Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches

FINAL

VERSION 1.0

PUBLIC

DECEMBER 2015

www.enisa.europa.eu European Union Agency For Network And Information Security

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

In alphabetical order:

- Deloitte Bedrijfsrevisoren / Reviseurs d'Entreprises, Belgium[1]
- Jo De Muynck, ENISA
- Dr. Silvia Portesi, ENISA

Contact

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

Acknowledgements

We would like to thank the experts interviewed for their valuable insight during the data collection phase.

We would like also to thank the ENISA National Liaison Officers (NLOs) who kindly helped us with the data validation as well as the following experts who provided precious support with their peer-review of the study:

- Andrew Cormack (Jisc)
- Hans Graux (time.lex Law Offices)
- Ray Irving (FS-ISAC)
- Dr. Jan Kolouch (CESNET, a.l.e.)
- John Morgan Salomon (FS-ISAC)

Further acknowledgement should be given to the ENISA colleagues, in particular Aidan Ryan (Legal Officer and Head of Human Resources), who contributed to the compilation of the study.

[1] The analysis and the compilation of this report was produced in collaboration with Deloitte Bedrijfsrevisoren / Reviseurs d'Entreprises BV o.v.v.e CVBA/SC s.f.d SCRL ('Deloitte Belgium'), commissioned by ENISA according to tender ref. ENISA D-COD-15-T13. Acknowledgement should be given in particular to Dan Cimpean (Partner), Georgia Skouma (Director), Alexander Cespedes Arkush (Manager), Bert Verschelde (Senior Consultant) and Caroline Zerella (Consultant).

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

978-92-9204-131-1, 10.2824/43639

Table of Contents

Executive Summary

Cyber security incidents are constantly increasing in frequency and magnitude, becoming more complex and unconstrained by borders. These incidents can cause major damage to the economy, and hence, cyber security is one of the biggest issues governments and businesses in the European Union (EU) and globally are currently facing. The borderless nature of cyber incidents and attacks, regardless of sector or area, calls for rapid, cross-border and cross-sector responses. Efforts to prevent, better cooperate in relation with, and to be more transparent about cyber incidents must still improve. In the cyber security community, there is currently a strong need for the exchange of data to support the management of vulnerabilities, threats and incidents, as well as other cyber security activities. This study aims to present the regulatory and non-regulatory approaches of EU Member States as well as EEA and EFTA countries to share information on cyber incidents, the different sector regulation challenges of managing cyber security issues, and their key practices in addressing them.

This study identifies three types of approaches to share information on cyber security incidents: 1) traditional regulation; 2) alternative forms of regulation, such as self- and co-regulation; 3) other approaches to enable information sharing, such as information and education schemes.

The proposed NIS Directive (European Commission, 2013a) and the accompanying Impact Assessment of the European Commission (European Commission, 2013b) identify six key sectors to preserve the good functioning of the internal market. These sectors are public administrations, finance and banking, energy, transport, health and Internet services. The information sharing initiatives in this report were identified and structured based on these criteria.

Despite the increasing number of national initiatives to create a legal framework to share information on cyber incidents, the co- and self-regulation approaches seem to be the most used in the EU and EEA/EFTA countries. While traditional legislation appears to tackle information sharing only partially (with the emphasis on breach notification requirements and incident reporting) and in reality not always in a consistent way all over Europe, the major challenges for alternative forms of regulation are the hesitation to share information with external parties and the lack of mechanisms to enforce the rules to share information. Another element that seems to prevent stakeholders from reaping fully the benefits of alternative forms of regulation is that the positive aspects of information sharing within such business communities are not sufficiently clear to encourage their members to participate in the information exchange process. Finally other approaches exist to inform and educate the community on certain topics with the aim to change the behaviour of the stakeholders in the information sharing on cyber incidents. However, these initiatives often take time to reach a wide community and, hence, it is rather difficult to measure their effectiveness in raising awareness and in changing market behaviour towards more transparency.

In the context of the information sharing initiatives, it is worth also mentioning the important role of national and governmental CSIRTs. In a number of countries, CSIRTs are (co-)founders of initiatives on information sharing or take an active role in bringing stakeholders together into a constructive dialogue and actions focused on cyber threats and cyber incidents.

Throughout the initiatives discussed here, it is pointed out that **trust** is a key element to enhance information exchange. At present, members of the initiatives identified do not always feel inclined to share information, for a variety of reasons. Hesitation to share and even mistrust may exist, for instance, as a consequence of a lack of interaction between members, or because passive/non-contributing members are not penalised. Another reason may be that conditions to become member of certain initiatives are

rather loose. The findings of our analysis also pinpoint cases whereby initiatives are short of members' buy-in, meaning that they find it hard to convince their members that non-participation in the initiative, and thus no information sharing, will be detrimental to the one who refuses to join. Moreover, the results of the stocktaking concur that most of the co- and self-regulatory schemes at present lack truly enforceable means in order to: a) discourage the reluctance of some participants to share information and b) penalise the members who do not respect the confidentiality rules that the initiative's stakeholders agreed to abide by.

In addition, it must be emphasised that one of the biggest weaknesses of the initiatives discussed herein is that, quite often, the conditions and modalities regarding how the information will be communicated within the members of the initiative, or towards other groups or the public, are not sufficiently defined, unclear or even not well understood. There are cases whereby widely-acknowledged practices in terms of information sharing, such as the Traffic Light Protocol (TLP) are applied within certain initiatives, but other initiatives rely on less-acknowledged practices or even ad hoc rules, such as ad hoc confidentiality agreements or membership clauses.

Finally, most of the information sharing initiatives are cross-sector, which means that organisations from different sectors are involved in the information exchange process. However, the finance and banking sector and the public administration sector seem to be the most developed in terms of information sharing as a good number of sector specific information sharing initiatives do gather together stakeholders of these sectors.

