental CSIRTs] […] play a key role in coordinating incident management with the relevant stakeholders at national level. They also bear responsibility for cooperation with the national and governmental teams in other countries" (ENISA, n.d.(a)).
- **Network and Information Security** means "the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems" (European Parliament and the Council, 2016).
- **Resilience** is "also known as 'Critical Infrastructure and Information Protection' (CIIP) […]. By the use of the term resilient, we characterise the networks that provide and maintain an acceptable level of service in face of faults (unintentional, intentional, or naturally caused) affecting their normal operation" (ENISA, 2011). In other words, resilience is a "concept associated with resisting to the loss of capacity of a failure or foreseen overload, optimizing the availability and quality of service of telecommunications systems and support resources enabling a system to return to a previous normal condition" (ENISA, 2011a).
- **Traffic Light Protocol (TLP):** is a "means for someone sharing information to inform their audience about any limitations in further spreading the information. […] The TLP can be used in all forms of communication, whether written or oral. […] The TLP is in principle easy to use: the sharer of information tags the information with a colour. […] The meaning of the colour indicates the possibilities for further spreading of the information" (ENISA, n.d.(b)). There exist different wordings of the TLP, but most of them boil down to:

Table 1: TLP – Colours, Meaning and Examples

COLOUR	MEANING	EXAMPLE
RED	Not for disclosure, restricted to participants only. Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.	Information shared with people in a meeting; direct email.
AMBER	Limited disclosure, restricted to participants' organizations. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources	Sharing of Indicators of Compromise (IoCs) to an organisation's CSIRT. These could be forwarded to the SOC [Security Operations Centre] for further action.

COLOUR	MEANING	EXAMPLE
	are at liberty to specify additional intended limits of the sharing: these must be adhered to..	
GREEN	Limited disclosure, restricted to the community. Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.	Sharing of a malware analysis with a specific sector.
WHITE	Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction..	Public security advisory.

Source: ENISA, n.d.(b)

"Tagging information consists simply of adding "TLP: COLOUR" on a document or part of it" (ENISA, n.d.(b)).

The concept of TLP was originally developed by the UK Centre for the Protection of National Infrastructure (CPNI). However, since then a number of slightly different variations have appeared and are currently in use (Millar, 2015). "CSIRT community recently made an effort to clarify[6] the TLP" (ENISA, n.d.(b).

- **Trust:** "Trust can be defined in terms of a set of expectations […Fukuyama, 1996]. Previous work by ENISA […(ENISA, 2012)] shows that […CSIRT] that meet the following expectations are more likely to be trusted by other […CSIRTs]:
  - Technical expertise
  - Active membership in […CSIRT] initiatives
  - Ability to respond quickly and act on security threats
  - Stability of the team
  - Maturity level of the team

In other words, a trusted […CSIRT is a] mature team that acts on shared information and shares back" (ENISA, 2014b). This definition of trust in the context of this report is also applicable to organisations participating in ISACs and information sharing initiatives in general.

[6] Reference is made here to https://www.first.org/tlp, last access 10 October 2016.

2. Methodology

In line with the report objectives as outlined in Chapter 1, the report work done is based on a multi-dimensional qualitative methodological approach, including a desk review of the key legal and policy documents, as well as other sector specific literature.

Interviews were conducted with key experts and relevant stakeholders from the CSIRTs, ISACs and from the information security and cyber security community focusing on the energy sector and data collected was analysed and corroborated with additional desk research information.

The European national and governmental CSIRTs were also briefly consulted via the dedicated ENISA mailing list. In addition to these sources, validation of the findings and conclusions was provided by four subject matter experts.

2.1 Information Collection Instruments Used

2.1.1 Desk Research

A key part of the information presented in this report was collected through desk research based on both public and non-public information sources. A wide and diverse array of sources - public, private, business and academia - were consulted, including websites of the European institutions, ENISA deliverables, public databases, research engines, and publications of external bodies. This type of analysis was fundamental to understand, in the first steps of the report, the specifics of the energy sector, and of the CSIRTs, ISACs and other stakeholders involved in information sharing initiatives.

After the interviews (see Section 2.1.2), a supplementary desk research was also performed to look for in-depth data based on the information received by the stakeholders and to complement it.

2.1.2 Interviews

Fifteen interviews were conducted with the respondent out of a pool of thirty-six potential respondents selected based on the criteria described in Section 2.2.1. The team conducted the interviews, either in person (with the stakeholders located in Brussels, Belgium) or via phone. The interviews were conducted mainly during the month of June 2016. Each interview lasted around one hour. The somewhat modest response rate is attributed to the fact that several respondents were unavailable during the summer months. This was mitigated by an in-depth review of the subject matter experts.

The interviews were carried out in a semi-structured manner allowing for auxiliary questions and for new lines of questioning depending on the responses of the respondents. During the interviews, the report team followed an agreed-upon protocol (see Annex B) covering all the different themes that were treated during the interviews. However, interview respondents were free to discuss additional relevant topics they considered as important or interesting.

Note taking was used to capture the content of the interviews. Interviewees were assured of non-attribution and anonymity when using direct quotes, unless they gave the study team explicit consent to be quoted. As a result, in reporting on the interviews in this report, a quasi-anonymous approach is followed, with references only being made to a participant's role or type of host organisation, i.e. CSIRT, private sector actor, energy company/organisation, policy-making body, or other.

2.1.3 Brief Survey via the ENISA Mailing List of European National and Governmental CSIRTs

The following brief question was sent on 8 June 2016 to the ENISA closed mailing list of European national and governmental CSIRTs, which include addressees of around forty teams: "Are you aware of any CSIRTs, ISACs or other cyber security incident information sharing initiative in the energy sector in your country?"

Only a few, but very detailed, replies were received and used to complete and further validate the data collected via desk research and with the interviewees.

2.2 Selection and Classification of the Stakeholders

2.2.1 Selection Criteria

For the purpose of this report, a set of selection criteria was adopted to ensure the contribution of a wide range of stakeholders and respondents as a part of the interviews during the data collection phase. The following main criteria guided the selection of relevant respondents from the energy sector:

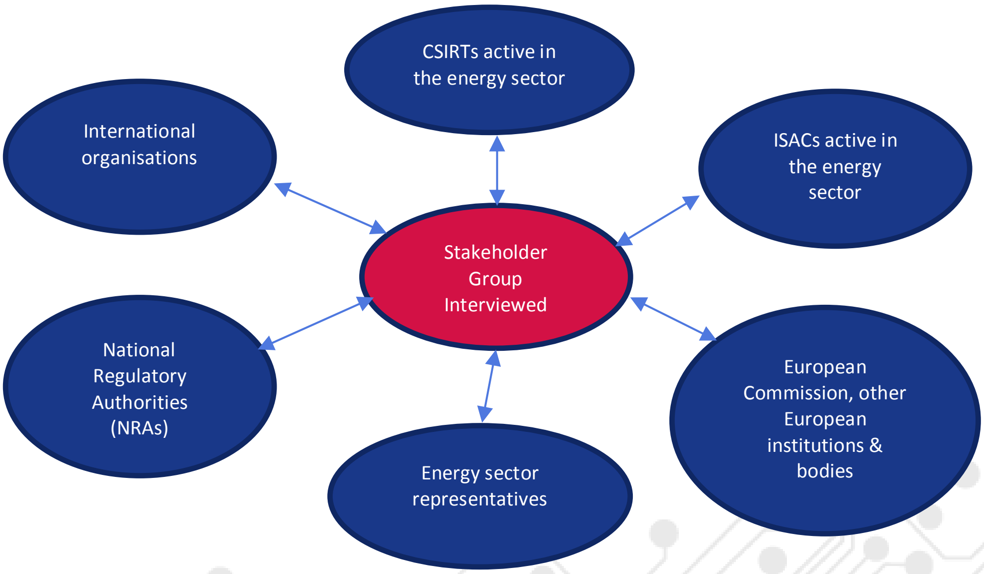
- The **size** of the CSIRT/ISAC/initiative in the energy sector – a mix of small, medium and large size CSIRTs/ISAC/initiatives, was considered as useful to include in the report in order to collect views from various perspectives.
- The focus of activities within the **energy sector** – the aim was to involve a balanced group of stakeholders reflecting the different subsectors (electricity, oil, gas, nuclear, and alternatives) in scope of the report.
- The **geographic location** (national, pan European or international) – a geographical spread was considered as beneficial for the report.
- **Level of engagement and maturity** of information sharing initiatives (e.g. website, articles, working groups, task and forces), to the extent information about their activities is available to the public;
- Wide coverage of **governmental, national or private sector** driven CSIRTs/ISAC's/initiatives.

2.2.2 Stakeholders

The stakeholders interviewed for the purpose of this report included the following categories:

- CSIRTs active in the energy sector
- ISACs active in the energy sector
- European Commission, other European institutions and bodies
- Energy sector representatives (cyber)
- National Regulatory Authorities (NRAs)
- International Organisations.

Figure 1 – Overview of Host Organisations of Interview Respondents


CSIRTs active in the energy sector
International organisations
ISACs active in the energy sector
Stakeholder Group Interviewed
National Regulatory Authorities (NRAs)
European Commission, other European institutions & bodies
Energy sector representatives

2.3 Contribution by Subject Matter Experts

In order to increase the quality and to make sure that the content of the work performed reflects the reality, four external experts were asked to review and validate this report. The external reviewers were selected based on their knowledge of the energy sector and their involvement in information sharing initiatives on cyber security. The reviewers are part of the EU public or the private sector.

For this purpose, the draft report was submitted to all four external reviewers. Feedback on the draft was integrated into the final report.

3. Policy Context

This chapter presents the key strategic documents outlining the EU policies in the domain of energy and network and information security. It also provides a high-level description of the energy regulators in the EU.

3.1 EU Energy Policy

3.1.1 European Energy Security Strategy

The 2014 Energy Security Strategy (European Commission, 2014) was developed in response to concerns about Europe's dependency on imported energy (since the EU imports more than half of all the energy it consumes) and the need for stable and abundant supply of energy for European citizens and the economy. The total import bill is more than €1 billion per day (European Commission, n.a.(b)). In particular, many EU Member States are heavily reliant on a single (or very few) energy supplier(s), some of which entirely relying on Russia for e.g. natural gas. This dependence leaves them vulnerable to supply disruptions, be it related to political or commercial disputes, or infrastructure failure.

Hence, the EU was in need of a "hard-headed strategy for energy security which promotes resilience to these shocks and disruptions to energy supplies" (European Commission, 2014). However, in relation to the protection of critical infrastructure, the strategy emphasises that while the EU has started to develop a policy to address important issue of securing energy supply and ways to ensure the "physical protection of critical infrastructure (against threats, hazards, etc.), which includes energy infrastructure"[7] (European Commission, 2014), IT security should be given "increasing attention" (European Commission, 2014). Moreover, several Framework Guidelines were drafted with the cooperation of the European Commission, Agency for the Cooperation of Energy Regulators (ACER) and European Network of Transmission System Operators of Electricity promoting cross-border cooperation between operators and regulatory authorities in case of issues. Yet, the five key actions proposed in the strategy to address long-term security of supply challenges do not include any IT security related measures.

3.1.2 Energy Union Package

The Energy Union (European Commission, 2015) aims to ensure affordable, secure and sustainable energy for Europe. It builds on the 2030 Climate and Energy Framework and the Energy Security Strategy, while integrating several policy areas into a single unified strategy. It proposes specific measures covering five key areas, including energy security, energy efficiency and decarbonisation. The Energy Union Framework Strategy is based on the three long-established objectives:

- security of supply
- sustainability
- competitiveness.

It is primarily the first objective which focuses on "energy security, solidarity and trust" that is relevant to this report. Echoing the Commission's energy security strategy, the aim is to make the EU less vulnerable to

[7] In European Commission, 2014 reference is made here to the Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Council of the European Union, 2008).

external energy shocks and reduce dependency on specific fuels, energy suppliers and routes. The proposed measures intend to ensure the diversification of supply (energy sources, suppliers and routes), encourage Member States and the energy industry to work together to ensure security of supply, and increase transparency on gas supplies – in particular for agreements on buying energy from non-EU countries.

The only explicit reference to cyber security in the Energy Union Package document is in relation to "develop synergies between the Energy Union and the Digital Single Market agenda and take measure to ensure privacy protection and cyber security" (European Commission, 2015).

3.1.3 European Programme for Critical Infrastructure Protection

In 2008, the Council of the European Union adopted the "Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection" (Council of the European Union, 2008). It has the objectives of establishing a procedure for the identification and designation of European critical infrastructures (ECIs), and a common approach to the assessment of the need to improve the protection of such infrastructures in order to contribute to the protection of people. In terms of the scope, the Directive lists transport and energy as the target sectors within which critical infrastructures should be identified. The following energy subsectors are included:

- electricity
- oil
- gas.

Acknowledging the importance of information sharing regarding ECIs, the Directive stresses that this is done coherently in a secure environment, to ensure trust building among the companies and organisations involved. Moreover, this Directive lays down that each Member State implements an appropriate communication mechanism between the relevant state authority, and the Security Liaison Officers[8] "with the objective of exchanging relevant information concerning identified risks and threats in relation to the ECI concerned" (Council of the European Union, 2008).

3.2 EU Network and Information Security Policy

3.2.1 Europe 2020 and the Digital Agenda for Europe

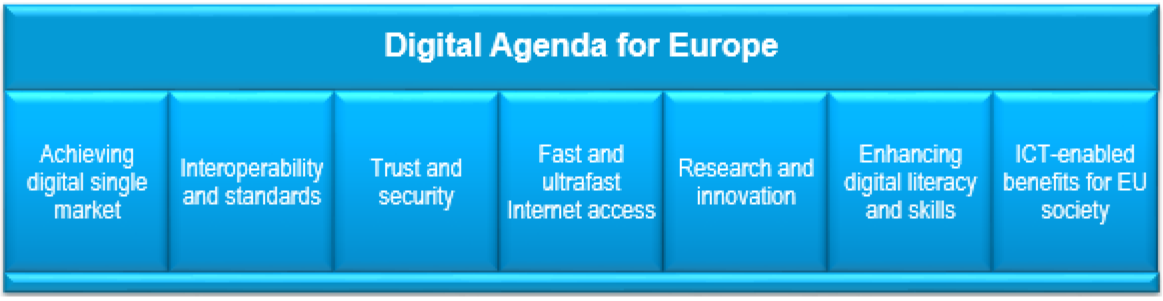
Over the past decade, EU policy makers have launched a number of digital policy initiatives with the ambition of paving the way for Europe to make the most of Information and Communication Technologies (ICT) in economic and societal growth.

Europe 2020 (European Commission, 2010) is a key EU growth strategy for the coming decade, with the aim to support the exit from the economic crisis and to prepare the EU Member States economies for the next challenges. Its vision is to achieve high levels of employment, a low carbon economy, productivity and social cohesion. One of the seven flagship initiatives of the Europe 2020 strategy for smart growth is the Digital Agenda for Europe (European Commission, 2010a) (hereunder "DAE" or "Digital Agenda").

[8] As stated in the Directive "the Security Liaison Officer shall function as the point of contact for security related issues between the owner/operator of the ECI and the relevant Member State authority" (see Article 6 of Council of the European Union, 2008).

The Digital Agenda defines the key enabling role that the use of Information and Communication Technologies will have to play if Europe wants to succeed in its ambitions for 2020. The Digital Agenda frames its key actions around the need to tackle seven challenges (i.e. "pillars") linked to the three growth dimensions set out in Europe 2020. The seven pillars of the Digital Agenda include:

Figure 2 – Pillars of the Digital Agenda for Europe


Digital Agenda for Europe
Achieving digital single market
Interoperability and standards
Trust and security
Fast and ultrafast Internet access
Research and innovation
Enhancing digital literacy and skills
ICT-enabled benefits for EU society

The main objective of the Digital Agenda is to develop a digital single market in order to generate smart, sustainable and inclusive growth in Europe, which is also one of the key political priorities of the Commission. Security and resilience issues are addressed under the Trust and Security pillar of the Digital Agenda, which calls for measures aimed at a reinforced and high level NIS policy. This action presents measures aiming at a reinforced and high-level NIS policy, including measures allowing faster reactions in the event of cyber-attacks.

In light of the Digital Agenda, this report, with the focus on better cooperation in cyber security information sharing initiatives within the European energy sector, contributes to the overall improvement of the security and resilience as covered by the "Trust and Security" pillar of the DAE.