Core findings of this study are:

- The prevalence of traditional regulation, alternative forms of regulation (such as self- and co-regulation) and other approaches to enable information sharing on cyber incidents, varies from country to country;
- There is a general prevalence of alternative types of regulatory initiatives (co- and self-regulation) in the field of information sharing on cyber incidents;
- Different regulatory and non-regulatory approaches bring different challenges with them (as discussed in the following pages of this report);
- Trust is a key element for the success of the information sharing on cyber incidents;
- National and governmental CSIRTs play an important role in the field.

Core recommendations are:

1. EU and national policy makers, law makers and regulators, governmental institutions and administrative bodies (as they have an influence and control on the policy and legislative framework) and the actors of the initiatives (e.g. initiatives' founding or supporting bodies being CSIRTs or other) should **leverage existing self-regulatory and co-regulatory initiatives**;
2. European oversight and regulatory bodies competent by sector, European policy and law makers, national regulatory and oversight bodies and standard-setting bodies should **harmonise regulation rather than attempt to enact new mandatory rules**;
3. National governmental institutions and information sharing initiatives' facilitators (e.g. CSIRTs or administrative bodies supporting an initiative financially or in another way) should **further develop intra- and cross-sector information exchange with the intervention of the government or other stakeholders**;
4. National governmental institutions, information sharing facilitators with the support of CSIRTs, and any stakeholder willing to engage in a new information sharing initiative should **take advantage of the practices developed by national and governmental CSIRTs**;

5. EU and national policy makers including administrative institutions and regulatory and oversight bodies should **build upon existing work performed by EU institutions and bodies – including ENISA – and by the EU Member States whenever this is the case, in the field of information sharing on cyber security incidents**. In addition, the European Commission (e.g. DG Communications Networks, Content and Technology (DG CONNECT), DG Research and Innovation (DG RTD)) and ENISA should **find ways to boost the interactive dissemination of the knowledge and good practices**;
6. EU Member States, European Commission (e.g. DG Communications Networks, Content and Technology (DG CONNECT), DG Research and Innovation (DG RTD), DG Internal Market, Industry, Entrepreneurship and SMEs (DG GROW), DG Migration and Home Affairs (DG HOME), DG Joint Research Centre (DG JRC) and DG Energy (DG ENER)), ENISA and current and future initiators, founders and facilitators of initiatives should **encourage cross-border cooperation and build joint initiatives at EU level without excluding an international reach whenever possible**.

1 Introduction

1.1 Purpose

The purpose of this report is to take stock of the regulatory and non-regulatory approaches used to enable cyber security information sharing in the EU, EEA and EFTA countries. A particular focus is given to cross-sector information sharing about cyber incidents between different stakeholders (ENISA, 2015a).

This report presents firstly the regulatory and non-regulatory approaches to share information on cyber incidents and secondly insights into the different sector regulation challenges of managing cyber security issues as well as the practices of the countries in scope in addressing them.

1.2 Background of the Study

As of 2015, ENISA's core operational activities are aligned with the four Strategic Objectives from the ENISA strategy document and the multi-annual planning for 2015 to 2017, which are summarised in ENISA's Work Programme 2015 (ENISA, 2014). The work packages (WPKs) in ENISA's SO4 aim "to enhance cooperation both between the Member States (MS) of the EU and between related NIS communities".

Work Package 4.1 aims at supporting "EU cooperation initiatives amongst NIS–related communities" in the context of the Cybersecurity Strategy of the European Union (European Commission, 2013) (Council of the European Union, 2013) (EU CSS) through two deliverables.

- First deliverable (D1) of WPK 4.1 of the ENISA Work Programme 2015 (ENISA, 2014), whose goal is to "develop and provide guidance based on best practice for cooperation between key stakeholder communities";
- Second deliverable (D2) - this study -, the goal of which is to "identify practices of Member States in addressing different sector regulation challenges of managing cyber security issues".

It is in ENISA's and other EU communities' interest to gain knowledge in the field of information sharing. Indeed, it is a fact that "communicating incident information to others will foster future cooperation and coordination in incident prevention, prompt rapid reaction to incidents and will improve overall security with the community". Moreover, the information shared between communities "should be performed to reduce the risks of similar incidents and develop a better understanding of the risks facing the community and any related significant information infrastructure" (International Organization for Standardization (ISO), 2012a).

1.3 Study Objectives and Scope

This study aims to identify practices of EU Member States as well as EEA and EFTA countries in addressing different sector regulation challenges of managing cyber security issues.

It is important however to clarify that the word 'issues' from the ENISA's Work programme 2015 (ENISA, 2014) is replaced in this report by 'incidents' since the term 'issue' is rather a broad one and it is usually used in national, EU or international level strategies to talk about long-term 'problems', which in most cases refer to 'a cause of one or more incidents' (ITIL (IT Service Management), 2007). Besides, for the purpose of this report the term 'incident' seems more appropriate as it refers to specific events such as network failures, service interruptions and security breaches (see 'Key concepts and definitions' here below for the precise definition of incidents).

This report presents the regulatory and non-regulatory approaches of EU Member States as well as EEA and EFTA countries to sharing information on cyber security incidents, the different regulation challenges of managing those incidents within sectors and cross-sectors, and the observed current practices of the Member States in addressing them.

1.4 Policy Context

On 7 February 2013, the Commission released the Cybersecurity Strategy of the EU with the subtitle 'An Open, Safe and Secure Cyberspace' (EU CSS) (European Commission, 2013) (Council of the European Union, 2013). The strategy defines five short and long-term priorities and actions that involve EU institutions, Member States and industry:

1. Achieving cyber resilience;
2. Drastically reducing cyber crime;
3. Developing cyber defence policies and capabilities related to the Common Security and Defence Policy (CSDP);
4. Developing the industrial and technological resources for cyber security; and
5. Establishing a coherent international cyber space policy for the European Union and promote core EU values.

One aspect that can be found in almost every strategic priority is the sharing of cyber security information within and between the private sector, national entities, Member States, and EU institutions (Deloitte, 2013).

Since WPK 4.1 of the ENISA Work Programme 2015 (ENISA, 2014) aims at supporting EU cooperation initiatives amongst NIS–related communities in the context of the EU CSS, **this study takes the EU CSS as the basis for the identification of main relevant sectors where information sharing takes place** and the **main relevant areas of cyber security** in the chapters to come.

According to the EU CSS (European Commission, 2013) (Council of the European Union, 2013), cyber incidents do not stop at geographical borders in the interconnected digital economy and society. Therefore, to address cyber security in a comprehensive way, activities should span across three key pillars which also operate within different legal frameworks.

Within the EU CSS, these pillars are **Network and Information Security**, **Law Enforcement** and **Defence**, as depicted in the following figure (Figure 1).

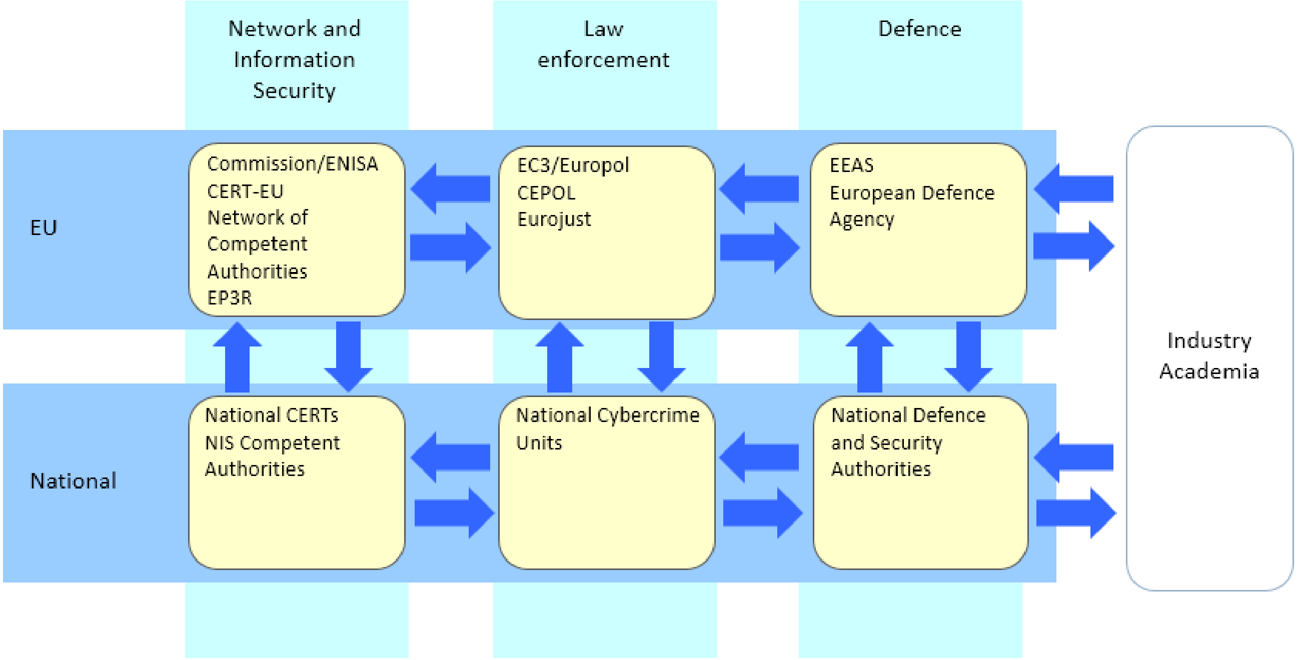

Network and Information Security
Law enforcement
Defence
EU
Commission/ENISA
CERT-EU
Network of Competent Authorities
EP3R
EC3/Europol
CEPOL
Eurojust
EEAS
European Defence Agency
National
National CERTs
NIS Competent Authorities
National Cybercrime Units
National Defence and Security Authorities
Industry
Academia

Figure 1 - Roles and responsibilities to strengthen cyber security both nationally and at EU-level- Source: (European Commission, 2013), p. 17.

These pillars correspond to the strategic priorities of the EU CSS. In addition, the European Union Agency for Network and Information Security (ENISA), the Europol/European Cybercrime Centre (EC3)[2] and the European Defence Agency (EDA)[3] are the three main EU agencies from the perspective of NIS, law enforcement and defence, respectively.

These agencies have Management Boards where the EU Member States are represented, and they offer platforms for coordination at EU level.

The table below (Table 1) represents a summary view of the relevant elements of these three pillars, their corresponding strategic priorities as deriving from the EU CSS, their corresponding lead agencies active at EU level, and their corresponding legal framework at EU level.

PILLAR OF THE EU CSS	CORRESPONDING STRATEGIC PRIORITY FROM THE EU CSS	CORRESPONDING EU LEVEL LEAD AGENCIES	LEGAL FRAMEWORK AT EU LEVEL
NIS	Achieving cyber resilience	ENISA	Digital Agenda
Law Enforcement	Drastically reducing cyber crime	Europol/EC3	Law Enforcement and Home Affairs
Defence	Developing cyber defence policy and capabilities	EDA	Foreign Affairs and Security Policy

Table 1: Overview of EU CSS pillars, priorities, lead agencies and related legal framework

[2] European Cybercrime Centre (EC3)'s: https://www.europol.europa.eu/ec3 (last access date: 30 March 2015)
[3] European Defence Agency (EDA)'s: http://www.eda.europa.eu/ (last access date: 30 March 2015)

1.5 Target Audience

The primary target audience of this report are policy and lawmakers at EU and Member State level, the CSIRT community (in particular national and governmental CSIRTs), the law enforcement community and other operational communities.