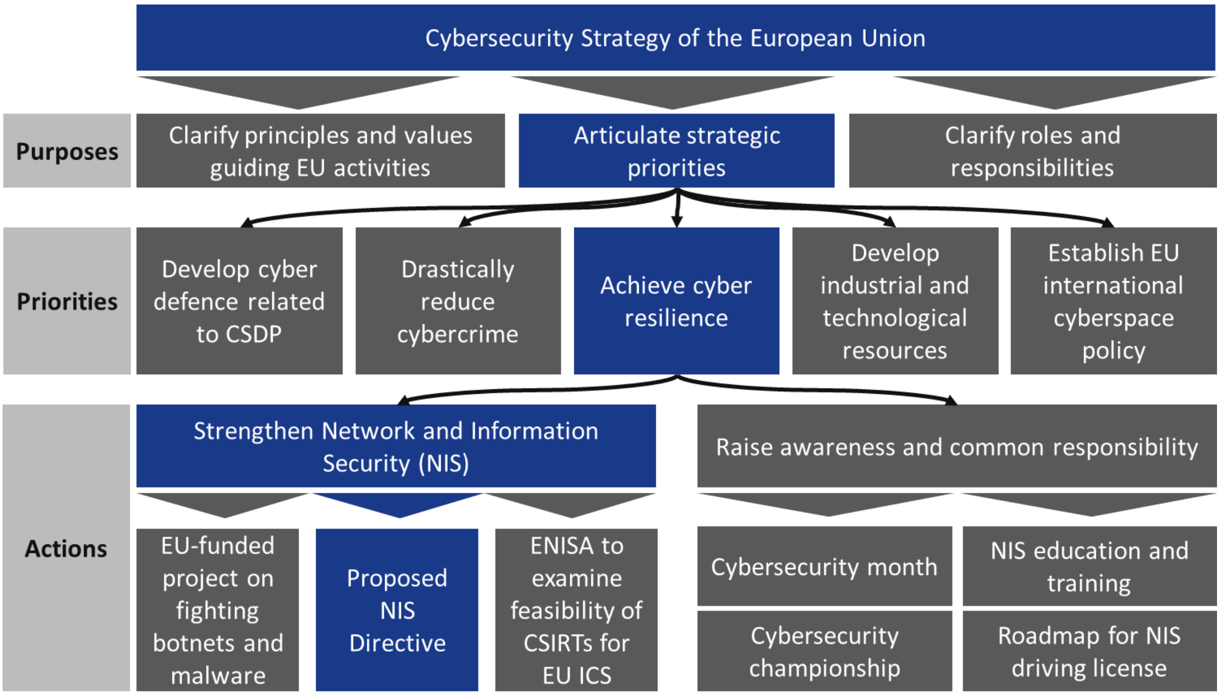
3.2.2 Cyber Security Strategy of the EU

The Cyber Security Strategy of the EU (European Commission, 2013) is the first comprehensive policy document in the area of NIS resulting in a coordination of policy across three areas:

- law enforcement and home affairs
- "Digital Agenda"
- defence, security, and foreign policy.

The objective of the strategy is to ensure a secure and trustworthy digital environment, while promoting and protecting fundamental rights and EU's core values. It proposes actions to enhance the EU's performance both in the short and long term, includes a variety of policy tools and involves different types of actors including the European Institutions, Member States and industry. It outlines the EU's vision in the domain of cyber security, clarifying roles and responsibilities, and specifying required actions to promote online security and citizens' rights. The vision presented in the Cyber Security Strategy is articulated in five priorities of which the first one is achieving cyber resilience. To boost cyber resilience, both public and private sector must develop capabilities and cooperate effectively.

Figure 3 – Overview of the Cyber Security Strategy Based on the Joint Communication on the Cyber Security Strategy of the European Union (European Commission, 2013)


Cybersecurity Strategy of the European Union
Purposes
Clarify principles and values guiding EU activities
Articulate strategic priorities
Clarify roles and responsibilities
Priorities
Develop cyber defence related to CSDP
Drastically reduce cybercrime
Achieve cyber resilience
Develop industrial and technological resources
Establish EU international cyberspace policy
Actions
Strengthen Network and Information Security (NIS)
Raise awareness and common responsibility
EU-funded project on fighting botnets and malware
Proposed NIS Directive
ENISA to examine feasibility of CSIRTs for EU ICS
Cybersecurity month
NIS education and training
Cybersecurity championship
Roadmap for NIS driving license

According to the Cyber Security Strategy, network and information security is of paramount importance to our society and the economy as they are becoming increasingly dependent on information systems.

Consequently, in July 2016, the European Parliament and the Council adopted the "Directive concerning measures for a high common level of security of network and information systems across the Union", the so-called "Network and Information Security Directive" or simply "NIS Directive" (European Parliament and Council, 2016), described below.

3.2.3 Network and Information Security (NIS) Directive

The NIS Directive lays down security obligations for operators of essential services[9] (in critical sectors such as energy, transport, health and finance), as well as for digital service providers such as online marketplaces, search engines and cloud services(European Parliament and Council, 2016). Each EU Member State is also required to designate one or more national authorities and to establish a strategy for dealing with cyber threats, and CSIRTs with NIS tasks.

Furthermore, the NIS Directive creates a cooperation group in order to facilitate strategic cyber security cooperation and information sharing among Member States and further develop trust amongst them. In parallel, it creates a CSIRTs network to build confidence between Member States and to boost operational cyber security cooperation.

The energy sector is emphasised as one of the key sectors identified in the NIS Directive. The Directive provides criteria to determine whether an incident would have a significant disruptive effect on the provision

[9] The NIS Directive (Art. 5) describes essential services as follows: a) an entity the provides a service which is essential for the maintenance of critical societal and/or economic activities; (b) the provision of that service depends on network and information systems; and (c) an incident would have significant disruptive effects on the provision of that service.

of an essential service. It is suggested that Member States should take into account a number of different factors, such as the number of users relying on that service, the dependency of other sectors listed in the Directive, the market share of that entity, the geographic spread with regard to the area that could be affected by an incident, and impact that incidents could have (see Article 6 - Significant disruptive effect). In terms of assessing the significance of the impact that an incident could have, the Directive identifies some parameters, in particular the number of users affected by the disruption of the essential service, the duration of the incident, the geographical spread with regard to the area affected by the incident (see Article 1 - Security requirements and incident notification) (European Parliament and Council, 2016).

The NIS Directive also highlights a number of sector–specific factors, which should be considered in order to determine whether an incident would have a significant disruptive effect on the provision of an essential service. With regard to energy suppliers, such factors could include the volume or proportion of national power generated; for oil suppliers, the volume per day (European Parliament and Council, 2016).

In the Impact Assessment (European Commission 2013b) accompanying the proposal for this Directive (European Commission, 2013a) it is stated: “Generation, transmission and distribution of energy are highly dependent on secure network and information systems. Ensure the resilience of utilities is particularly important since virtually all other sectors and the wellbeing of our society depend upon them” (European Commission 2013b).

3.2.4 EU Data Protection Legislation

Data protection in Europe is still governed by the Data Protection Directive (European Parliament and Council, 1995), which will be replaced by the General Data Protection Regulation (hereunder, the “GDPR”) (European Parliament and Council, 2016a), and by a specific Directive that will apply to the processing of personal data in criminal matters[10]. The GDPR entered into force on 24 May 2016 and it shall apply from 25 May 2018. During this time the European Commission “work[s] together with the Member States and the data protection authorities - the future European Data Protection Board - to ensure a uniform application of the new rules” (European Commission, 2016a).

With the entering into force of the GDPR, the data protection legal framework will change dramatically, in part due to the fact that it will be directly applicable in all Member States, thereby replacing the national laws which are currently implementing the Data Protection Directive. The GDPR will also apply to the processing of personal data not covered by sectoral legislation such as the Directive on personal data in criminal matters. The GDPR will strengthen data protection and enhance the harmonisation of legislation across the EU.

With reference to CSIRTs, Recital 49 of the GDPR states that “The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security […] and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems”.

[10] The Directive on processing of personal data in criminal matters entered into force on 5 May 2016 and EU Member States have to transpose it into their national law by 6 May 2018.

The sharing and exchange of information between CSIRTs and various information sharing initiatives can be indeed considered as processing of personal data if some conditions are met. The Data Protection Directive (Article 2(a)) states that personal data is information relating to an identified or identifiable natural person. Therefore, the exchange of personal data between entities is deemed to be a processing activity.

Similarly, the GDPR (Article 4), defines the “data subject’’ as an identifiable person “who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person”.

In line with general data protection principles, when a CSIRT or a participant in a ISAC or in an information sharing initiative shares personal data, such as an email address or other personal information of an alleged cyber attacker, a victim of the threat or any other person, with a CSIRT or a participant in a ISAC or in an information sharing initiative in another country, both bodies are considered to be processing personal data. It is also considered that processing of personal data is taking place when it is possible to link the information exchanged to an identifiable person. This is the case when the shared information is related to, for instance, IP addresses and user activity.

Data security plays a prominent role in the GDPR and, compared to the Data Protection Directive, it imposes stricter obligations on data processors and controllers with regard to data security. It also offers more guidance on appropriate security standards and specific breach notification guidelines.

The GDPR stipulates, Article 32, that controllers and processors are required to “implement appropriate technical and organisational measures” taking into account “the state of the art and the costs of implementation” and “the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.” In addition, the GDPR provides specific suggestions concerning the kinds of security actions that might be considered “appropriate to the risk,” including:

- The pseudonymisation and encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Moreover, the GDPR defines “personal data breach” as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.” In the event of a personal data breach, notice must be provided to the supervisory authority “without undue delay and, where feasible, not later than 72 hours after having become aware of it.” Failure to notify the supervisory authority within 72 hours will require a “reasoned justification” for the delay.

3.2.5 Coordinated Vulnerability Disclosure Manifesto

During the 2016 High Level Meeting on Cyber Security, organised by the Ministry of Security and Justice during the Netherlands’ Presidency of the EU, the Coordinated Vulnerability Disclosure Manifesto, initiated by CIO Platform Nederland and Rabobank (CIO Platform Nederland and Rabobank, 2016), was signed by nearly 30 organisations. Since organisations from the energy sector are also part of it, considering its scope, this manifesto is mentioned in this report.

By signing the manifesto, the participating organisations acknowledge the importance of efforts of the research and white-hat communities to make the internet and society safer. The signatories declare to support the principle of having a point of contact to report IT vulnerabilities and already have this set up in their own organisations, or they plan to do so soon (ENISA, 2016a).

In short, the Manifesto enforces the signing parties to follow the same process when facing vulnerabilities and incidents. They agree to do their utmost to create a safer cyber security space, to take measures for their vulnerabilities, to follow the good practices proposed by the community, e.g. the Good practice guide on vulnerability disclosure published by ENISA (ENISA, 2016b) and to participate to the effort of improving the practices. Besides, they commit to take into consideration the work performed by the academic sector, to provide information to the community in a transparent way and to promote the good practices outside the community.

Although the Manifesto does not constitute a piece of legislation, this initiative is nevertheless an important step in the policy space for information sharing in the energy sector.

3.3 Energy Regulators

Energy regulators have the task to enforce the application of the network and information security policies and strategies by all energy market players. As such, they guarantee the security, safety, transparency and competitiveness in the energy sector. National regulatory authorities (NRAs), the Agency for the Cooperation of Energy Regulators (ACER) and the Council of European Energy Regulators (CEER) play key roles in the EU energy regulatory landscape.

The NRAs are entrusted and consulted by their national government and public authorities on the organisation and operations of the energy sector. They receive the mission of supervision and enforcement of the applicable laws and regulations that regulate the Member State's energy markets. NRAs ensure that all energy market players active in their country comply with the rules defined in the national energy policies and regulatory framework.

ACER is the Agency for the Cooperation of Energy Regulators, a European Union Agency, established by Regulation (EC) No 713/2009 (European Parliament and Council, 2009). Its mission is to complement and coordinate the work of EU NRAs and to work towards the completion of a single EU energy market for electricity and gas. In 2011, ACER received additional tasks under Regulation (EU) No 1227/2011 on wholesale energy market integrity and transparency (REMIT) (European Parliament and the Council, 2011) and in 2013 under Regulation (EU) No 347/2013 on guidelines for trans-European energy infrastructure (European Parliament and the Council, 2013).[11]

CEER is a not-for-profit association, which enables the cooperation and exchange of good practices among NRAs of electricity and gas at EU and international level. The facilitation of the creation of a single, competitive, efficient and sustainable internal energy market is part of CEER's objectives.

While ACER plays a key role in providing a framework at EU level for NRAs to cooperate, CEER complements ACER's work by providing a platform to EU NRAs to develop common pan-European interests on specific topics and issues (e.g. smart grids and sustainability). CEER does not overlap the work performed by ACER.

Concerning the regulation of the oil sector, EU national governments control their respective territories. They determine the areas in which companies can search for and produce oil resources. To ensure fair

[11] For more information on ACER mission and objectives see: ACER, n.d.

competition, a set of common EU rules exist and are applied by national governments when granting licenses for hydrocarbon prospection, exploration and production (European Parliament and Council, 1994).

The peaceful use of nuclear energy within the EU is governed by the 1957 Euratom Treaty, which established the European Atomic Energy Community (Euratom). While Euratom is a separate legal entity from the EU, it is governed by the EU's institutions. In the EU, the safety of nuclear energy production is the primary responsibility of power plant operators supervised by independent national NRAs.

The Nuclear Safety Directive (Council of the European Union, 2014) requires EU countries to give the highest priority to nuclear safety at all stages of the lifecycle of the nuclear energy facility, from the design phase to the decommission of the facility, and ensuring significant safety enhancements for old reactors.

In 1999, the Western European Nuclear Regulators Association (WENRA) was established to become a network of chief nuclear safety regulators in EU and Switzerland exchanging experiences and discussing significant safety issues (WENRA, n.d.).

In addition to European and national nuclear safety standards, EU nuclear regulatory framework also includes good practices and recommendations from the International Atomic Energy Agency (IAEA) and the United States Nuclear Regulatory Commission (US-NRC).

In terms of their mission of warranting security and safety in the energy sector, national governments and related regulators are putting more effort into integrating cyber security standards in their regulatory framework. Computer systems and industrial control systems used in the energy facilities are often used for safeguards, security and safety, requiring an increased attention from the authorities, the facility operators and the supply chain to strengthen the resilience of these systems against cyber threats. As a result, energy regulators are involved in some initiatives to share information on cyber security at national, European and international level, e.g. with other public authorities and energy operators.

4. An Overview of the Energy Sector and Its Subsectors

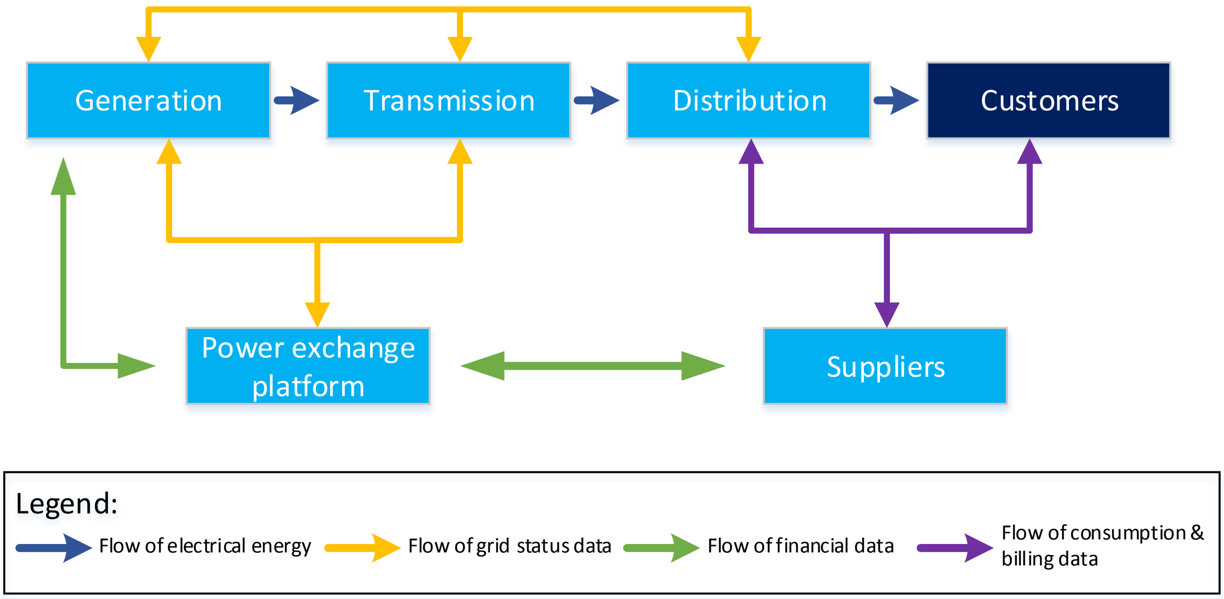
The purpose of this report is to identify the development of information sharing initiatives and to provide a high-level overview of these initiatives in all main segments of the energy sector. Therefore, this chapter sets the stage for understanding cyber security information sharing within the energy sector by introducing the selected energy subsectors and by providing the reader with a general overview of the energy subsectors and their segments of activities. The objective is to provide a background of the inherently complex energy sector by providing the reader with the keys to understanding the main issues and challenges of sharing cyber security information in the sector, addressed in this report.

The NIS Directive, mentioned above, identifies the following subsectors in the energy sector: electricity, oil and gas. This report also considers the nuclear and alternative fuels as relevant energy subsectors. The sections below provide a short description of these subsectors.

4.1 Electricity

The electricity subsector is mainly made of the following segments: generation, transmission and distribution, energy supply and power exchange platforms. The organisation of the electricity subsector requires that all segments interact together through a complex flow of electrical energy, grid status data, financial data and consumption and billing data as summarised in Figure 4. For simplicity, Figure 4 does not depict the flow of raw energy sources (e.g. fossil fuels) used by the generation segment to produce electricity.

Figure 4 – Segments and Actors of the Electricity Subsector



- **Generation** of electricity is realised at large **electric power stations** that are connected to an electrical transmission network and transform hydraulic, fossil, nuclear and renewable energy into electrical power. Electricity can also be generated in a decentralised way and via renewable energy sources (i.e. wind-generation, photovoltaics, etc.).

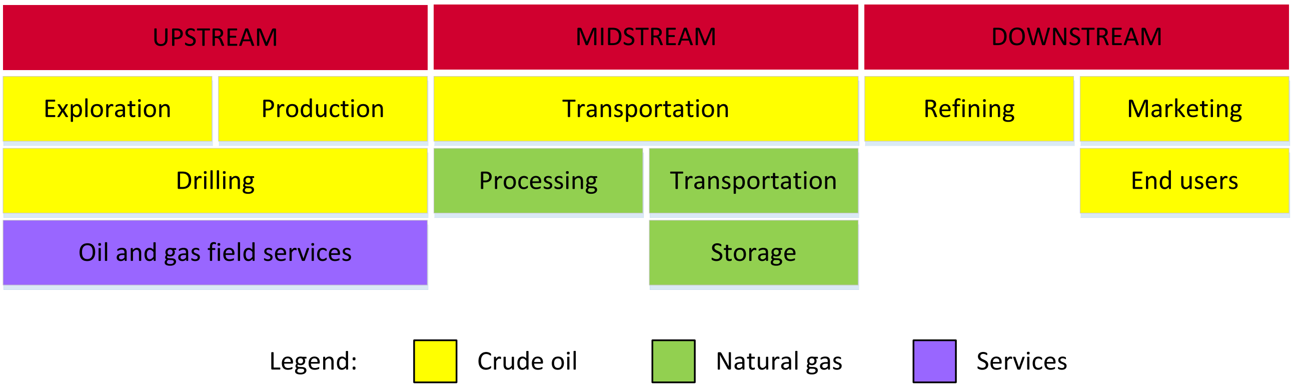
- **Transmission** and **distribution** of electricity is managed by Transmission System Operators (TSOs)[12] and Distribution System Operators (DSOs), who are responsible for the reliable and efficient operations of very high to low voltage transmission and distribution systems. As such, TSOs are responsible for maintaining the frequency of the European transmission network by ensuring that production of electricity meets consumption demand at all time and DSOs distribute electricity to customers, including residential and small and middle enterprises (SMEs).
- **Energy suppliers** are responsible for the supply of electricity to end customers. Energy suppliers buy electricity on the wholesale market and sell to the end customers.
- **Power exchange platforms** were set up when the electricity market was liberalised (European Parliament and Council, 2003) to enable market players to anonymously negotiate same-day or next-day purchases and sales of electricity. Their objectives are to provide an open market, to organise competition and to establish a transparent reference price for market participants.

Generation, transport and distribution of electricity extensively implements PCN (Process Control Networks) and SCADA (Supervisory Control and Data Acquisition) networks. SCADA networks are being integrated with traditional corporate IT systems to increase data visibility across operational and corporate IT assets. The energy supply and power exchange platforms process strategic financial data and sensitive customer data in large corporate IT systems and datacentres. As a result, all segments of the electricity subsector should be considered as potential prime target for exploitation by cyber criminals and therefore be accordingly protected.

4.2 Oil and Gas

The oil and gas subsector is a global industry, dominated by private integrated oil companies and government-owned national oil companies. The subsector is composed of the following segments: upstream, oil and gas field services, midstream and downstream. In Europe, major oil and gas companies have integrated operations in these segments, with a continuously increasing level of automation and digitisation that make these a target for cyber-attacks. The energy resources include crude oil, natural gas, natural gas liquids and unconventional resources like oil sands, shale gas, tight gas and oil shales.

Figure 5 – Crude Oil and Natural Gas Value Chain



[12] Forty-two electricity transmission system operators (TSOs) from 35 countries across Europe are members of the European Network of Transmission System Operators for Electricity (ENTSO-E). ENTSO-E "represents. ENTSO-E was established and given legal mandates by the EU's Third Legislative Package for the Internal Energy Market in 2009" (ENTSO-E, n.d.). A list of ENTSO-E members is available at https://www.entsoe.eu/about-entso-e/inside-entso-e/member-companies/Pages/default.aspx

- **Upstream** focuses on acquisition, exploitation and development of properties for production of crude oil and natural gas from underground reservoirs, including drilling.
- **Oil and gas field services** (or oilfield services) serve the upstream segment by supplying manufactured equipment, technology and services related to evaluation of hydrocarbon formations, drilling and completion, and production of oil and natural gas.
- **Midstream** is active in gathering, storage and transmission[13] or transportation of natural gas and crude oil. Companies active in this segment are also active in transportation, fractionation and storage of natural gas liquids (NGLs).
- **Downstream** is the refining and marketing segment of the oil and gas subsector. It is active in refining crude oil into various hydrocarbon products (e.g. gasoline, jet fuel, fuel oils and diesel, etc.) and market and trade of oil and gas products through wholesale and retail channels.

Operations of oil and gas companies depend on PCN, SCADA systems, large corporate IT systems and satellite communications that have a unique set of cyber security issues to face. Furthermore, the risks related to cyber security threats on computer systems used by ports and merchant marine for the transportation of oil and natural gas products should be taken into consideration. Oil and gas companies are prime targets for exploitation by potential cyber criminals because of their high-value intellectual property information and the strategic nature of their physical assets.

4.3 Nuclear

Nuclear is a global and highly regulated subsector. The activities include the production of electricity, the operation of nuclear research reactors, the production and usage of radioisotopes for medical and non-medical purposes, the transport of radioactive material and the processing and storage of nuclear waste. Furthermore, service companies provide engineering services, manufactured equipment, technology and services related to the operations and maintenance of nuclear facilities. At each moment, stakeholders involved in nuclear activities must comply with the safety criteria defined in the nuclear regulatory framework of the EU Member State.

According to ENTSO-E, the net generating capacity of nuclear power plants in Europe equals 12% (ENTSO-E, 2015) of the total capacity and is quite stable in comparison with previous years, representing a total power of 120GW. ENTSO-E forecasts that this capacity will be maintained until 2020 (ENTSO-E, 2015a). “There are 130 nuclear reactors in operation in 14” (European Commission, n.d.) of the 28 EU Member States. Nine Member States generate more than 30% of their electricity from nuclear reactors, making nuclear power an important source of energy (World Nuclear Association, 2016).

Over the years nuclear power plant facilities have developed robust safety mechanisms and make use of ICS within safeguards, security and safety systems. There has been an increase in the use of information technology to monitor and control these industrial control systems, increasing the need to address cyber security threats.

Nuclear energy used for other purposes than electricity production have not been taken into consideration for this report.

[13] Forty-five TSO for gas are members of the European Network of Transmission System Operators for Gas (ENTSOG). ENTSOG mission is to “facilitate and enhance cooperation between national gas transmission system operators (TSOs) across Europe in order to ensure the development of a pan-European transmission system in line with European Union energy goals” (ENTSOG, n.d.). A list of ENTSOG -E members is available at http://www.entsog.eu/members

4.4 Alternative Fuels

The alternative fuels subsector produces fuels other than the conventional ones provided by the oil and gas subsector. It operates facilities that manufacture biodiesel, methanol, ethanol, butanol, hydrogen, fuel cells and biomass. The alternative fuels facilities make use of corporate IT, PCN and SCADA systems to manage and monitor the production processes and the safety and security systems, increasing the risk of exposing the industrial processes to cyber security threats.

5. ISACs, CSIRTs and Cyber Security Information Sharing Initiatives in the Energy Sector

The implementation and use of new technology (e.g. smart grids) and increased connectivity to the internet bring very real and new risks to the energy industry. Cyber security measures need to be taken in parallel to the implementation of new technology, starting from the design phase. It is no longer just a question of protecting governmental or corporate IT systems. Cyber threats are now directed at the national and European levels, resulting in an urgent need for a collaborative approach at this level.

The energy sector needs to increase the current maturity level with regards to management of cyber security. Several stakeholders interviewed made a comparison with the financial sector, which has developed a relatively high level of maturity of cyber security, which is an example for management of cyber risks and sharing of cyber security incidents. This low maturity of the energy sector is explained by historical reasons, where physical security and safety threats have always been considered above all other threats by the sector. As the energy sector is experiencing a digital transformation, with the processing of digital data to monitor and process the critical infrastructure, safety and security, the sector needs to target high maturity levels on cyber threat management. Cyber security should be seen as one important components of the "multifaceted challenge" (IEA, 2016) of energy security[14].

At the EU level, cyber security is increasingly a key priority because communication and information have become a key factor in economic and societal development – therefore cyber security is a challenge shared by all EU Member States. An efficient cooperation and information exchange mechanism between the key stakeholders (e.g. the national and governmental CSIRTs) that enables them to address risks, vulnerabilities and threats is crucial for providing high levels of cyber security in Europe. As showed in the context of the cyber-attacks against power plants in Ukraine (ICS-CERT, 2016), information sharing is critical in overcoming cyber-attacks (E-ISAC and SANS, 2016), and effective detection and prevention of cyber-attacks relies on information exchange via trusted initiatives. Similarly, tackling energy security in a fast-changing environment where actors (e.g. aggregators of data, distribution system operators) and evolving trends (e.g. use of data in smart grids, smart meters) will require flexibility and capacity to adapt and change.

The importance of cyber security is increasing in the energy sector and this, in turn, relies on established and trusted information sharing initiatives. Below ISACs, CSIRTs and cyber security information sharing initiatives in the energy sector are presented.

5.1 Information Sharing and Analysis Centres (ISACs)

Information Sharing and Analysis Centres (ISACs) are trusted entities established by infrastructure owners and operators, in some cases facilitated and supported by governments, to foster information sharing on good practice regarding physical and cyber threats, including the mitigation of these threats. Typically, non-profit organisations and ISACs can reach deep into their sectors, communicating quickly information far and wide, and maintaining sector-wide situational awareness (National Council of ISACs, n.d.). In practical terms, ISACs help the infrastructure owners and operators protect their facilities, personnel and customers from

[14] IEA, 2016 refers to electricity security, but the considerations made are widely applicable more to energy security in general. It is interesting to note that the International Energy Agency (IEA), composed of 29 member countries, has as "one of the first roadmaps planned to be developed under the new Technology Roadmap cycle […] the [updated] smart energy system roadmap". One of the major components of the related analysis is cyber security (see IEA, 2016a and IEA n.d.). More information on the IEA are available at https://www.iea.org, last access: 31 October 2016.

cyber and physical security threats and other hazards. They do so by collecting, analysing and disseminating actionable information to their members and by providing members with tools to mitigate risks and enhance resiliency (National Council of ISACs, n.d.).

ISACs have been successful in providing operational services – such as risk mitigation, incident response, and information sharing, which protect critical infrastructures. Additional ISAC services include annual meetings, technical exchanges, workshops and webinars (National Council of ISACs, n.d.).

The strength of the ISACs lies with their ability to:

- Leverage the expertise and experience of existing private/public sector critical infrastructure protection organisations to improve the resilience;
- Maximise the operational foundations of the ISACs that share information between the government and private sector critical infrastructures, as well as share information among sectors;
- Support the needs of all critical infrastructures to provide trusted and secure actionable information sharing and sector specific analytical capabilities while respecting the individuality of each sector (National Council of ISACs, n.d.).

To illustrate how ISACs can be set up and be operational, we present below a few examples of energy sector ISACs.

At national level in Europe:

- The **National Cyber Security Centre (NCSC) Energy ISAC**[15] is a Dutch public-private partnership, which enables participants to exchange information and experiences about cyber security in the energy sector. This ISAC also enables participants to build up trust among each other and informally exchange knowledge and experience on cyber security issues.
- The **National Cyber Security Centre (NCSC) Nuclear ISAC**[16] is a Dutch public-private partnership that enables participants to exchange information and experiences about cyber security in the nuclear subsector. This ISAC also enables participants to build up trust among each other and informally exchange knowledge and experience on cyber security issues.
- The **Cyber Security Information Sharing Partnership (CiSP)**[17] is a UK's joint industry government initiative that enables its members from across sectors and organisations to exchange cyber threat information in real time, while protecting the confidentiality of the shared information.

At European level:

- The **European Energy – Information Sharing Analysis Centre (EE-ISAC)**[18] is a main outcome of the Distributed Energy Security Knowledge (DENSEK) project[19]. EE-ISAC was established in 2015. Its

[15] https://www.ncsc.nl/english/Cooperation/isacs.html, last access: 3 August 2016.
[16] https://www.ncsc.nl/english/Cooperation/isacs.html, last access: 3 August 2016.
[17] https://www.cert.gov.uk/cisp, last access: 3 August 2016.
[18] http://www.ee-isac.eu, last access: 3 August 2016.
[19] The Distributed Energy Security Knowledge (DENSEK) was a project of the European Commission, DG Home Affairs, which ran from July 2013 to July 2015. The project deliverables were the establishment of a European Information Sharing and Analysis Centre (ISAC) for the energy sector, a situation awareness network to allow Member States to proactively take mitigating actions when a threat occurs in Europe and an information sharing platform to facilitate distribution of information within the energy sector. For more information: http://www.densek.eu, last access: 5 October 2016.

creation responds to the need for European collaboration in protecting the energy sector from cyber-attacks. EE-ISAC is a network of trust in which private and public parties share security information via member meetings, via an information sharing platform or via situational awareness networks.

At national level outside Europe:

- The **Oil and Natural Gas Information Sharing Analysis Center (ONG-ISAC)**[20] provides a secure and trusted environment for sharing cyber security information across the oil and natural gas industry in the USA. It provides relevant cyber security information to integrated oil, natural gas, upstream, mid-stream and down-stream companies, field services, including industry associations and energy service and supply companies.
- The **Downstream Natural Gas Information Sharing Analysis Center (DNG-ISAC)**[21] serves natural gas utility distribution companies in the USA, by facilitating communications on threat information and indicators between participants, the US federal government and other critical infrastructures.

At international level outside Europe:

- The **Electricity Information Sharing and Analysis Center (E-ISAC)**[22] provides security services to electricity service owners and operators in the USA, Canada and portions of Mexico. It acts as the trusted source of information sharing for the electricity subsector on cyber threats, vulnerabilities and incidents.

It is important to note that ISACs, including those not specifically focused on the energy sector, might have some activities (e.g. awareness raising campaigns and training) also relevant for the energy sector (an example mentioned by one of the interviewees is the NCSC-FI, the Finnish National Cyber Security Centre).

5.2 Computer Security and Incident Response Teams (CSIRTs)

A CSIRT is a team mainly consisting of IT security experts whose core business is to respond to computer security incidents. It provides the necessary services to handle cyber security incidents and support their constituents in recovering from cyber security breaches. Most CSIRTs also provide preventative and educational services to raise awareness of their constituents.

Acting as subject matter experts, CSIRTs issue advice on vulnerabilities in the software and hardware in use, and inform the users about exploits and malware that take advantage of these flaws. This allows the CSIRT constituents to quickly react and take action to e.g. patch and update their systems. Over the years, the CSIRTs have extended their capabilities from reaction force to a complete security service provider covering various areas of services such as alerts and warnings; incident handling; incident analysis; incident response support, and incident response coordination.

An important part of a CSIRT mission - although not the core one - is to share the lessons learned, to contribute to the knowledge of others and to enable constituents to get appreciation of what the CSIRT is doing for them. CSIRTs are also important actors to take into consideration for information sharing initiatives in the energy sector and beyond. For peers and technical audience, expert papers are shared or expert sessions are organised. An efficient co-operation between CSIRTs is essential for mitigating even fairly limited incidents, and especially when the scope of an issue is larger.