1.6 Key Concepts and Definitions

In the context of this study, the following definitions apply – see alphabetically:

- **Co-regulation** refers to "a mechanism whereby the legislator entrusts the attainment of specific policy objectives set out in legislation or other policy documents to parties which are recognised in the field (such as economic operators, social partners, non-governmental organisations, or associations)" (European Commission, 2015).
- **Cross-sector information sharing** refers to communication of information between communities established in different sectors (International Organization for Standardization (ISO), 2012a).
- **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, 2015b).
- **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" (International Organization for Standardization (ISO), 2012b).
- **Cyber security** refers to "the safeguards 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, p. 3).[4] As highlighted in some previous ENISA work (ENISA, 2014b), 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, unauthorized changes, or destruction, with the aim of guaranteeing their confidentiality, integrity, and availability."[5] In a best practice context, cyber security refers to the "[p]reservation of confidentiality, integrity, and availability of information in the Cyberspace".[6]
- **Cyber space** is a "complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form" (International Organization for Standardization (ISO), 2012b).

[4] For a definition of cyber security see also (ENISA, 2014b, p. 29).

[5] In footnote 40 of (ENISA, 2014b, p. 29) the following source is ackwnoledged: Putnik, Ž. (2013). Cyber security. In K. Penuel, M. Statler, & R. Hagen (Eds.), Encyclopedia of crisis management. (pp. 218-220). Thousand Oaks, CA: SAGE Publications, Inc.

[6] In footnote 41 of (ENISA, 2014b, p. 29) the following source is acknowledged: ISO/IEC 27032 (2012).

- **Incident** (ENISA, n.d., p. 26)[7] is an event that has been assessed as having an actual or potentially adverse effect on the security or performance of a system. Subcategories of incidents are information security (IT) incidents[8] and cyber incidents.[9] These terms are often used in an interchangeable manner.
- **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' (Robinson & Disley, 2010).
- **Information sharing initiative** means "actions taken, in the form of activities or projects which support and solve challenges facing information sharing" (Robinson & Disley, 2010).
- **Intra-sector information sharing** refers to communication of information between communities within the same sector (International Organization for Standardization (ISO), 2012a).
- **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, 2013).
- **Regulation** refers to a "rule or order prescribed for management or government; a regulating principle; a precept. [It is a] rule of order prescribed by superior or competent authority relating to action on those under its control" (InterActive Terminology for Europe, 2014).
- **Sector regulation challenges**, in our understanding, is a situation where requirements imposed by an existing sector-specific regulation impedes or precludes the sharing of cyber security threats information by actors in the affected sector.
- **Self-regulation** "typically involves a group of economic agents, such as firms in a particular industry or a professional group, voluntarily developing rules or codes of conduct that regulate or guide the behaviour, actions and standards of its members" (OECD, n.d.).
- **Traffic Light Protocol (TLP)**: the basic concept of TLP is widely understood as being a mechanism used in information sharing communities to determine the allowed distribution of information. The TLP is based on the concept of the originator labelling information with colours to indicate what dissemination is allowed by the recipient. Usually, four colours are used:
  - RED - Personal for Named Recipients Only;
  - AMBER - Limited Distribution;
  - GREEN - Community Wide; and
  - WHITE - Unlimited.

  The concept was originally developed by the UK's 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).

[7] 'n.d.' is used in the case no date could be found for the cited sources.

[8] Therefore, information security (IT) incidents are defined as "a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security" (International Organization for Standardization (ISO), 2011).

[9] Along the same lines, cyber incidents refer to a "single or a series of unwanted or unexpected information security events (see above) which occur in a "complex environment resulting from the interaction of people, software and services on the internet by means of technology devices and networks connected to it, which does not exist in any physical form" (ISO, 2012b).

2 Methodology

This chapter details the methodology applied and the choices made to collect information for this study.

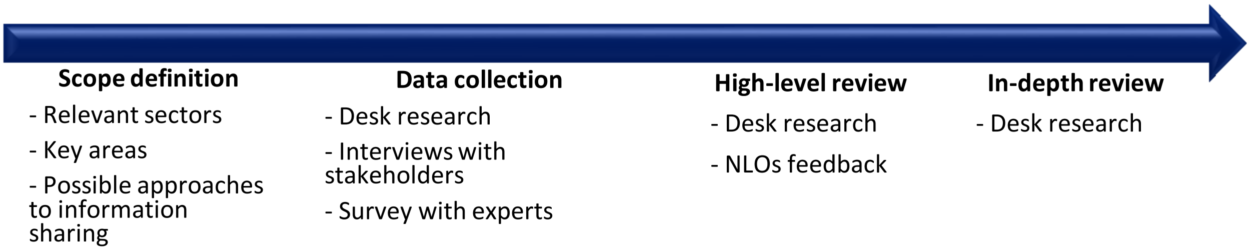
As a first step in this study, the scope and a regulatory framework were determined and refined in order to increase the focus on the information sharing elements that are most relevant from a regulatory and non-regulatory approach viewpoint. For this purpose the most relevant sectors where information sharing takes place were selected based on the proposal for an NIS Directive (European Commission, 2013a)[10], which identifies key sectors. The names of the key sectors were then formalised based on the NACE (Nomenclature des Activités Économiques dans la Communauté Européenne) structure (Eurostat, 2008). Afterwards, possible regulatory and non-regulatory approaches to share information were distinguished, such as traditional regulation, alternative forms of regulation (co- and self-regulation) and other approaches (e.g. information and education schemes).

As a second step in this study, a fact-finding exercise took place with the objective to identify pertinent information on the subject matter of this study (i.e., take stock of initiatives or regulation EU and Member States have been implementing to share information related to cyber security incidents and to address relevant challenges). This task has been carried out through: 1) an extensive desk research that included, amongst others, public information sources; 2) interviews with a selected group of stakeholders involved in information sharing initiatives; and 3) interviews with experts from the selected sectors having hands-on experience in information security and who have reflected on the subject matter of this study.

Concurrently, the collected information and research findings were validated with the support of the network of National Liaison Officers[11] (NLOs) of ENISA. During the fact-finding exercise, a number of countries were identified whereby either the first findings of the desk research, or other factors (see Chapter 2.4) justified, according to the project team, additional collection of information and/or a more in-depth review.