[20] http://ongisac.org, last access: 3 August 2016.
[21] https://www.dngisac.com, last access: 3 August 2016.
[22] https://www.esisac.com, last access: 3 August 2016.

It is very valuable to invest in relationships surrounding the CSIRT environment of operations, such as:

- Law enforcement
- Professional organisations involved with security issues
- Professional organisations outside the security community
- Other security service providers
- Regional, local and domestic cooperation between CSIRTs.

There are also national and governmental CSIRTs that serve the government of a country by helping to protect the critical information infrastructure. National and governmental CSIRTs play a key role in coordinating incident management with the relevant stakeholders at the national level. They also bear the responsibility for cooperation with the national and governmental teams in other countries.

This report has identified specific CSIRTs for energy in the private sector and trends to establish similar incident response teams by national governments. It is important to mention that this list is based on the available online documentation and on information provided by the stakeholders who agreed to contribute to this report and is therefore non-exhaustive:

- **KraftCERT** (Norwegian energy sector CERT)[23] provides support for the entire power industry in preventing and handling security incidents. The CERT is specialised in monitoring, counselling and incident response and facilitates exchange of security incidents information between its members.
- **Statoil CSIRT**[24], in Norway, provides cyber security incident response capabilities to Statoil (oil and gas) and to its joint ventures. The Statoil CSIRT is currently involved in information sharing initiatives with other government and private entities in Norway and the UK on specific cyber threats affecting the oil and gas subsector.
- **EDP Distribuição CSIRT**[25], in Portugal, provides cyber security incident response capabilities to the electrical distribution company EDP Distribuição. This CSIRT is involved in information sharing initiatives with the EE-ISAC at the EU level.
- National Grid Cyber Response Team (**NGRID-CSIRT**)[26] in the UK, provides cyber security incident response capabilities to the electrical transport and distribution company National Grid.

In addition, Austria is in the process of implementing a CSIRT for the energy sector that will be responsible for the reception and sharing of information on cyber security incidents and vulnerabilities in the energy sector. The CSIRT will support Austrian energy companies in their response to cyber security incidents and will collaborate with public organisations such as the NRAs, critical infrastructure providers and public authorities.

It is important to note that CSIRTs, including those not specifically focused on the energy sector, might have some activities (e.g. awareness raising campaigns and training) also relevant for the energy sector (an example mentioned by one of the interviewees is the Slovenian CSIRT).

5.3 Cyber Security Information Sharing Initiatives

Actors in the energy sector have developed information sharing initiatives to enable all market players, whether public or private, to have access to relevant cyber security information. Some initiatives cover all energy subsectors and other are specific to a certain subsector. The sections below provide an overview of

[23] https://www.kraftcert.no/english/om.html#, last access: 3 August 2016.
[24] http://www.statoil.com/en/EnvironmentSociety/security/Pages/CSIRT.aspx, last access: 3 August 2016.
[25] http://www.edp.pt/PT/Pages/SegurancaInformatica.aspx, last access: 3 August 2016.
[26] http://www2.nationalgrid.com, last access: 3 August 2016.

the key initiatives identified during data collection of this report. They should be considered as a representative, but not as an exhaustive list of initiatives.

5.3.1 Cyber Security Information Sharing Initiatives Covering All Energy Subsectors

- The European Commission set up an **Energy Expert Cyber Security Platform (EECSP)** composed of an expert group and a forum (European Commission, 2015a). The expert group is an informal and temporary Commission expert group on cyber security. The forum is an annual conference, on top of the expert group, with open participation. The mission of the expert group is to provide guidance to the European Commission on policy and regulatory directions at European level by addressing the energy sector key points including infrastructural issues, security of supply, smart grid technologies as well as nuclear.
- The **Thematic Network on Critical Energy Infrastructure Protection (TNCEIP[27])** is an initiative of the DG Energy of the European Commission, and is composed of European owners and operators of energy infrastructure in the electricity, the gas and the oil sectors. It allows energy sector operators to exchange information on, as other, threat assessment, risk management and cyber security.
- The **Incident and Threat Information Sharing EU Centre (ITIS-EUC)[28]** aims to improve the situational awareness of critical energy infrastructures by providing information on incidents and emerging threats and fostering information sharing among the relevant energy stakeholders. ITIS is an initiative of DG Energy and "its operation (portal maintenance, content, user support) is entrusted to DG JRC [Joint Research Centre] of the European Commission" (European Commission, n.d.(a)).
- The **Dutch National Cyber Security Centre (NCSC)[29]** launched an information sharing initiative to support the energy sector in the identification of relevant cyber threats, vulnerabilities and cyber security good practice.
- In 2013, France passed a law (military programming law) that, among others, gives **ANSSI** (Agence Nationale de la Sécurité des Systèmes d'Information, the National Cybersecurity Agency of France)[30] the ability to set minimum cyber security requirements at the technical and organisational levels for operators of critical infrastructures. In order to define rules that are efficient, compatible with the specific context of each sector, and economically viable, ANSSI created and steers **sectorial working groups.** Each of these groups gathers, for a given sector, the critical infrastructures operators, the coordinating ministries and the sectoral authorities.
- The **European Network for Cyber Security (ENCS)[31]** is a non-profit member organisation founded in 2012, which brings together critical infrastructure stakeholders and security experts to deploy secure European critical energy grids and infrastructure. The ENCS provides cyber security solutions and counsel to grid operators and regulators. The ENCS research based services include member collaboration projects, security testing, training, information and knowledge sharing. The information and knowledge sharing service comprise of assembly meetings, security roundtables, member and partner events, webinars and a portal with content and good practices created by ENCS experts and associated members and partners.
- The **European SCADA and Control Systems Information Exchange (EUROSCSIE)[32]** was set up in 2005 by the UK Centre for the Protection of the National Infrastructures (CPNI). The initiative was created

[27] https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure, last access: 17 October 2016.

[28] https://itis.jrc.ec.europa.eu, last access: 3 August 2016.

[29] https://www.ncsc.nl/english/Cooperation/isacs.html, last access: 5 October 2016.

[30] http://www.ssi.gouv.fr, last access: 3 August 2016.

[31] https://www.encs.eu, last access: 5 October 2016.

[32] https://espace.cern.ch/EuroSCSIE/default.aspx, last access: 3 August 2016.

to address the increasing number of cyber threats and the potential effects of cyber-attacks against industrial control systems. The initiative is composed of members of the EU governments, research institutions, operators and industries that depend or are responsible for the security of critical infrastructure' industrial control systems. ENISA runs the secretariat for this expert group now.

- The Organization of American States (**OAS**)[33] set up the **Cyber Security Program** in the early 2000s in order to strengthen cyber security capacities in OAS member state by performing in-depth analysis and understanding of the extent of cyber threats and by evaluating existing national capabilities to deal with such threats. The programme is managed by the Secretariat of the Inter-American Committee Against Terrorism (CICTE). In 2004, the OAS adopted a comprehensive cyber security strategy (OAS, n.d.) and subsequently adopted the declaration on strengthening cyber security in the Americas (OAS, 2012) and the declaration on protection of critical infrastructure from emerging threats (OAS, 2015). The OAS Cyber Security Program addresses seven challenges: national cyber security strategy development, cyber security training, CSIRT development and hemispheric network, crisis management exercises, awareness raising, cyber security technical assistance missions and access to cyber security expertise (OAS, n.d(a)).

5.3.2 Cyber Security Information Sharing Initiatives Specific to the Electricity Subsector

We identified the following key information sharing initiatives that are specific to the electricity subsector:

- The **Energy Emergencies Executive Committee for Cyber (E3CC)** is an information sharing roundtable of senior information security professionals across UK electricity generation, transmission and distribution operators. Government participation is through DECC, CPNI and Ofgem, respectively Department of Energy & Climate Change, Centre for the Protection of National Infrastructure and the Office of gas and electricity markets. Through individual membership of CiSP (Cyber Security Information Sharing Partnership) and other communications, the group shares information on security incidents that are of help to all stakeholders in the electricity subsector.
- The European Agency for the Cooperation of Energy Regulators (ACER)[34] set up the **ARIS**, the **ACER REMIT (Wholesale Energy Market Integrity and Transparency) Information System**[35] **portal**. The portal is a single entry point to a compilation of information and applications that ACER made available to electricity and gas market participants and other stakeholders in order to implement the Regulations EU No 1227/2011 (European Parliament and Council, 2011) and Commission Implementing Regulation No 1348/2014 (European Commission, 2014a) on wholesale energy market integrity and transparency and REMIT implementation. Due to the sensitivity of information and to the legal constraints concerning operational reliability of the system, under the REMIT umbrella, the different representatives of the National Regulatory Authorities (NRAs) for Energy represented into ACER share information and good practices on information and cyber security matters, including cyber security incidents. In addition, under the same activity, the NRAs coordinate themselves, together with ACER, in order to properly address emerging cyber security threats that may have an impact on the operations.

5.3.3 Cyber Security Information Sharing Initiatives Specific to the Oil Subsector

No initiatives specific to the oil subsector were identified.

[33] http://www.oas.org/en/topics/cyber_security.asp, last access: 3 August 2016.
[34] http://www.acer.europa.eu/fr/Pages/default.aspx, last access: 3 August 2016.
[35] https://www.acer-remit.eu/portal/home, last access: 5 October 2016.

5.3.4 Cyber Security Information Sharing Initiatives Specific to the Gas Subsector

Apart from the ACER REMIT portal described in the electricity subsection, no initiatives specific to the gas subsector were identified.

5.3.5 Cyber Security Information Sharing Initiatives Specific to the Nuclear Subsector

The following information sharing initiatives were identified:

- In 2016, the members[36] of the **Nuclear Security Summit** agreed on a joint statement on cyber security (NSS, 2016). The members agreed to participate in two international workshops on the cyber security of industrial control systems used in the nuclear facilities. The initiative will enable states and their nuclear sectors to identify threats, vulnerabilities, and incidents and share good practices in managing risks to industrial control systems and evaluate the impact of using information technologies in the safety and security systems of nuclear facilities.
- The International Atomic Energy Agency (**IAEA**) has set up a **Computer Security Programme** (IAEA, n.d.) to provide states with the necessary guidance and external expertise to support the detection of, and response to, criminal or intentional cyber-attacks involving/impacting or directed at nuclear facilities[37].
- The **Civil Nuclear Sector SCADA Information Exchange (CNSSIE**) was set up by the UK Centre for the Protection of the National Infrastructures (CPNI). It was created in order to address the increasing number of cyber threats and the potential effects of cyber-attacks against industrial control systems used in the civil nuclear facilities.

5.3.6 Cyber Security Information Sharing Initiatives Specific to the Alternative Fuels Subsector

No initiatives specific to the alternative fuels subsector were identified.

[36] Argentina, Armenia, Australia, Belgium, Canada, Chile, China, Denmark, Finland, France, Georgia, Germany, Hungary, Japan, Jordan, Kazakhstan, Republic of Korea, the Netherlands, Norway, the Philippines, Poland, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Arab Emirates, the United Kingdom, the United States of America and the United Nations.

[37] On the topic of computer security at nuclear facilities, see: IAEA, 2011.

6. Challenges for and Good Practices in the Information Sharing Initiatives in the Energy Sector

This chapter examines shortcomings and problems, and identifies good practice, in energy sector information sharing.

6.1 Identified Shortcomings and Problems

The main shortcomings and problems that hinder information sharing on cyber incidents in the energy sector are identified and described below. It must be noted that they might be inter-related or even inter-dependant. However, as the scope of the report is primary to identify these shortcomings and propose recommendations to address them, we did not analyse the inter-dependencies between the shortcomings.

6.1.1 Lack of Trust

"Trust is an essential ingredient for the success of sharing initiatives" (ENISA, 2011c). From the interviews we understand that this element can be either a driver - when it is present - or an obstacle - when it is lacking - regarding information sharing on cyber security between energy sector actors.

Indeed, it seems that the **lack of trust** (at times even high levels of mistrust) is a key problem among the members of information sharing initiatives. It takes time and it is difficult to build trust for multiple reasons and we observe that the challenges mentioned by the interviewees are related to the following aspects:

Table 2 –Possible Explanations of Elements Having a Negative Impact on Trust

ELEMENTS IMPACTING TRUST	POSSIBLE EXPLANATION
Lack of interaction between members of the information sharing initiative	If certain participants do not share information within the initiative, there will be a perception that they are only receivers/users of the shared information and they are not active contributors. This may undermine the general trust and the basic principles and purpose of the information sharing initiative.
Conditions to become a member of certain initiatives are not specific enough, not well defined, either too restrictive or too generic	Criteria and conditions to join an initiative need to be always precise and well balanced – considering the purpose and specificities of the initiative.
Sensitivity of cyber threats and issues in the energy sector	The energy sector is closely linked to national security interests and critical infrastructures of a Member State. Therefore, sharing information is more difficult to achieve.
Large size of the sharing initiative (multiple participants)	An information sharing initiative composed by many members is more difficult to manage. The size is not always an advantage in such cases, especially in instances when participating stakeholders are looking forward to interact closer, to establish trust and personal direct contacts. Consequently, information sharing initiatives consisting of many members may not function efficiently and achieve their objectives. This does not mean however that there are no successful examples of large-size initiatives.
Different interests of the participants	Some companies are afraid that other members are only participating for commercial or lobbying purposes and not to really share on cyber security, threatening the success of the initiative.

ELEMENTS IMPACTING TRUST	POSSIBLE EXPLANATION
Insufficient protocols/agreements to guarantee information sharing	Certain initiatives do not use protocols (such as the TLP) or agreements on the way the information should be dealt with (such as non-disclosure agreements). Therefore, companies do not know how their information will be handled by others (Bartnes, 2015).
Cultural differences	Members of information sharing initiatives may come from different countries or different segments of the energy sector – this impacts their way of communicating and behaving especially during direct interaction. These differences tend to make the information sharing and the trust building process more difficult. Although this is not necessary specific for energy, it is an aspect that cannot be neglected.
Concerns about sharing proprietary, confidential or secret information	As the energy sector processes a large variety of sensitive and strategic information, some participants may rise concerns about sharing proprietary, confidential or secret information. This is related to their need, and sometimes legal obligations, to protect these information.

On the other hand, trust is also an important driver for the success of the initiative. When a good level of trust is achieved in a group, information is more likely to be exchanged. As trust is a key element for information sharing, good practices and recommendations are suggested in the next sessions.

6.1.2 Constrains to the Commitment of Those Participating in the Information Sharing Process

The interviewees mentioned that one of the shortcomings relates to the commitment and the role of participants in information sharing initiatives, especially initiatives involving cyber security information. From their experience, certain energy sector organisations usually welcome information provided by other members, but only share limited information in return. One explanation for this relates to the fact that the organisations in question are facing many constraints and do not always appoint the right or the most relevant person to the information sharing meeting/discussion. Instead of sending technical people who could give precise and detailed information, many participating organisations choose to send professionals from mid-management or in lobbying positions. Often, these persons may not be able to follow a technical conversation and may fail to pass the key information and messages back to their organisation.

One key weak point linked to the attendance of energy sector stakeholders to cyber security information sharing initiatives is that the top management of participating organisations is rarely or never represented. The apparent lack of interest, participation or proper representation (via delegates) of the top management is not encouraging the information sharing initiatives and simply undermines them in the medium to long term. This is particularly important in the energy sector and its subsectors, due to the noted positive “snowball effect” of various initiatives directly led or supported by the leaders of organisations relevant for the sector. Unfortunately, the cyber security information sharing initiatives in the energy sector do not yet benefit from the public and clear involvement, commitment and support of the sector leaders.

6.1.3 Complexity of the Energy Systems and of Cyber Security and Lack of Specialist Knowledge

Nowadays, the energy sector systems, processes and technologies used by the sector stakeholders are becoming increasingly complex. The energy system is a fast-growing environment where new actors (e.g. aggregators of data) and trends (e.g. smart grids, smart meters, new services, etc.) are emerging and evolving. In this context, cyber security is increasingly important in this sector and this might also involve more difficulties for those who would like to share information. The level of maturity and knowledge must be the same and this balance is not always easy to find (Wueest, 2014; Bartnes, 2015). This complexity, partially described in Chapter 4, was confirmed during the interviews with the stakeholders. According to one interviewee, only a few energy sector specialists have a real in-depth understanding of what is key and what is actually happening in the cyber security domain in the energy sector. This situation is mainly due to complexity of the energy sector, and because these knowledgeable people often carry heavy workloads. Therefore, it is very difficult for a broader group of energy sector professionals to have access to relevant information – especially when it comes down to cyber security.

6.1.4 National Interests

Interviewees mentioned that too often energy security issues are addressed only at the Member State level (i.e. with a national focus only) without taking into account the complexity of the interdependence of Member States in multiple aspects of the energy area, including cyber security. The key to improved energy security lies first in a more collective approach through a functioning internal market and greater cooperation at regional and European levels, in particular for coordinating network developments and opening up markets, and second, in a more coherent external action.

6.1.5 Complexity and Fragmentation of the Legal and Policy Context, and Energy Relevant Legislation Not Addressing Cyber Security

In Chapter 3, we provided an overview of the EU policy relevant to cyber security and the energy sector. We noted that the EU institutions put a large and increasing focus on cyber security and especially on information sharing between stakeholders of the sector (authorities, associations, companies, experts etc.). That said, one issue is the complexity and the fragmentation of legislation within the EU, which makes the information exchange more difficult (ENISA, 2015a). Moreover, NRAs do not always have the means and the legal rights to execute their tasks. However, the adoption of the NIS Directive and the entering into force of the GDPR in 2018 are expected to help to overcome these obstacles.

In addition, as described in Chapter 3, energy relevant legislation does not address, or at least not in detail, cyber security and more specifically cyber security information sharing.

6.1.6 Possible Legal Constraints

When the legal framework is particularly complex and unclear, the CSIRTs are more inclined to keep information for themselves, instead of sharing information (ENISA, 2011b). Information sharing appears to be facilitated when the CSIRTs know they are not taking non-compliance risks (i.e. that there are no legal impediments to do so, or no limitations coming from own statute and rules). The hesitance to share information might also relate to the mandate of each CSIRT, in the sense that the powers and duties allocated to the CSIRTs may directly or indirectly limit the willingness and possibilities to share information. However, some of the interviews with the CSIRTs showed that this attitude is starting to change and that many, if not all, CSIRTs are aware of the importance and need of technical cooperation and exchange of information between them, both at national and international level.

Moreover, based on the interviews conducted for this report, we also understood that the anti-trust laws are sometimes a barrier to share information and have an effect on the way information is shared. Indeed, if companies share too many details on their way of working or of their strategy, this could be perceived as collusion. This is why certain sharing group have decided not to cite specific brands or vendors with the other members of the sharing group.

6.1.7 Enforcement of Standardisation

It appears that standards for supporting the implementation of information security and cyber security controls tailored to the specificities of the energy sector are used by some actors but not by all and their use is not strictly enforced. This has a negative impact on the implementation of common cyber security risk management practices across the sector. It also makes it more difficult to establish a common base of understanding of information and cyber security issues specific to the energy sector.

6.1.8 Quality of Information Shared

The success of the information sharing initiatives also depends on the quality of the information shared. According to one interviewee, sometimes organisations share information in a way that is not always readable or understandable (i.e. they do not give enough details or they excessively use internal acronyms/jargon/language), and do not use the applicable taxonomy of the sharing initiative. This makes it hard for the other participants to correctly understand the shared information or to properly leverage the information within their respective organisation.

6.1.9 Different Interests at Stake

The energy sector is broad and participating actors (especially commercial companies) do not always have the same interests when it comes to sharing information. Some wrongfully consider that the information sharing initiative is only an opportunity to build commercial relationships or to receive non-technical information. Not all members are on the same page or do not have the same vision on the purpose of the initiative and the way to share. Consequently, information sharing initiative participants are not always able to exchange information and views in an efficient and effective way.

One specific point of attention is the need for having credible and balanced moderators of the information sharing initiative, who have the capacity to reconcile the sometimes very different interests of the participants in order to maintain sharing in a manner which brings mutual benefit.

6.1.10 Public and Private

Interviewees mostly agreed that information sharing is more challenging in the public sector:

- In general, the public sector entities do not manage an operation technology and energy infrastructure. As a result, they do not easily identify the added value of sharing cyber security information.
- On the one hand, the public sector provides services of public interest and, by definition, should openly share information. On the other hand, the public sector has a strong interest to have the information on critical infrastructure protected. This can be seen as a blocking factor from energy stakeholders who tend to keep the information on their critical infrastructure secret. Therefore, the public sector needs to be careful with the information they are allowed to share to avoid losing the trust of the participants of information sharing initiatives.

Additionally, one interviewee mentioned that we cannot rely on the public sector only. To understand and address cyber issues we need to know what is happening in the public and private sectors because one cannot be separated from the other.

6.1.11 Heterogeneous Players

Based on the different interviews and as explained in the previous chapters, the energy market is complex and composed of many different stakeholders (distributors, producers, regulators, authorities, etc.). These stakeholders vary in size and they come from different regulatory landscapes or cultures. The level of maturity and investment is also not the same from a country to another or from a subsector to another (e.g. the electricity subsector appear to be more mature than the nuclear sector in terms of information sharing on cyber security).

All these differences between the stakeholders make the information exchange more difficult and less homogenous between the organisations.

6.1.12 Size of the Energy Market Player

The size of the information sharing participants (especially when several energy sector commercial companies are involved), in terms of turnover, number of employees or geographical coverage, is a key factor for their involvement in an information sharing initiative. As an example, an interviewee mentioned the case of Distribution System Operators (DSO) in Europe who are not currently highly involved in information sharing. Although there are many DSOs in the European landscape, most of them do not have the critical size to build information security risk management capabilities, which inherently limits their participation in information sharing initiatives. In some cases, the small size and lack of resources have an impact on their knowledge of the existence of information sharing initiatives.

In other cases, independently from their size, some companies are not internally ready to share information because they lack the tools, trainings and internal processes to implement a good workflow for sharing information. Some interviewees even reported that management does not invest enough in technical people and cyber security, and do not give the opportunity to technical teams to focus and gain experience in the field of cyber security. Finally, systems used to handle cyber security incidents are sometimes outdated in comparison with the current attacks and technologies, and technical teams often struggle in convincing the management to periodically invest in the security hardening of the systems against cyber threats.

6.1.13 Focus on Physical Security and Safety

The energy sector has to deal with two schools of thoughts, namely, people who think about safety first and people who think about security first.

Safety is related to the infrastructures and the physical security of people, networks, etc. The purpose is to be “free of harm”. Security encompasses safety and tries to go further by taking attacks, espionage or crime into account (Byres and Cusimano, 2010). This difference in the definitions and mentalities adds another difficulty layer in the path to improve awareness and preparedness on cyber security.

Two interviewees mentioned that many companies in the energy sector still give much more importance to the safety of their physical infrastructure than to the security of their IT systems. Both aspects need to be considered in the risk management approach. Interviewees reported that management needs to increase their awareness on the evolution of data and cyber security, and the transformation of the energy sector to include increasingly the data processing activities. Besides, they are not yet conscious, or willing to make the investments required, of the benefits that information sharing can bring to their organisation.

6.1.14 Lack of Good Practice and Promotion of the Information Sharing Initiatives

An important observation is that several interviewees mentioned that they are not aware of good practice in information sharing. This can be explained by the fact that either the stakeholders are not part of any initiative, or they are active in their own initiative and have not investigated the existing good practices at other information sharing initiatives.

Moreover, it seems that information sharing initiatives in the energy sector lack visibility within companies in the sector. This might be due to lack of promotion from certain initiatives or to the fact that certain organisations do not want to have too many members. Therefore, they limit the visibility of their sharing initiative.

6.2 Identified Good Practice

Focus is given below to the limited set of good practice that promote information sharing on cyber incidents in the energy sector. The limited amount of good practice is one of the shortcomings identified in the report.

6.2.1 Information Sharing Tools and Practices

During the interviews, we could confirm that that trust is the first driver for voluntary and mutual information sharing in the energy sector.

Ways of ensuring information sharing flows as suggested by the interviewees are:

- "Gentlemen's agreement", which is an informal legally non-binding agreement in which signing parties commit themselves in a mutual sharing (ENISA, 2015a).
- Non-disclosure agreement, which is a contractual arrangement.
- Chatham House Rule and the IRAM (Information Risk Assessment Methodology), which is a voluntary and non-enforceable arrangement as such.
- Potential exclusions of a member of the information sharing in case of information disclosure against agreed rules or in case of non-exchange of information.

The Chatham House rule states that "when a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed" (Chatham House, n.d.). The IRAM methodology "helps organisations better understand and manage their information risks" (ISF, n.d.). Certain organisations use this method to assess and give a score to each risk. Based on the score, people within the organisation know if they can share the information and if not, why they cannot share it.

In addition, some interviewees suggested that the (small) size of the forum has a positive impact on the information sharing as it instils mutual trust among the members. Indeed, members and organisers of initiatives tend to prefer interacting in smaller groups to create an environment where people know each other and feel comfortable exchanging information. For example, during conferences or big assemblies, participants are less prone to disclose many details as opposed to smaller for a, such as round tables.

Information sharing will depend on the type of activity organised to share information and the people representing the companies. For instance, if the sharing initiative is based on meeting and is composed by Chief Information Security Officers (CISOs) or high-level management, the discussions are likely to focus on governance or the strategy in the cyber security domain.

The following activities have been mentioned by the interviewees: training, workshops, round tables, webinars, assemblies, conferences, (virtual) portal, analysis/testing services, chat discussions, bi-lateral conversations, calls and exercises.

Specific tools can also help to ensure trust. For instance, the Cybersecurity Risk Information Sharing Program (CRISP), a public-private partnership, uses a tool that can be installed by stakeholders on their network. This device allows to share encrypted information on threats with an analysis centre. Afterwards, the centre shares the information and measures that can be taken with all other users (Reddi, 2016).

6.2.2 Legal and Regulatory Frameworks

While not "good practices" *per se*, regulatory changes in the last year do support the further establishment and formalisation of information sharing initiatives and cooperation – for the energy sector as well. This is the case with the adoption of the NIS Directive, which obliges each EU Member State to designate at least one CSIRT within a competent authority (Article 9). Member States shall ensure the effective, efficient, fast and secure cooperation of the national CSIRTs network, created in order to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation. Thus, it is expected that the NIS Directive (European Parliament and Council, 2016) will bring the actors of the public and the private sectors closer in terms of information sharing.

Importantly, the NIS Directive also lays down the creation of a CSIRTs network composed of representatives of Member States' CSIRTs and CERT-EU (Article 12). The network will be tasked with the exchange of information on CSIRTs services, operations and cooperation capabilities, the exchange and discussion of non-commercially sensitive information related to an incident and associated risks, the exchange and making available on a voluntary basis of non-confidential information on individual incidents.

6.2.3 Internal Processes Improvement

According to some respondents, the most important step before starting to share information with other organisations is to be ready internally to promptly gather and process data on their own. For this purpose, organisations must be aware of the importance of cyber security and must know what to do in case of incidents. This is why many organisations provide awareness trainings in order to change people behaviour regarding cyber security and incidents (phishing, attacks, denial of service, etc.) and make incident reporting a faster or even automated process. Moreover, exercises are also organised for the employees. Technical teams are trained in order to stay updated on the current threats and vulnerabilities (e.g. by following the ENISA cyber exercises and ENCS Red team/ Blue team training), whereas non-technical employees are tested to increase their awareness of potential cyber threats (e.g. phishing exercises).

The involvement of high-level management seems to be another important factor to promote information sharing and to actually prepare the organisations to share information. Organisations where the management invested to create a team of dedicated technical experts, to train the employee and raise awareness seem more ready to address cyber challenges and are more mature to share relevant information. This involvement and the level of investment is closely related to the understanding and the awareness from the management. Indeed, if managers understand the importance of cyber security, they will more likely give the opportunity to their technical teams to attend meetings with external groups, to participate to conferences or any other sharing initiative.

Finally, for organisations that cannot invest in internal and dedicated experts, the possibility to outsource this department exists and is used in the energy sector. In this case, an external provider does take care of the cyber security management aspects.

7. Conclusions and Recommendations

This report identifies the development of CSIRTs, ISACs, as well as relevant initiatives and propose recommendations to further enhance information sharing on cyber security incidents in the energy sector in EU Member States as well as EFTA countries. After the initial background information and description of the methodology, we first analysed the policy context and the functioning of the energy sector. Secondly, based on desk research and interviews with public and the private stakeholders from the energy sector, we identified several information sharing initiatives in EU and EFTA countries (as well from North and South America). Finally, challenges and good practice were identified to help the stakeholders of the energy sector to understand what can be improved in the field of information sharing and to show the possible ways to do it.

In this chapter we present our conclusions and propose some recommendations.

7.1 Conclusions

7.1.1 Main Actors and Initiatives in the Energy Sector

This report shows that information sharing analysis centres are not widely developed in Europe. The report identifies some ISACs specific to the energy sector, two in the Netherlands (Energy and Nuclear ISACs), one in the UK (CiSP) and the EE-ISAC active at EU level. Clearly, the Netherlands and the United Kingdom appear to be pioneers in the implementation of ISACs and these examples should be reproduced in all EU Member States. At the EU level, the EE-ISAC, launched in 2015, enables sharing of information beyond the borders of a Member State. Moreover, since 2012, ENCS has been active in the creation and sharing of security expertise for energy grid operators.

Although CSIRTs are widely developed in Europe (ENISA, 2015) and provide security services to all sectors of activities, very few are focused solely on incident management in the energy sector. There are private CSIRTs specific to the energy sector, for instance, in Norway, Portugal and the United Kingdom, conducting their activities in the electricity, oil and gas segments. The Dutch NCSC have built strong CSIRT capabilities too, although their scope is larger than the energy sector. Representatives from two out of the four CSIRTs interviewed for this report confirmed that their CSIRT was involved in information sharing initiative with the EE-ISAC at EU level and CiSP in the UK.

In total, thirty-five ISACs, CSIRTs, and information sharing initiatives have been identified (see Annex C). Some of these are national, other European or international. Some of them covers the all energy sector (two are actually broader than the energy sector, in particular the NCSC-FI and Slovenian CSIRTs), some are focused on specific energy subsectors.

Overall, it appears that the promotion of information sharing initiatives in the energy sector could be further developed. Many companies, for instance, are not very aware of good practices or good initiatives in their sector.

An important challenge for the existing and future ISACs lies in the promotion of their activities to enable to gain more members and enable access to relevant cyber security information that can benefit all actors of the energy sector.

7.1.2 Added Value of Information Sharing for the Energy Sector

Based on the interviews conducted, we conclude that the value added of information sharing practices in the energy sector is not widely known. Nevertheless, from the interviews, we understand that the information initiatives provide the possibility to interact with similar and relevant actors with the aim to secure their organisations and its information. It is a mean to gain experience from others, to improve work behaviours and to reach a certain level of standardization and maturity throughout the sector in order to achieve higher maturity with regards to security. By leveraging on the work performed by peers, efficiency is gained.

Nevertheless, sharing information is perceived as a long-term investment by certain companies. Some companies sharing a lot of information right now might only receive something "in exchange" in many years.

7.1.3 Importance of Trust in Information Sharing Initiatives

The results of the interviews confirmed the key role of trust on information sharing in the cyber security area. Trust is a driver and a challenge at the same time. We understood that trust is difficult and time consuming to build but once it is achieved, community members are more likely to exchange information. On the contrary, if trust does not exist between stakeholders, the amount and the quality of shared information may be lower than expected and sometimes, even useless.

To build trust, information sharing organisations use tools and practices. Moreover, elements such as the size of the organisation and the setting of the meetings (informal meetings, conferences, calls, trainings) could have an impact on the trust too.

7.1.4 Heterogeneity of Players Involved in Information Sharing Initiatives

In terms of actors, the energy sector is quite complex. Distributors, producers, regulators, authorities, etc. all have an important and different role in the sector and consequently, have different objectives and visions. This complexity affects the willingness of the organisations to share information as it includes having to deal with different levels of maturity, different cultures and ways of working.

In fact, as the energy market is still mainly managed at national level, different interests exist. Moreover, it seems that differences in terms of maturity can also be found between the various actors. For example, distributors of energy seem to be less mature and less aware of the potential benefit of information sharing than the producers of energy. This can be observed when reviewing the feedback provided by participants or members of the information sharing initiatives.

Finally, it is a fact that people participating to the information exchanges have also different backgrounds. Certain initiatives gather a mix of technical people, decision makers and policy people at the same time. This makes the communication more difficult as they do not always have the same views on a cyber security matter, the same knowledge and understanding, and - in many cases - they do not use the same definitions and a common taxonomy on cyber incidents and cyber issues in general.