[10] The proposed NIS Directive (European Commission, 2013a) is now undergoing the final stage of negotiations between the EU legislative bodies; it is hoped that it will be adopted shortly (Latvian Presidency of the Council of the European Union, n.d.). As recently reported, the "EU Digital Commissioner Günther Oettinger said […] [on 9 November 2015] that an agreement on new, long-awaited cybersecurity legislation is only "days or weeks" away. European Commission, Parliament and Council officials are about to sign off on a compromise deal on the network and security information (NIS) directive, according to Oettinger. […] Luxembourg, the current holder of the 6-month rotating Council presidency, is now trying to push through an agreement in the last weeks before its term ends on 31 December." (Stupp, 2015). To follow the status of the procedure, including proposed amendment to the proposal, see: http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2013/0027(COD)#basicInformation (last access date: 14 November 2015)

[11] ENISA has set up a network of National Liaison Officers (NLOs) which serve as ENISA's important point of reference into the Member States on specific issues: https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office (last access date: 11 September 2015)



Scope definition

- Relevant sectors
- Key areas
- Possible approaches to information sharing

Data collection

- Desk research
- Interviews with stakeholders
- Survey with experts

High-level review

- Desk research
- NLOs feedback

In-depth review

- Desk research

Figure 2 - Methodological process used in this study

2.1 Desk Research

A part of the information used in this study has been collected via desktop research on publicly available information sources. These sources were, for example, official websites of initiatives/organisations, reports published by organisations or other external parties, public databases, research engine search results, various publications and relevant presentations made during CSIRT conferences or events. The desk research was used to collect the initial part of the data. Then, based on the interviews and the feedbacks received, a second desk research has been carried out to find more specific information.

For example, the result of the first desk research that was carried out is a list of relevant recent initiatives that have a strong component related to cyber security incident sharing - see the table below (Table 2).

LEVEL	COUNTRY	SECTOR	STAKEHOLDER	SUMMARY OF INITIATIVE
EU	n/a	Cross-sector	**European Advanced Cyber Defence Centre (ACDC)**[12]	This EU pilot project fosters extensive sharing of information across Member States to improve the early detection of botnets and creates an open community; a unique opportunity to share information.
EU	n/a	Cross-sector	**Europol (Joint Cybercrime Action Taskforce team)**[13]	Joint Cybercrime Action Taskforce: Opportunity for international law enforcement agencies to collectively share their knowledge to defend against cyber related attacks and cyber crime.

[12] European Advanced Cyber Defence Centre (ACDC): https://www.acdc-project.eu/ (last access date: 13 April 2015)

[13] Joint Cybercrime Action Taskforce (J-CAT): https://www.europol.europa.eu/content/expert-international-cybercrime-taskforce-launched-tackle-online-crime (last access date: 13 April 2015)

LEVEL	COUNTRY	SECTOR	STAKEHOLDER	SUMMARY OF INITIATIVE
EU	n/a	Cross-sector (CSIRTs)	**Connecting Europe Facility Cyber Security Digital Service Infrastructure (CEF Cyber Security DSI)**[14]	The CEF Cyber Security DSI is defined in the CEF Annual Work Programme (WP) 2014 and 2015. The preparatory actions foreseen in the CEF WP 2014 (European Commission, 2014b) are aimed at preparing the DSI as a mature DSI for the CEF WP 2015 (European Commission, 2014a) to establish and launch a core cooperation platform and mechanisms that will enhance the EU capability for preparedness, cooperation and information exchange, coordination and response to cyber threats. Such mechanisms will be used by EU Member States on a voluntary basis, to strengthen capacity building and cooperation, in line with established governance structure and requirements (European Commission, 2014c).
EU	n/a	Intra-sector (Energy)	**Thematic Network on Critical Energy Infrastructure Protection (TNCEIP)** [15]	An initiative of the European Commission, and is made up of European owners and operators of energy infrastructure in the electricity, gas and oil sectors.
EU	n/a	Intra-sector (Finance and banking)	**European Financial Institutes – Information Sharing and Analysis Centre (European FI-ISAC)**[16]	Country representatives from the financial sector, national CSIRT's and Law Enforcement Agencies (LEA's) meet to exchange information related to cyber threats, incidents and vulnerabilities. Members meet twice a year, share relevant information via the EU FI-ISAC list server and via direct individual communication.
EU	n/a	Intra-sector (Internet services)	**ENISA Electronic Communications Reference Group (ECRG)**[17]	Includes European providers of public electronic communications networks and services (mobile and fixed telecom operators, VoIP providers, ISPs, IXP providers etc.). This group is composed by CISOs of the main operators and it addresses security topics across the electronic communications area - including security measures, incident reporting, data protection, botnet mitigation, interconnection security and other topics.

[14] Connecting Europe Facilitiy: http://ec.europa.eu/digital-agenda/en/connecting-europe-facility#digital-service-infrastructures-dsis (last access date: 25 June 2015)
[15] Thematic Network on Critical Energy Infrastructure Protection (TNCEIP): http://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure (last access date: 30 April 2015)
[16] European FI-ISAC: https://www.enisa.europa.eu/activities/cert/support/information-sharing/european-fi-isac-a-public-private-partnership (last access date: 29 May 2015)
[17] Electronic Communications Reference Group (ECRG) https://resilience.enisa.europa.eu/ecrg (last access date: 10 June 2015)

LEVEL	COUNTRY	SECTOR	STAKEHOLDER	SUMMARY OF INITIATIVE
MS	Netherlands	Cross-sector	***Nationaal Cyber Security Centrum* (NCSC)**[18]	NCSC is the facilitator of several ISACs, which are set up per sector (e.g. Water, Telecom, Nuclear etc.). Each ISAC is composed of sector-related members and has a chair. NCSC encourages meetings between ISACs' chairs for cross-sector information sharing.[19]
MS	Germany	Cross-sector	***Kooperation zwischen Betreibern Kritischer Infrastrukturen* (UP KRITIS)**[20]	A joint initiative of the Federal Office of Civil Protection and Disaster Assistance (BBK) and the Federal Office for Information Security (BSI).
MS	Finland	Cross-sector	**FICORA**[21]	FICORA is the Finnish communications regulatory activity authority. One of its core function is to disseminate information about cyber security. This function has been determined by the Finnish government and is enshrined in local legislation (Section 304 of Information Society Code).
MS	Czech Republic	Cross-sector	**CZ NSA**[22]	CZ NSA is the national authority for cyber security in the Czech Republic which consists of the National Cyber Security Centre (NCSC). The main task of NCSC is to coordinate cooperation on both national and international level to prevent cyber attacks, as well as to propose and adopt measures for incident solving and against ongoing attacks.[23]
MS	Belgium	Cross-sector	**Cyber Threat Intelligence Research Project (CTISRP)**[24]	Initiative launched by Deloitte Belgium in 2013 for public and private organisations from across Europe to discuss sharing of cyber threat information. Members come from 13 different sectors and meet several times a year.

[18] *Nationaal Cyber Security Centrum* (NCSC): https://www.ncsc.nl/english (last access date: 4 September 2015)

[19] Information Sharing and Analysis Centres (ISACs): https://www.ncsc.nl/organisatie/publiek-private-samenwerking/isacs.html (last access date: 4 September 2015)

[20] *Kooperation zwischen Betreibern Kritischer Infrastrukturen* (UP KRITIS): http://www.kritis.bund.de/SubSites/Kritis/EN/publications/Fortschreibungsdokument_engl..html (last access date: 10 June 2015)

[21] FICORA: https://www.viestintavirasto.fi/en/cybersecurity/ficorasinformationsecurityservices/cert-fi/rfc2350.html (last access date: 10 June 2015)

[22] CZ NSA: http://www.nbu.cz/en/ (last access date: 15 May 2015)

[23] Ibidem.

[24] Cyber Threat Intelligence Research Project (CTISRP): http://www.politiestudies.be/userfiles/20141202%20BISC%20Luc%20Beirens%20voor%20verspreiding.pdf (last access date: 15 May 2015)

LEVEL	COUNTRY	SECTOR	STAKEHOLDER	SUMMARY OF INITIATIVE
Global	n/a	Cross-sector (CSIRTs)	**FIRST**[25]	FIRST brings together a variety of worldwide security and incident response teams from the government, commercial, and academic sectors. FIRST is an organisation that brings together several collaborative and cooperative approaches of the disciplines involved in computer and network security incident response.
Global	n/a	Cross-sector	**Meridian Conference**[26]	Conference held once a year in different locations since 2005. Officials of critical infrastructure meet and share information on cyber incidents during the conference and via a platform by using the Traffic Light Protocol rules.
Global	n/a	Intra-sector (Finance and banking)	**Financial Services Information Sharing and Analysis Center (FS-ISAC)**[27]	"FS-ISAC, or the Financial Services Information Sharing and Analysis Center, is the global financial industry's go to resource for cyber and physical threat intelligence analysis and sharing. FS-ISAC is unique in that it was created by and for members and operates as a member-owned non-profit entity" (FS-ISAC, n.d.).

Table 2: Non-exhaustive list of relevant recent initiatives that have a strong component related to cyber security incident sharing

Table 2 above does not represent an exhaustive list of information sharing initiatives in EU Member States, EEA and EFTA countries, or at global/international level. This table has been extended and refined during the fact-finding exercise and has been used as working tool for the review of the information by the National Liaison Officers (NLOs) of ENISA.

[25] FIRST: https://www.first.org/ (last access date: 25 June 2015)

[26] Meridian Conference: http://www.meridianprocess.org/ (last access date: 15 May 2015)

[27] Financial Services Information Sharing and Analysis Center (FS-ISAC): https://www.fsisac.com/ (last access date: 29 May 2015)

2.2 Interviews with a Selected Group of Stakeholders Involved in Information Sharing Initiatives

Interviews were performed with key stakeholders involved in information sharing initiatives (i.e. mainly EU-wide or EU-focused projects aimed at further facilitating information sharing activities between stakeholders, global initiatives or partnerships at Member State level).

The objective of these interviews was to collect first-hand information on the regulatory and non-regulatory approaches used in five EU Member States, five EU projects and by three global/international organisations – approached to share information and to manage challenges related to cyber security issues. The involved stakeholders were jointly identified by the study team via desktop research and via inquiry with ENISA and industry experts. Key criteria in selection of these stakeholders were the level of engagement in an information sharing initiative, the level of maturity of the initiative in which they are active and the experience or the level of knowledge on the information sharing topic.

Regarding the methodological approach followed for the interviews held with the involved stakeholders, it is relevant to mention that the approach chosen by the study team was to use a questionnaire, structured as follows:

- Part 1: General questions about the initiatives and the sectors involved in the sharing of information.
- Part 2: Questions on the approaches to share information, considering the following three types:
  - ✓ Traditional regulation;
  - ✓ Other forms of regulation;
  - ✓ Other alternatives to share information.
- Part 3: Questions on the challenges to share information and the approaches to address them.

A sample questionnaire, used for the interviews with a selected group of stakeholders involved in information sharing initiatives, can be found in Annex 2.

2.3 High Level Review of Regulatory and Non-regulatory Approaches

A high-level review of regulatory and non-regulatory approaches used in the EU and EEA Members States and at global level to share information on cyber incidents was performed by the study team via an extensive desk research. More than eighty (80) initiatives and organisations and more than fifty (50) national and governmental CSIRTs involved in information exchange on cyber incidents were identified at EU and EEA level.

The collected information was validated with the support of the network of National Liaison Officers (NLOs) of ENISA. More specifically, these Member State representatives gave feedback on the completeness of the initiatives and relevant organisations (including national and governmental CSIRTs) listed as well as on the correctness and relevance of the information associated to their Member State. More information on this list of identified initiatives and relevant organisations as well as on the manner to access it can be requested by contacting cert-relations@enisa.europa.eu.