7.1.5 Importance Given to Cyber Security in Comparison to Cyber Safety

A number of interviewees mentioned that many energy sector private organisations (companies) have still a so called "old management style" of their information. This means that these companies are not yet aware that besides their principal role of energy producer or distributor, they are becoming a huge possessor of data. It seems there is also a tendency by energy sector companies to consider that safety of their physical infrastructure is more important than the security of their system, which also encompasses non-physical/cyber information. Because of that, some companies have not yet understood the importance of sharing information about cyber issues.

On the other hand, we note that companies that are aware of the importance of cyber security and the risks involved make the needed investment. Dedicated teams are built, top-management is involved in these issues and awareness is also raised among non-technical employees of the energy sector company / organisation.

7.1.6 Policy and Legal Framework Facilitating Information Sharing

Increased effort and focus is put on information sharing in the energy sector. The public sector wants to understand how the market works and wants to join efforts with the actors of the energy market. Certain actors, such as the European Commission, are motivated to raise awareness on the subject and to make all actors understand that energy companies are all interrelated and that their security is only possible if all actors are secured. For this purpose, actors must cooperate and collaborate.

For the moment, a lack of alignment still exists between the regulatory frameworks for information sharing and regarding data protection in EU. However, this should be alleviated with the entering into force of the GDPR and the NIS Directive, which will provide enhanced legal certainty to the sector in terms of information exchange.

Along with legal reporting issues, it was also mentioned that anti-trust laws can sometimes hinder information sharing initiatives as it might be perceived as collusion by authorities.

7.2 Recommendations

Based on the results of this report and the practices highlighted, several recommendations are proposed, aimed to improve information sharing on cyber security topics in the energy sector. Each recommendation is relevant for certain categories of stakeholders.

7.2.1 Invest in Cyber Security Internally and in the Information Sharing to Increase the Maturity of the Organisation and the Sector

The management of the private companies in the energy sector should invest in cyber security – currently cyber security receives low priority and has a lower level of maturity compared with other sectors. First, technical employees should be trained and some of them should be dedicated to cyber security. Knowledge, capabilities and information exchanges can be built by participating to conferences, calls, access to (virtual) library, etc. Secondly, awareness should be raised throughout the entire organisation – at all levels. Non-technical employees and top-management should be informed of potential cyber security issues and their impact on the organisation. Typical examples are trainings, internal exercises, awareness raising campaigns, etc.

Finally, the tools used to manage cyber security should also be taken into account in this investment perspective as they are crucial for technical teams. The purchase of a tool should be part of a long-term plan within the energy sector company/organisation and should be thoroughly analysed by the procurement team – with direct input from the cyber security experts. This better knowledge and planning of the tool will allow the cyber team to easily identify their vulnerabilities on the long-term and to plan updates or the replacement of the technologies.

Recommendation for:

- Energy sector companies (high-level management and IT management).

7.2.2 Make Top Management More Involved in Cyber Security Issues

The high-level (top) management and IT management should become more involved in the cyber security issues related to their organisation and should be well aware of them. This is particularly important in the energy sector and its subsectors, especially due to the noted positive “snowball effect” of various initiatives directly led or supported by the leaders of organisations relevant for the sector.

The top management representatives should promote cyber security within their organisation and endorse/sponsor the implementation of processes aimed to better share information internally and externally.

Information sharing initiatives' facilitators, if needed with the support of ENISA, should develop material and provide opportunities to disseminate the message that the involvement of management of energy companies in cyber security issues is essential.

Moreover, participation or proper representation (e.g. via delegates) of the top management in information sharing initiatives will be a strong motivator and will be further encouraging these initiatives.

Recommendation for:

- Information sharing initiatives' facilitators
- Energy sector companies (high-level management and IT management)
- ENISA.

7.2.3 Promote ISACs, CSIRTs and Information Sharing Initiatives

Many energy companies are not aware of the ISACs and of the existing information sharing initiatives in the energy sector and their benefits. In this context, information sharing initiatives need to be more visible in the energy sector in order to involve all the actors. Instead of using commercial means to reach stakeholders, information sharing organisations should promote their activities by showing the added value of their initiative in an informal and trustful way. The initiatives themselves should not neglect the awareness aspect and the need to reach out to larger audiences and groups of energy sector stakeholders.

To offer a better view on the way to share information, one of the ISACs, CSIRT or information sharing initiatives' facilitators/moderators already active in the field, if needed with the support of ENISA, should compile and keep updated a map of all energy ISACs, CSIRTs (public or private) and existing information sharing initiatives.

Finally, even if the size of the group has an impact on information sharing, members should promote their group externally in order to have all the relevant actors in their initiative.

Recommendation for:

- ISACs, Information sharing initiatives' facilitators/moderators
- Members of the information sharing initiatives
- ENISA.

7.2.4 Harmonise the Legal Framework to Share Information

Given the importance of cyber security information sharing in the energy sector, the size and the number of actors involved, as well as the high level of inter-relations in the energy sector, mechanisms should be put in place to circulate information promptly and even automatically.

In this context, it is important to have a legal framework to facilitate information sharing between companies and countries. However, it seems that, for instance, data protection laws slightly differ from a Member State to another based on different implementation of the European Union directives in national laws and different interpretations. The adoption of the NIS Directive (European Parliament and Council, 2016) and the entering into force of the General Data Protection Regulation (GDPR) (European Parliament and Council, 2016a) in 2018 are expected to help to provide a more harmonised legal framework.

Moreover, according to certain interpretations of anti-trust laws, information sharing initiatives might sometimes be perceived as collusion. This might find application also in the information sharing in the energy sector.

EU and national policy makers, law makers and regulators should continue working together toward a legal framework as clear and as harmonised as possible to share information on cyber incidents. ENISA could support them by injecting its expertise. The information sharing in the energy sector would also benefit from this.

Recommendation for:

- EU and national policy makers, law makers and regulators
- ENISA.

7.2.5 Promote the Use of Existing Definitions and of a Common Taxonomy, Enhance the Information Flow Internally and with Other ISACs and Information Sharing Initiatives

Based on the interviews, it appears that energy sector organisations do not yet use the already existing definitions that have been developed in the cyber security arena for sharing information about incidents. In addition, they do not use a common taxonomy, preferably to be selected among already existing taxonomies[38]. This might be because different professional profiles (policy people, technical people, lobbies, etc.) participate to the information sharing meetings. As these people have different backgrounds, it is difficult to always share precise and relevant information.

To avoid misunderstandings, in addition of limiting as much as possible the changes in their representation in the ISAC/information sharing initiative, members of ISACs/information sharing initiatives should align on the definitions and a common taxonomy by using those that have been already developed by the CSIRT community for sharing information about incidents.

In addition, they should identify mechanisms to share information with other ISACs, CSIRTs and initiatives. This with the aim also to avoid duplications of work and to exploit possible synergies. This would allow them to find commonalities, to enhance their information flow and to improve their way of working internally and with other ISACs/initiatives.

Information sharing initiatives' facilitators have an important role to play in promoting the use of existing definitions and a common taxonomy as well as identifying information sharing mechanisms.

Recommendation for:

- Members of ISACs/information sharing initiatives
- Information sharing initiatives' facilitators.

7.2.6 Ensure Trust

As stated before, trust is a major component of information exchange in cyber security. Based on the examples given by the community, organisations could use the following to build and ensure trust:

- Develop a code of conduct or an internal agreement: this agreement will state all the rules that members have to follow when they become part of the initiative. For example, they could implement rules on the number of participants, on the background of the participants or the way information shared must be handled
- Chatham House rule: this should allow members to handle information exchanged following a rule that is known worldwide
- Traffic Light Protocol (TLP): this tool would be used as a standard practice to share information by using a code known by all the member of the initiative.

[38] For an overview of some of the existing taxonomies, see ENISA, 2015b.

Finally, as the location and setting of the information sharing initiative seem to have an impact of trust building, information sharing organisations should allow members to meet and to relate easily. Small and informal meetings seem to be the best way to build a community of trust. The organisations should limit as much as possible the changes in their representation in the ISAC/information sharing initiative.

Recommendation for:

- Information sharing initiatives' facilitators
- Members of ISACs/information sharing initiatives.

7.2.7 Learn from the Experience of Other Sectors

The energy sector can learn and benefit from the cyber security developments in the financial or the chemical sector. Because of the high exposure of the computer systems that process operations and financial data and the high impact on their business activities and financial assets, the financial sector highly invested in the improvement of their cyber security capabilities and in the sharing of information on cyber security. The same applies for the chemical sector.

Nowadays, the energy sector activities are transforming by integrating more and more digital information processing (e.g. smart grid data), which have a high business value. Organisations from the energy sector (energy sector companies in general, information sharing initiatives' facilitators and members of ISACs and information sharing initiatives) should leverage on the security work performed in sectors such as the financial and the chemical sectors and apply lessons learned from these sectors.

They could engage in cross-sector information sharing or in bi-lateral relations with organisations or information sharing initiatives of these sectors. This would allow them to find out good practices and lessons learned that apply to the energy sector.

Recommendation for:

- Energy sector companies
- Information sharing initiatives' facilitators
- Members of ISACs/information sharing initiatives.

7.2.8 Further Develop and Use Standards on Information and Cyber Security Management in the Energy Sector

Standards can be developed and used to further improve harmonisation of the cyber security risk management practices across the energy sector and to establish a common base of understanding of security issues that are specific to the energy sector. As an example, the ISO 27000 series of standard[39] is a well-recognised and established standard for information security management developed by the International Organization for Standardization (ISO). The organisation has developed the ISO 27019 standard[40] for process control systems specific to the energy utility industry.

A collaboration between standard developing organisations, energy companies, facilitators of sharing initiatives and any other parties can enable adoption and can be a solid platform to enforce the use of information security standards tailored to the energy sector. ENISA could support this process by identifying gaps and proposing possible solutions.

[39] http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=66435, last access: 10 August 2016.

[40] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43759, last access: 10 August 2016.

Recommendation for:

- Standards developing organisations
- Energy sector companies
- ENISA.

8. Bibliography

Note: “n.d.” (for “no date”) is used in the case when no date could be found for the sources.

ACER (Agency for the Cooperation of Energy Regulators), ‘Mission & Objectives’, n.d. Retrieved October 13, **2016**, from http://www.acer.europa.eu/en/The_agency/Mission_and_Objectives/Pages/default.aspx

Bartnes L., ‘Understanding Information Security Incident Management Practices – A Case Study in The Electric Power Industry’, **2015**. Retrieved June 8, 2016, from http://infosec.sintef.no/wp-content/uploads/2015/09/2015-MBL-PhD-thesis-Part-1-2.pdf

Byres, E., Cusimano, J., ‘Safety and Security: Two Sides of the Same Coin’, **2010**. Retrieved July 4, 2016, from http://www.controlglobal.com/articles/2010/safetysecurity1004/

Chatham House, ‘Chatham House Rule’, n.d. Retrieved 17 October 2016 from https://www.chathamhouse.org/about/chatham-house-rule

Council of the European Union, ‘Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection’, **2008**, p. 79. Retrieved August 3, 2016, from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN

Council of the European Union, ‘Directive 2014/87/EURATOM - Establishing a Community Framework for the nuclear safety of nuclear installations’, **2014**. Retrieved June 1, 2016, from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0087&from=EN

CIO Platform Nederland and Rabobank, ‘Coordinated Vulnerability Disclosure Manifesto’, 2016. Retrieved June 15, **2016**, from http://www.cio-platform.nl/uploads/CioPublicatie2016%20CEG%20Information%20Security%20Coordinated%20Vulnerability%20Disclosure%20Manifesto%202016-04-18.pdf

E-ISAC and SANS, ‘Analysis of the Cyber Attack on the Ukrainian Power Grid’, March 18, **2016**, p. 21. Retrieved November 15, 2016, from https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

EE-ISAC (European Energy - Information Sharing & Analysis Centre), ‘Home page’, **n.d.** Retrieved May 13, 2016, from http://www.ee-isac.eu/

EFTA (European Free Trade Association), ‘The EFTA States’, **n.d.** Retrieved October 9, 2016, from http://www.efta.int/about-efta/the-efta-states

ENISA, ‘Incentives and Challenges on Information Sharing’, **2010,** p. 9. Retrieved May 17, 2016, from https://www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing

ENISA, ‘Getting the right concept by using the right words: obtaining a common glossary for resilience’, **2011,** Retrieved October 30, 2016, from https://www.enisa.europa.eu/news/enisa-news/getting-the-right-concept-by-using-the-right-words-ontology-taxonomies-for-critical-infrastructures

ENISA, ‘Ontology and taxonomies of resilience’, **2011a**, p. 41. Retrieved October 30, 2016, from https://www.enisa.europa.eu/publications/ontology_taxonomies

ENISA, ‘A flair for sharing - encouraging information exchange between CERTs’, **2011b**, p. 7. Retrieved May 15, 2016, from https://www.enisa.europa.eu/publications/legal-information-sharing-1

ENISA, ‘Protecting Industrial Control Systems. Recommendations for Europe and Member States’, **2011c**, p. 23. Retrieved June 8, 2016, from https://www.enisa.europa.eu/publications/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states

ENISA, ‘Deployment of Baseline Capabilities of n/g CERTs - Status Report 2012’, **2012**. Retrieved June 8, 2016, from https://www.enisa.europa.eu/publications/status-report-2012

ENISA, 'Good practice guide for CERTs in the area of Industrial Control Systems - Computer Emergency Response Capabilities considerations for ICS', 2013, p. 29. Retrieved June 8, 2016, from https://www.enisa.europa.eu/publications/good-practice-guide-for-certs-in-the-area-of-industrial-control-systems

ENISA, 'Report on Cyber Crisis Cooperation and Management', **2014a**. Retrieved May 17, 2016, from https://www.enisa.europa.eu/publications/ccc-study

ENISA, 'Scalable and Accepted Methods for Trust Building', **2014b**, p. 1. Retrieved August 29, 2016, from https://www.enisa.europa.eu/publications/scalable-and-accepted-methods-for-trust-building

ENISA, 'ENISA – CERT Inventory', **2015**, p 7. Retrieved May 17, 2016, from https://www.enisa.europa.eu/publications/inventory-of-cert-activities-in-europe

ENISA, 'Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches', **2015a**, pp. 12ff, p. 29. Retrieved June 8, 2016, from https://www.enisa.europa.eu/publications/cybersecurity-information-sharing

ENISA, 'Information sharing and common taxonomies between CSIRTs and Law Enforcement', **2015b**, pp. 20ff. Retrieved October 31, 2016 from https://www.enisa.europa.eu/publications/information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement

ENISA, 'Work Programme for 2016 – Including multiannual planning', **2016**, pp. 42ff. Retrieved May 17, 2016, from https://www.enisa.europa.eu/publications/programmes-reports/enisa-work-programme-2016

ENISA, 'From the Netherlands Presidency of the EU Council: Coordinated vulnerability disclosure Manifesto signed', **2016a**. Retrieved June 8, 2016, from https://www.enisa.europa.eu/news/member-states/from-the-netherlands-presidency-of-the-eu-council-coordinated-vulnerability-disclosure-manifesto-signed

ENISA, 'Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations', **2016b**. Retrieved May 17, 2016, from https://www.enisa.europa.eu/publications/vulnerability-disclosure

ENISA, 'ENISA Threat Taxonomy', **2016c**, p. 4. Retrieved October 5, 2016c, from https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information

ENISA, 'Glossary', **n.d.** Retrieved May 17, 2016, from https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary

ENISA, 'National/governmental CERTs - Baseline Capabilities', **n.d.(a)**. Retrieved May 17, 2016, from https://www.enisa.europa.eu/topics/national-csirt-network/csirt-capabilities/baseline-capabilities

ENISA, 'Considerations on the Traffic Light Protocol', **n.d.(b)**. Retrieved June 8, 2016, from https://www.enisa.europa.eu/topics/national-csirt-network/glossary/considerations-on-the-traffic-light-protocol

ENTSO-E, 'Synthetic overview of electric system consumption, generation and exchanges in the ENTSO-E area', **2015**, p. 6. Retrieved May 17, 2016, from https://www.entsoe.eu/Documents/Publications/Statistics/electricity_in_europe/entsoe_electricity_in_europe_2014.pdf

ENTSO-E, 'Scenario outlook & adequacy forecast', **2015a**, p. 5. Retrieved May 17, 2016, from https://www.entsoe.eu/Documents/SDC%20documents/SOAF/150630_SOAF_2015_publication_wcover.pdf

ENTSO-E (European Network of Transmission System Operators), 'Who Is ENTSO-E?', **n.d.** Retrieved October 14, 2016 from https://www.entsoe.eu/about-entso-e/Pages/default.aspx

ENTSOG (European Network of Transmission System Operators for Gas), 'Mission', **n.d.** Retrieved October 14, 2016 from http://www.entsog.eu/mission