Furthermore, various industry experts were contacted through a high-level survey, with the objective of receiving additional input on information sharing initiatives coming from industry and cyber security experts.

2.4 In-Depth Review of Regulatory and Non-regulatory Approaches Used in Some Selected Countries

An in-depth review was performed via desktop research to identify regulatory and non-regulatory approaches used in selected EU Members States to share information on cyber incidents and practices to address sector regulatory challenges of managing cyber security issues.

This in-depth review focused on a selection of eight EU Member States – the selection was based on the following criteria:

- The **size** of the Member State and the specifics of the national regulatory system concerning cyber security;
- The **geographical location** of the country (fair geographical representation across Europe);
- The **type of legal system** in force: common or civil law;
- The **level of government centralisation**: federal or centralised;
- The **relative strength of the cyber legal framework** of the Member State considered (taken the EU level as the average one setting the minimum requirements);
- The **level of maturity** of the national cyber security policy of the country, notably the appointment of national and governmental CSIRTs;
- The **active role of the sector regulators or the business community** concerned with information sharing, notably whether self- or co-regulatory efforts have been undertaken; and
- **Actions and specific initiatives** a Member State has taken in relation to information sharing at sector or cross-sector levels.

Based on these criteria, the following EU Member States were selected for the in-depth review – see below in alphabetical order:

- **Cyprus**, a Southern European Member State with a common law tradition;
- **Estonia**, a Baltic Member State with active government involvement in regulating cyber security (established national and governmental CSIRT) and exposure to nationwide cyber attacks (2007);
- **Finland**, for its active and centralised government involvement in information sharing and geographical location (Northern EU Member State);
- **Germany**, as it is a large, decentralised (federal) Member State with a strict cyber legal framework;
- **The Netherlands**, as it has many co-regulatory information sharing initiatives, including at sectoral level;
- **Poland**, as it is a large Eastern European Member State with a strict cyber legal framework (e.g. information security officer requirement);
- **Spain**, as it is a large Southern European Member State with many examples of self-regulatory initiatives for sharing cyber threat information; and
- **United Kingdom**, a common law Member State with many information sharing initiatives in place.

As a result, chapters three, four and five of this document present the sectors selected for the study (Chapter 3), the areas of cyber security (Chapter 4) and the identified possible regulatory and non-regulatory approaches to share information on cyber incidents (Chapter 5).

Chapter 6 summarises the main findings of the study. Finally, the last chapter (Chapter 7) presents preliminary conclusions and recommendations.

3 Sectors Where Information Sharing Initiatives on Cyber Security Incidents Take Place

This chapter presents the main relevant sectors where information sharing about cyber incidents takes place among the different stakeholders.

3.1 Selection of Relevant Sectors Based on the Relevant Policy Context

One of the main actions of the EU is the proposed NIS Directive (European Commission, 2013a). This proposal is accompanied by an impact assessment (hereafter 'the Impact Assessment') (European Commission, 2013b) that covers policy options to improve the security of the Internet and other networks and information systems underpinning services which support the functioning of our society. It identifies six (6) sectors (according to the NACE rev.2 classification (Eurostat, 2008)) for which the correct functioning of NIS is key in order to preserve the correct functioning of the internal market. These identified sectors are the following: **public administrations**, **finance and banking**, **energy**, **transport**, **health** and **Internet services** enabling key economic and societal processes, such as e-commerce platforms and social networks.

The infrastructure and service providers in these sectors are particularly vulnerable to cyber attacks and to other categories of cyber incidents, in particular due to their "**high dependence on correctly functioning network and information systems**" and "their **essential role in providing key support services for our economy and society**, including health, safety, security and the economic and social wellbeing of people".

In summary, the Table 3 below identifies the sectors identified in the Impact Assessment where "the well-functioning of NIS is key to preserve the well-functioning of the internal market".

SECTOR	RATIONALE FOR INCLUSION IN SCOPE OF THIS STUDY BASED ON THE IMPACT ASSESSMENT
Energy	Generation, transmission and distribution of energy are highly dependent on secure network and information systems. Major gas and electricity companies for example, suffer increased amounts of cyber attacks motivated by commercial and criminal intent.
Transportation	Key transport infrastructure such as airports, ports, railways, traffic management systems and logistics suffer increased amounts of cyber attacks motivated by commercial and criminal intent.
Health	Hospitals and clinics are becoming more reliant on sophisticated ICT systems which need to be secure in order to ensure continuity of service and avoid fatal disruptions.
Finance and banking	Banks are the backbone of our financial system. They are common targets of fraudsters. The stock exchange, insurance, retail and investment banking for example, are increasingly adopting networks and information systems and Internet based commerce systems.
Internet services	It is important to ensure the security of Internet companies which provide key inputs enabling important economic and societal processes. This is essential to preserve trust in the digital ecosystem.
Public administration	E-Government and e-participation are increasing with citizen demand for timely and cost-effective services and so are the NIS risks for state and local administrations. The risk for public online services to be hindered by NIS problems exist at all levels.

Table 3: Rationale to select sectors in scope for this study

However, it is important to note that the Impact Assessment does not cover EU Member States' activities concerning national security and defence.

In addition, according to Article 1 of the ENISA's Regulation, "the objectives and the tasks of the Agency shall be without prejudice to the competences of the Member States regarding network and information security and in any case to activities concerning public security, defence, national security" (European Parliament and the Council, 2013). Therefore, national security and defence matters were specifically considered as not within the scope of this study.

Through the research work performed by the study team, we found a number of relevant information sharing initiatives in other sectors such as the water, pharmaceutical or nuclear sectors that are worth analysing and worth mentioning due to their specific elements that may be relevant for the cyber security domain.