European Commission, 'EUROPE 2020 - A strategy for smart, sustainable and inclusive growth', **2010**. Retrieved May 25, 2016, from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:EN:PDF

European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe, COM/2010/0245 final, **2010a**. Retrieved 14 November 2016, from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52010DC0245

European Commission, 'Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', **2013***.* Retrieved April 30, 2016, from http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

European Commission, 'Proposal for a Directive of the European Parliament and the Council concerning measures to ensure a high common level of network and information security across the Union', **2013a**. Retrieved May 25, 2016, from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013PC0048

European Commission, Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union, SWD/2013/032 final, **2013b**, p. 16. Retrieved October 30, 2016 from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013SC0032

European Commission, 'Communication from the Commission to the European Parliament and the Council 'European Energy Security Strategy'*,* **2014**, p. 6. Retrieved April 24, 2016, from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0330&from=EN

European Commission, 'Commission Implementing Regulation (EU) No 1348/2014 of 17 December 2014 on data reporting implementing Article 8(2) and Article 8(6) of Regulation (EU) No 1227/2011 of the European Parliament and of the Council on wholesale energy market integrity and transparency', **2014a**. Retrieved October 13, 2016, http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32014R1348

European Commission – DG Energy, 'Energy Union Package – Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank, A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy'*,* **2015**, p. 14. Retrieved May 17, 2016, from http://eur-lex.europa.eu/resource.html?uri=cellar:1bd46c90-bdd4-11e4-bbe1-01aa75ed71a1.0001.03/DOC_1&format=PDF

European Commission – DG Energy, 'Energy Expert Cyber Security Platform (EECSP). Terms of References (EECSP) & Call for Experts (EESCP-Expert Group)', **2015a**. Retrieved June 2, 2016, from http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=21274&no=1

European Commission, 'Press release - Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats', 5 July **2016**, from http://europa.eu/rapid/press-release_IP-16-2321_en.htm Reference is made in this press release to the survey available at http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html on 5 July 2016

European Commission, 'Fact Sheet: Questions and Answers - Data Protection Reform', **2016a**. Retrieved June 8, 2016, from http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm

European Commission, 'Nuclear Energy – Overview', **n.d.** Retrieved August 11, 2016, from https://ec.europa.eu/energy/en/topics/nuclear-energy

European Commission, 'ITIS-EUC FAQ', **n.d.(a)**. Retrieved October 11, 2016, from https://itis.jrc.ec.europa.eu/faq

European Commission – DG Energy, 'Energy Security Strategy', **n.d.(b)**. Retrieved May 18, 2016, from http://ec.europa.eu/energy/en/topics/energy-strategy/energy-security-strategy

European Parliament and Council, 'Directive 94/22/EC - Conditions for granting and using authorizations for the prospection, exploration and production of hydrocarbons', **1994**. Retrieved June 1, 2016, from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31994L0022&from=EN

European Parliament and Council, 'Directive 95/46/EC of the on the protection of individuals with regard to the processing of personal data and on the free movement of such data', **1995**. Retrieved on June 17, 2016, from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046

European Parliament and Council, 'Directive 2003/54/EC of the European Parliament and of the Council of 26 June 2003 concerning common rules for the internal market in electricity and repealing Directive 96/92/EC', **2003**. Retrieved May 17, 2016, from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003L0054

European Parliament and Council, 'Regulation (EC) No 713/2009 - Establishing an Agency for the Cooperation of Energy Regulators', **2009**. Retrieved June 1, 2016, from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:211:0001:0014:EN:PDF

European Parliament and Council, 'Regulation (EU) No 1227/2011 - Wholesale energy market integrity and transparency', **2011**. Retrieved June 1, 2016, from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011R1227&from=FR

European Parliament and Council, 'Regulation (EU) No 347/2013 - Guidelines for trans-European energy infrastructure and repealing Decision No 1354/2006/EC and amending Regulations (EC) No 713/2009, (EC) No 714/2009 and (EC) No 715/2009', **2013**. Retrieved June 1, 2016, from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:115:0039:0075:en:PDF

European Parliament and Council, 'Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union', **2016**, pp. 27ff, p. 13, p. 15, pp. 11-12, p. 5, . Retrieved August 25, 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

European Parliament and Council, '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)', **2016a**. Retrieved June 9, 2016, from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Fukuyama, F., 'Trust: The Social Virtues and The Creation of Prosperity', Free Press, **1996**.

IAEA (International Atomic Energy Agency), 'IAEA Nuclear Security Series No. 17 – Technical Guidance Reference Manual - Computer Security at Nuclear Facilities', **2011**. Retrieved August 10, 2016, from http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf

IAEA (International Atomic Energy Agency) – Office of Nuclear Security, 'Cyber Security Programme', **n.d.**, Retrieved June 6, 2016, from https://www.iaea.org/NuclearPower/Downloadable/Meetings/2013/2013-05-22-05-24-TWG-NPE/day-2/4.cyber_security_introduction.pdf

IAEA (International Atomic Energy Agency), 'IAEA Safeguards Overview', **n.d.(a)**. Retrieved October 6, 2016 from https://www.iaea.org/publications/factsheets/iaea-safeguards-overview

ICS-CERT (Industrial Control Systems Cyber Emergency Response Team), 'Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure', Original release date: February 25, **2016**. Retrieved November 15, 2016 from https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

IEA (International Energy Agency), 'Energy Investment for Global Growth', 2016, p. 6. Retrieved October 30, **2016**, from

IEA (International Energy Agency), 'Cyber Security Collaboration Platforms: Reducing Risks for the Energy Sector'**, 2016a**. Retrieved June 6, 2016, from http://www.iea.org/media/topics/engagementworldwide/g7/IEAPresentationonCybersecurityatG7.pdf

IEA (International Energy Agency), 'IEA Energy Technology Roadmaps', **n.d.**, p.2. Retrieved October 30, 2016, from https://www.iea.org/media/topics/engagementworldwide/g7/IEAEnergyTechnologyRoadmapsNotefortheG7.pdf

ISF (Information Security Forum), 'Information Risk Assessment Methodology 2 (IRAM2)', **n.d**. Retrieved June 16, 2016, from https://www.securityforum.org/tool/information-risk-assessment-methodology-iram2/

ISO (International Organization for Standardization), 'Information technology - Security techniques - Guidelines for cybersecurity (ISO/IEC 27032:2012)', **2012**, p. 4. Retrieved May 17, 2016, from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44375

ISO (International Organization for Standardization), 'Information technology - Security techniques - information security management for inter-sector and inter-organizational communications (BS ISO/IEC 27010:2012). (British Standards Institution (BSI))', **2012a**. Retrieved May 17, 2016, from http://shop.bsigroup.com/ProductDetail/?pid=000000000030204594

Millar, T., 'Traffic Light Protocol (TLP) - BoFReturn to TOC', **2015**. Retrieved September 14, 2016, from http://www.first.org/conference/2015/program#ptraffic-light-protocol-tlp-bof

National Council of ISACs, 'About ISACs', **n.d.** Retrieved May 13, 2016, from http://www.nationalisacs.org/#!about-isacs/vu5l7

NIST (National Institute of Standards and Technology), 'Computer Security. Guide to Industrial Control Systems (ICS) Security', **2011**, p. 1. Retrieved October 30, 2016, from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82.pdf

NSS (Nuclear Security Summit), 'Joint Statement on Cyber Security', **2016**. Retrieved June 6, 2016, from http://www.nss2016.org/document-center-docs/2016/4/1/joint-statement-on-cyber-security.

OAS (Organization of American States) – Inter-American Committee Against Terrorism (CICTE), 'Declaration on Strengthening Cyber Security in the Americas', **2012**. Retrieved June 3, 2016, from https://www.oas.org/en/sms/cicte/Documents/Declarations/DEC_1%20rev_1_DECLARATION_CICTE00749E04.pdf.

OAS (Organization of American States) – Inter-American Committee Against Terrorism (CICTE), 'Declaration on Protection of Critical Infrastructure from Emerging Threats', **2015**. Retrieved June 3, 2016, from https://www.sites.oas.org/cyber/Documents/CICTE%20DOC%201%20DECLARATION%20CICTE00955E04.pdf

OAS (Organization of American States), 'Appendix A. A comprehensive Inter-American cybersecurity strategy: A multidimensional and multidisciplinary approach to creating a culture of cyber security', **n.d.** Retrieved June 3, 2016, from http://www.oas.org/juridico/english/cyb_pry_strategy.pdf.

OAS (Organization of American States), 'About us', **n.d.(a)**. Retrieved June 3, 2016, from https://www.sites.oas.org/cyber/EN/Pages/contacts.aspx.

Reddi, R., 'Cybersecurity Information Sharing in Electric Utilities', **2016**, p. 12. Retrieved June 8, 2016, from http://www.sgip.org/wp-content/uploads/SGIP-White-Paper-Cybersecurity-Information-Sharing-in-Electric-Utilities.pdf

Symantec, 'Targeted Attacks Against the Energy Sector, **2014**. p. 3. Retrieved October 21, 2016, from http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf

WENRA (Western European Nuclear Regulators Association), 'The mission of WENRA', **n.d.** Retrieved June 1, 2016, from http://www.wenra.org/about-us/.

World Economic Forum, 'Partnering for Cyber Resilience – Risk and Responsibility in a Hyperconnected World – Principles and Guidelines', **2012**. Retrieved June 17, 2016, from http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf

World Nuclear Association, 'Nuclear power in the European Union', **2016**, p. 14.Retrieved May 18, 2016, from http://www.world-nuclear.org/information-library/country-profiles/others/european-union.aspx

Wueest, C., 'Attacks Against the Energy Sector', **2014**. Retrieved June 8, 2016, from http://www.symantec.com/connect/blogs/attacks-against-energy-sector

Annex A - Acronyms

ACRONYM	DESCRIPTION
ACER	(EU) Agency for the Cooperation of Energy Regulators
ACT	Austrian Trust Circle
A-ISAC	Aviation - Information Sharing and Analysis Centre
ANSSI	(French) Agence Nationale de la Sécurité des Systèmes d'Information (National Cybersecurity Agency of France)
ARIS	ACER (Agency for the Cooperation of Energy Regulators, EU) REMIT (Wholesale Energy Market Integrity and Transparency) Information System
BWR	Boiling Water Reactor
CEER	Council of European Energy Regulators
CERT	Computer Emergency Response Team
CICTE	Secretariat of the Inter-American Committee Against Terrorism
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CiSP	Cyber Security Information Sharing Partnership
CIWIN	Critical Infrastructure Warning Information Network
CNSSIE	Civil Nuclear Sector SCADA Information Exchange
CNCS	(Portuguese) Centro Nacional de Cibersegurança (National Centre for Cybersecurity)
CPNI	Centre for the Protection of National Infrastructure
CRISP	(US Department of Energy) Cybersecurity Risk Information Sharing Program
CSDP	Common Security and Defence Policy
CSIRT	Computer Security and Incident Response Team
D	Deliverable
DAE	Digital Agenda for Europe
DECC	(UK) Department of Energy & Climate Change
DENSEK	Distributed Energy Security Knowledge
DG	Directorate General
DG CONNECT	(European Commission) Directorate General for Communications Networks, Content & Technology
DGO	Distribution Grid Operator
DNG- ISAC	Downstream Natural Gas - Information Sharing Analysis Center
DSO	Distribution System Operator
E3CC	Energy Emergencies Executive Committee for Cyber

ECI	European Critical Infrastructures
EEA	European Economic Area
EECSP	Energy Expert Cyber Security Platform
EE-ISAC	European Energy - Information Sharing Analysis Centre
EFTA	European Free Trade Association
E-ISAC	Electricity - Information Sharing and Analysis Center
ENCS	European Network for Cyber Security
ENISA	European Union Agency for Network and Information Security
ENTSO-E	European Network of Transmission System Operators for Electricity
ENTSOG	European Network of Transmission System Operators for Gas
EU	European Union
EURATOM	European Atomic Energy Community
EUROSCSIE	European SCADA and Control Systems Information Exchange
FI-ISAC	Financial Information Sharing and Analysis Centre
GCR	Gaz Cooled Reactor
GDPR	General Data Protection Regulation
IAEA	International Atomic Energy Agency
ICS	Industrial Control Systems Industrial Control Systems
ICT	Information and Communication Technologies
IEA	International Energy Agency
IoCs	Indicators of Compromise
IRAM	Information Risk Assessment Methodology
ISAC	Information Sharing and Analysis Centreer
ISF	Information Security Forum
ISO	International Organization for Standardization
IT	Information Technology
ITIS-EUC	Incident and Threat Information Sharing EU Centre
LRLIBEK	(Hungarian) Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ (Crucial Information Security Systems Facilities and Event Management Agency)
MS	Member State
NCSC	National Cyber Security Centre
NGL	Natural Gas Liquids
NGRID-CSIRT	National Grid Cyber Response Team
NIS	Network Information Security

NIST	National Institute of Standards and Technology
NRA	National Regulatory Authority
NSS	Nuclear Security Summit
OAS	Organization of American States
Ofgem	(UK) Office of gas and electricity markets
OGISF	Oil and Gas Information Sharing Forum
ONG-ISAC	Oil and Natural Gas Information Sharing Analysis Center
OT	Operations Technology
PCN	Process Control Networks
PHWR	Pressurised Heavy Water Reactor
PWR	Pressurised Water Reactor
REMIT	Wholesale Energy Market Integrity and Transparency
SCADA	Supervisory Control and Data Acquisition
SI-CERT	Slovenian Computer Emergency Response Team
SME	Small and Middle Enterprises
SO	Strategic Objective
SOC	Security Operations Centre
TLP	Traffic Light Protocol
TNCEIP	Thematic Network on Critical Energy Infrastructure Protection
TSO	Transmission System Operator
UP KRITIS	(German) UP Kooperation zwischen Betreibern Kritischer Infrastrukturen (Internet platform on Critical Infrastructure Protection)
US-NRC	United States Nuclear Regulatory Commission
WENRA	Western European Nuclear Regulators Association
WPK	Work Package

Annex B - Sample Questionnaire

Nr.	QUESTION
1.	**Is your organisation/company part of any ISAC or other information sharing initiative?** *Examples of possible organisations and participants:* ▪ *Intra-sector (only within the energy sector), cross sector (e.g. participants from energy sector and also other sectors such as water, finance, internet service, etc), intra-subsector (only oil, gas, nuclear, electricity, alternative fuels, etc energy subsector), cross-energy subsector (i.e. mix of participants from different energy subsector (oil, gas, nuclear, electricity, alternative fuels, etc.))* ▪ *Public/private organisations (e.g. only private companies, private and public, only public)* ▪ *CSIRTs representatives* o *National CSIRT?* o *Energy companies CSIRTs* o *Other CSIRTs?* ▪ *Only particular stakeholders/segments are involved, e.g. only Transmission System Operators (TSOs), only Distribution System Operators, only utilities companies, only vendors, etc.* ▪ *Etc* Answer:
2.	**Can you please describe your information sharing initiative/s (including ISAC and CSIRT) within the energy sector, and tell us about your role in the initiative?** *General info:* ▪ *Name* ▪ *Main subsector (e.g. oil, gas, nuclear, electricity, alternative fuels, etc.)* ▪ *Size (approximate number of members)* ▪ *Geography* ▪ *Are you a (co)-funder of the initiative? Are you member of it? Since when?* Answer:
3.	**What is the foundation for the information sharing initiative?** *Possible bases might be:* ▪ *Legal (the organisation had to be created based on the law)* ▪ *Private (sub)sector initiative (in case, please specify the subsector)* ▪ *Governmental (the initiative came from the government)* ▪ *Contracts between parties* ▪ *Private-public partnership* ▪ *Other internal rules* ▪ *Other* Answer:

Nr.	QUESTION
4.	**What ensures the information sharing within your initiative?** *Possible drivers might be:* ▪ *Trust-based* ▪ *Legal framework/ ad hoc rules* ▪ *Specific cyber threats* ▪ *Other* Answer:
5.	**What are the information sharing mechanisms used within the scope of the initiative?** *Possible ways to share information might be:* ▪ *Traffic Light Protocol (TLP)* ▪ *Conferences, seminars or workshops* ▪ *Training sessions* ▪ *Informal meetings* ▪ *Newsletters* ▪ *Platform/Forum (e.g. Cyber Threat Intelligence platform)* ▪ *Organisation of exercises* ▪ *Face-to-face meetings* ▪ *Mailing lists* ▪ *Portals* ▪ *Other* Answer:
6.	**What type of information is shared within the initiative?** *Possible information shared might be:* ▪ *Information on specific actual cyber incidents* ▪ *Modus operandi in certain topical cyber incidents* ▪ *Information on specific actual cyber threats* ▪ *Cyber security governance policies* ▪ *Cyber security management good practices* ▪ *Applicable laws and regulatory frameworks* ▪ *Cyber threat landscape* ▪ *Cyber threat mitigation procedures* ▪ *Lessons learned on cyber security events and/or incidents* ▪ *Other* Answer:
7.	**What is the typical information flow within the initiative you are involved in?** *Possible information flows might be:* ▪ *Constituents/participants share information between themselves directly.* ▪ *Constituents send the information to a single point of contact, being the organisation. The point of contact will then spread the information among the constituents.* ▪ *The organisation/secretariat of the information sharing initiative looks for/researches information and spreads it to the constituents* ▪ *Other* Answer:

Nr.	QUESTION
8.	**What are the main challenges that you face when sharing information on cyber incidents? Are there any challenges specific for the energy sector?** Answer:
9.	**What could be the possible ways to overcome these obstacles to the information sharing on cyber incidents in the energy sector or relevant for the energy sector too?** Answer:
10.	**What do you consider being "good practices" in the information sharing organisation in which you are involved?** **Could it be replicated in other information sharing initiatives?** Answer:
11.	**What can be improved in the information sharing, not only in your initiative?** ▪ *More public driven/more private driven* ▪ *More cross-country* ▪ *Etc.* Answer:
12.	**What incentives can be used to create and maintain an information sharing initiative (including ISACs and CSIRTs) in the energy sector or relevant for the energy sector?** Answer:
13.	**Do you think that sharing information is more challenging in a public or private sector?** Answer:
14.	**What is the added value to take part in the initiative?** Answer:
15.	**In addition to the initiative mentioned, do you sometimes share information on cyber incidents with other organisations directly?** **If yes, are these organisations active in the energy sector? Are these organisation from your country or from a different country?** Answer:
16.	**Have you participated in the past in another information sharing initiative on cyber incidents in the energy sector or relevant for the energy sector too?** Answer:
17.	**Are you aware of these information sharing initiatives within the energy sector or others relevant to the energy sector?** • European Network for Cyber Security (ENCS), EU • Joint Statement on Cyber Security, Intl • Cyber Security Collaboration Platform, IEA • Cyber Security Program, IAEA • Cyber Security Program, OAS • Distributed Energy Security Knowledge (DENSEK), EU

Nr.	QUESTION
	• European Energy – Information Sharing & Analysis Centre (EE-ISAC), EU • Energy Emergencies Executive Committee (E3CC), UK • European SCADA and Control Systems Information Exchange (EuroSCSIE), UK • Civil Nuclear Sector SCADA Information Exchange (CNSSIE), UK, • Groupes de travail sectoriels dédiés à la preparation des règles de sécurité prévues par l’article 22 de la loi de programmation militaire, FR, • Electricity Information Sharing and Analysis Center (E-ISAC), USA • Incident and Threat Information Sharing EU Centre (IT IS-EUC), EU • Downstream Natural Gas Information Sharing Analysis Center (DNG-ISAC), USA • Oil and Natural Gas Information Sharing Analysis Center (ONG-ISAC) • ACER REMIT Information System (ARIS), EU • Thematic Network on Critical Energy Infrastructure Protection (TNCEIP), EU • Civil Nuclear Sector SCADA Information Exchange (CNSSIE), UK • Nationaal Cyber Security Centrum (NCSC) Nuclear ISAC, Netherlands • Nationaal Cyber Security Centrum (NCSC) Energy ISAC, Netherlands • European Energy Expert Cyber Security platform (EECSP), EU Answer:
18.	**Do you know other relevant stakeholders from the energy sector that could be contacted for our study?** Answer:
19.	**Is there any additional information you wish to share with us?** Answer:

Annex C - Inventory of Identified ISACs, CSIRTs and Information Sharing Initiatives on Cyber Security in the Energy Sector

This non-exhaustive table lists energy sector-related ISACs and CSIRTs as well as information sharing initiatives existing in the energy sector that were found based on the desk research and the interviews with stakeholders.

First CSIRT, ISACs and initiatives related to all sector are listed, then those related to electricity, oil, gas, nuclear and alternative fuels subsectors.

	ISACS. CSIRTS AND INFORMATION SHARING INITIATIVE	ACRONYM/ABBREVATION	ENERGY SUBSECTOR	PUBLIC/ PRIVATE	KEY STAKEHOLDERS	GEOGRAPHIC COVERAGE	TYPE OF CYBER SECURITY INFO EXCHANGED	FREQUENCY TYPE OF FORUM	LINK
1.	European Energy - Information Sharing & Analysis Centre	EE-ISAC	All	Public Private	"Both private utilities and solution providers and (semi)public institutions such as academia, governmental and non-profit organizations share valuable information on cyber security & cyber resilience" (from EE-ISAC website) "Industry-driven, information sharing network of trust" (from EE-ISAC website: EE-ISAC, n.d.).		"Real-time security data & analysis Reports on security incidents and cyber breaches Technical & operational experiences with applied security solutions Lessons learned from past security issues Future challenges, security outlooks & warnings" (from EE-ISAC website: EE-ISAC, n.d.)	Meeting Platform	http://www.ee-isac.eu/

	ISACS. CSIRTS AND INFORMATION SHARING INITIATIVE	ACRONYM/ABBREVATION	ENERGY SUBSECTOR	PUBLIC/ PRIVATE	KEY STAKEHOLDERS	GEOGRAPHIC COVERAGE	TYPE OF CYBER SECURITY INFO EXCHANGED	FREQUENCY TYPE OF FORUM	LINK
2.	Electricity Information Sharing and Analysis Center	E-ISAC	Electricity	Public Private	Public institutions Private companies	United States of America	Security information	Platform	https://www.esisac.com/#about
3.	(Dutch) National Cyber Security Centre Energy ISAC	NCSC Energy ISAC	All	Public Private	Public institutions Private companies	The Netherlands	Cyber security incidents Red light sensitive information	Annual meeting	https://www.ncsc.nl/english/Cooperation/isacs.html
4.	Cyber Security Information Sharing Partnership, UK	CiSP	All	Public	Public institutions	Cyber Security Information Sharing Partnership, UK	Cyber security threats and vulnerabilities	Online Platform	https://share.cisp.org.uk (login required)
5.	National Cyber Security Centre Finland information sharing	NCSC-FI information sharing	All	Public	Public institutions Regulators Private companies	Finland	Cyber threats and vulnerabilities	Email	https://www.viestintavirasto.fi/en/cybersecurity.html
6.	KraftCERT (Norwegian energy sector CERT)	KraftCERT	All	Public Private	Statnett, Statkraft and Hafslund Established 30.10.2014 by Statnett, Statkraft and Hafslund after an initiative from NorCERT and Norwegian Water Resources and Energy Directorate	Norway (but also internationally especially in the future)	Security incidents		https://www.kraftcert.no/english/index.html

	ISACS. CSIRTS AND INFORMATION SHARING INITIATIVE	ACRONYM/ABBREVATION	ENERGY SUBSECTOR	PUBLIC/ PRIVATE	KEY STAKEHOLDERS	GEOGRAPHIC COVERAGE	TYPE OF CYBER SECURITY INFO EXCHANGED	FREQUENCY TYPE OF FORUM	LINK
					It is open for members to become owners.				
7.	EDP Distribuição CSIRT	N/A	Electricity	Private	Private company	Private company (Portugal)	Cyber security incidents	Company internal sharing mechanisms, plus part of the EE-ISAC	http://www.edp.pt/PT/Pages/SegurancaInformatica.asp
8.	Slovenian Computer Emergency Response Team	SI-CERT	All	Public Private	Public institutions Private sector	Slovenia	Cyber security incidents	Periodic awareness raising activities Periodic training	https://www.cert.si/en/
9.	CSIRT for the energy sector (under establishment)	N/A	All	Public Private	Government Public institutions	Austria	Cyber incidents and vulnerabilities Technical information Strategy	Meetings	N/A
10	Council of European Energy Regulators Cyber Security Task Force	CEER Cyber Security Task Force	All	Public	EU Energy Regulators, including Norway and Switzerland	European Union Norway Switzerland	Cyber security information	Annual and monthly Workshops/trainings	CEER website: http://www.ceer.eu/portal/page/portal/EER_HOME
11	Critical Infrastructure Warning Information Network	CIWIN	All	Public	European Commission Members of the EU's CIP Community	European	Critical Infrastructure Protection-related information	Portal	http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network/index_en.htm

	ISACS. CSIRTS AND INFORMATION SHARING INITIATIVE	ACRONYM/ABBREVATION	ENERGY SUBSECTOR	PUBLIC/ PRIVATE	KEY STAKEHOLDERS	GEOGRAPHIC COVERAGE	TYPE OF CYBER SECURITY INFO EXCHANGED	FREQUENCY TYPE OF FORUM	LINK
12	Energy Expert Cyber Security Platform (Expert Group lead by European Commission, DG Energy)	EECSP	All	Public	Individual experts Common interest representatives	European	Cyber security strategy	Expert group meetings Annual Forum	http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3341&Lang=EN
13	Thematic Network on Critical Energy Infrastructure Protection (initiative of European Commission, DG Energy)	TNCEIP	All	Public Private	European Commission Transmission operators	European	Governance Strategy Return of Experience Tools Lessons learned	2-3 meetings a year	https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure
14	Incident and Threat Information Sharing EU Centre (initiative of the DG Energy, European Commission - and its operation; portal maintenance, content, user support entrusted to JRC (Joint Research Centre), European Commission	ITIS-EUC	All	Public	Public institutions Private companies	European	Situational awareness on incidents and emerging threats	Platform	https://itis.jrc.ec.europa.eu/faq
15	European Network for Cyber Security	ENCS	All	Public Private	Infrastructure Owners Regulators Research Communities Supplying Industry	Europe	Security Requirements Good practices (design, testing monitoring) Cyber security threats & vulnerabilities Governance	Meetings Conferences Round tables Webinars	https://www.encs.eu/

	ISACS. CSIRTS AND INFORMATION SHARING INITIATIVE	ACRONYM/ABBREVATION	ENERGY SUBSECTOR	PUBLIC/ PRIVATE	KEY STAKEHOLDERS	GEOGRAPHIC COVERAGE	TYPE OF CYBER SECURITY INFO EXCHANGED	FREQUENCY TYPE OF FORUM	LINK
16	European SCADA and Control Systems Information Exchange	EuroSCSIE	All	Public	Public institutions Private companies	United Kingdom	Cyber security of SCADA systems	Meetings	http://www.cpni.gov.uk/about/Who-we-work-with/Information-exchanges/
17	Austrian Trust Circle	ATC	All	Public Private	Public institutions Regulators Private companies	Austria	Cyber security information	Secure emails	https://www.cert.at/about/atc/content.html
18	ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information, the National Cybersecurity Agency of France) Groupes de travail sectoriels dédiés à la préparation des règles de sécurité prévues par l'article 22 de la loi de programmation militaire (GT LPM) (Sectorial working groups dedicated to the drafting of security rules in the context on the article 22 of the Military Programming Law)	N/A	All	Public	Public institutions Private companies	France	Security of critical infrastructures	Regular working groups (periodicity to define)	http://www.ssi.gouv.fr/actualite/cybersecurite-et-loi-de-programmation-militaire-preparation-des-regles-de-securite/
19	Norway energy companies information sharing	N/A	All	Private sector	Private companies	Norway	Cyber Security incidents	Meetings Face to face Emails	N/A
20	Organization of American States Real Time Information Sharing	OAS Real Time Information Sharing	All	Public	Public institutions Private institutions	Americas	Cyber threat intelligence Policies	Online Platform	N/A

	ISACS. CSIRTS AND INFORMATION SHARING INITIATIVE	ACRONYM/ABBREVIATION	ENERGY SUBSECTOR	PUBLIC/ PRIVATE	KEY STAKEHOLDERS	GEOGRAPHIC COVERAGE	TYPE OF CYBER SECURITY INFO EXCHANGED	FREQUENCY TYPE OF FORUM	LINK
21	Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ (Crucial Information Security Systems Facilities and Event Management Agency)	LRLIBEK	All	Private	Private companies	Hungary	Incident management Cyber security threats & vulnerabilities	Exercises Peer-teaching activities Awareness activities	http://www.katasztrofavedelem.hu/index2.php?pageid=lrl_index
22	UP Kooperation zwischen Betreibern Kritischer Infrastrukturen (Internet platform on Critical Infrastructure Protection)	UP KRITIS	All	Public Private	Public institutions Critical infrastructure providers	Germany	Security information Cyber security incidents	Working groups Exercises	http://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/upk_node.html
23	Centro Nacional de Cibersegurança (National Centre for Cybersecurity)	CNCS	All	Public Private	Public institutions Private sector	Portugal	Cyber security incidents Security alerts	Email (ad hoc) Call (ad hoc)	http://www.cncs.gov.pt/pagina-inicial/index.html
24	Energy Emergencies Executive Committee Cyber	E3CC	Electricity	Public	Public institutions Electricity generation, transmission & distribution operators	United Kingdom	Information security incidents	Regular Roundtables	https://www.gov.uk/government/organisations/department-of-energy-climate-change
25	Information gathering initiative on smart metering systems cyber-security and privacy (initiative of JRC (Joint Research Centre), Directorate E - Space, Security and Migration, European Commission) and DG Energy.		Electricity	Public	Public institutions European electricity associations	European	Smart meters technologies and functionalities	Platform	Not available

	ISACS. CSIRTS AND INFORMATION SHARING INITIATIVE	ACRONYM/ABBREVATION	ENERGY SUBSECTOR	PUBLIC/ PRIVATE	KEY STAKEHOLDERS	GEOGRAPHIC COVERAGE	TYPE OF CYBER SECURITY INFO EXCHANGED	FREQUENCY TYPE OF FORUM	LINK
26	US Department of Energy - Cybersecurity Risk Information Sharing Program	CRISP	Electricity	Public Private	Public institutions Critical infrastructure owners	United States of America	Cyber threat data & analysis Mitigation measures	Real-time security monitoring	Not available
27	ACER (Agency for the Cooperation of Energy Regulators) REMIT (Wholesale Energy Market Integrity and Transparency) Information System portal	ARIS	Electricity Gas	Public	Public institutions Private companies Regulators	European	Status and alerts on cyber security (involving project activities)	Monthly meetings and portal with restricted access	https://www.acer-remit.eu/portal/home
28	Oil and Gas Information Sharing Forum	OGISF	Oil & Gas	Public Private	UK Gov (CPNI) Private companies	UK Norway	Cyber security-related information	4 meetings a year Weekly calls	N/A
29	Statoil CSIRT	N/A	Oil & Gas	Private	Private company	International	Cyber Security incidents	Company internal sharing mechanisms	http://www.statoil.com/en/EnvironmentSociety/security/Pages/CSIRT.aspx
30	Oil and Natural Gas Information Sharing Analysis Center	ONG-ISAC	Oil & Gas	Public Private	Public institutions Private companies	United States of America	Security information	Platform	http://www.ongisac.org/
31	Downstream Natural Gas Information Sharing Analysis Center	DNG-ISAC	Gas	Public Private	Public institutions Private companies	United States of America	Security information	Platform	https://www.dngisac.com/Home/Participation
32	Civil Nuclear Sector SCADA Information Exchange	CNSSIE	Nuclear	Public Private	Public institutions Private companies	United Kingdom	Cyber threats and vulnerabilities	Meetings	http://www.cpni.gov.uk/about/Who-we-work-

	ISACS. CSIRTS AND INFORMATION SHARING INITIATIVE	ACRONYM/ABBREVATION	ENERGY SUBSECTOR	PUBLIC/ PRIVATE	KEY STAKEHOLDERS	GEOGRAPHIC COVERAGE	TYPE OF CYBER SECURITY INFO EXCHANGED	FREQUENCY TYPE OF FORUM	LINK
									with/Information-exchanges/
33	IAEA (International Atomic Energy Agency) Computer Security Information Sharing	IAEA Computer Security Information Sharing	Nuclear	Public	Members of IAEA	International	Computer security-related information	Under development	N/A
34	(Dutch) National Cyber Security Centre Nuclear ISAC	NCSC Nuclear ISAC	Nuclear	Public Private	Public institutions Private sector	The Netherlands	Cyber security incidents Red light sensitive information	Regular meetings	https://www.ncsc.nl/english/Cooperation/isacs.html
35	Nuclear Security Summit - Joint Statement on Cyber Security	N/A	Nuclear	Public	Governments	International	Cyber security of industrial control systems	2 international workshops in 2016	http://www.nss2016.org/document-center-docs/2016/4/1/joint-statement-on-cyber-security

ENISA
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vasilissis Sofias
Marousi 151 24, Athens, Greece

TP-06-16-018-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-177-9
doi: 10.2824/960067