For example, we observed that the UK CPNI organises the Water Security Information Exchange (WSIE) and the Pharmaceutical Industries Information Exchange (PIIE) exchange information on cyber attacks between actors in the these sectors in the UK.[28]

Similarly, the National Cyber Security Center (Nationaal Cyber Security Centrum (NCSC)) in the Netherlands has put in place the Water ISAC and the Nuclear ISAC which are also an important building block of the information sharing initiative(s) in these Dutch sectors.[29] Therefore, wherever relevant, references have been made in the study, concerning initiatives and practices in the various sectors, in addition to those stemming from the Impact Assessment.

3.2 Identification of Information Sharing Initiatives per Sector

The purpose of this chapter is to provide examples of information sharing initiatives within and across the sectors identified in the chapter above. This is accomplished by listing a number of existing initiatives currently involved in exchanging information about cyber incidents in those sectors at EU and MS level. For this purpose, the following definition of an information sharing initiative is used: "Information sharing initiatives are actions taken, in the form of activities or projects which support and solve challenges facing information sharing" (Robinson & Disley, 2010).

In order to illustrate examples of information sharing initiatives, two lists have been created.

The first one (Table 4) lists intra-sector information sharing initiatives, while the second one (Table 5) shows examples of cross-sector information sharing initiatives at Member State or EU level. These examples have been identified via the performed desk research, and they should be considered as a representative, but non-exhaustive, list of such initiatives.

Please note that the initiatives identified in Tables 4 and 5 are primarily used here to highlight the sectors concerned (energy, transport, etc.). Further explanations on a number of initiatives mapped to these sectors are discussed in more detail in Chapter 6 of this report.

Table 4 lists a number of examples of **intra-sector** information sharing initiatives occurring in the sectors in scope and in several Members States.

[28] Centre for the Protection of National Infrastructure – Information exchanges: http://www.cpni.gov.uk/about/Who-we-work-with/Information-exchanges/ (last access date: 4 September 2015)
[29] Information Sharing and Analysis Centres (ISACs): https://www.ncsc.nl/english/Cooperation/isacs.html (last access date: 4 September 2015)

SECTORS	NATIONAL OR EU LEVEL	MEMBER STATE	EXAMPLE OF INTRA-SECTOR INFORMATION SHARING INITIATIVES
Energy	EU	n/a	**Distributed Energy Security Knowledge (DENSEK)[30]**: European project for the creation of a Situation Awareness Network to share information on cyber attacks.
Transportation	National	United Kingdom	**Transport Sector Information Exchange (TSIE)[31]**: Information Exchanges on cyber attacks within the transport sector.
Health	National	Netherlands	**Zorg ISAC[32]**: Information sharing initiative in the healthcare sector backed by the Dutch organisation Nationaal Cyber Security Centrum (NCSC).
Finance and banking	EU	n/a	**European Financial Institutes – Information Sharing and Analysis Centre (European FI-ISAC)[33]**: information exchange on cyber incidents (among others).
	National	United Kingdom	**Financial Services Information Exchange (FSIE)[34]**: Information Exchanges on cyber attacks between actors of the financial sector.
Internet services	National	United Kingdom	**UK Network Security Information Exchange (UK-NSIE)[35]**: Information Exchanges on cyber attacks and sensitive information between actors of the information and communications technologies sector.
	National	United Kingdom	**The Telecommunications Industry Security Advisory Council (TISAC):** awareness raising on cyber attacks in the UK telecom sector.
Public administration	National	Belgium	Belgian Network and Information Security (BELNIS): Established in 2005, it acts as a coordinating workgroup that includes representatives from government agencies engaged with cyber security. It provides advice to the government on cyber security incidents and cyber security.

Table 4: Non-exhaustive list of intra-sector information sharing initiatives on cyber incidents

Furthermore, Table 5 below lists examples of **cross-sector** information sharing initiatives.

NATIONAL OR EU LEVEL	MEMBER STATE	EXAMPLE ON CROSS-SECTOR INFORMATION SHARING INITIATIVES
30 D**EU**	n/a	**Network and Information Security Platform[36]**: platform where stakeholder communities a members and organisations across multiple sectors can share information on cyber incidents.
EU	n/a	**European Advanced Cyber Defence Centre (ACDC)[37]:** This EU pilot project fosters extensive sharing of information across Member States to improve the early detection of botnets and creates an open community, a unique opportunity to share information.
i b u**National** t	Austria	**The Austrian Trust Circle (ATC)[38]:** Founded in 2010 is an initiative of CERT.at and the Federal Chancellery. The primary goal is to build confidence between the responsible people and organisations in different sectors of strategic infrastructure to facilitate the exchange of security - related experience and ensure that swift and joint action will be taken in concrete cases.
National	Belgium	**Cyber Security Coalition[39]**: coalition for cross-sector knowledge exchange of cyber incidents, among others activities. Sectors such as the telecommunication, finance and banking, public administration and education are part of this initiative.

National	Belgium	**Cyber Threat Intelligence Sharing Research Project (CTISRP)**[40]: In December 2012, Deloitte Belgium took the initiative to invite a number of major public and private organisations from across Europe to discuss sharing of cyber threat information between these organisations. The goal is to understand better the benefit of exchanging information on cyber security incidents across countries, sectors (e.g. finance, public, telecom and energy sectors), and industries.
National	Germany	***Kooperation zwischen Betreibern Kritischer Infrastrukturen* (UP KRITIS)[41]:** A joint initiative of the Federal Office of Civil Protection and Disaster Assistance (BBK) and the Federal Office for Information Security (BSI).
National	Hungary	**Conference on Information Security and Cyber Defence (ISCD)[42]:** Conference held once a year in Budapest, organised by the National Security Authority of Hungary and started in 2011. This conference aims to exchange information related to security and cyber defence, cyber challenges, cyber threats, etc.
National	Spain	**Foro ABUSES[43]:** The objective of this initiative is to create a trusted environment among operations personnel for information sharing, experiences and coordination on/in security issues on Internet (spam, viruses, trojans, phishing, etc.). It is especially active in the telecommunication sector.

Table 5: Non-exhaustive list of cross-sector information sharing initiatives on cyber incidents

ergy Security Knowledge: http://www.densek.eu/ (last access date: 15 May 2015)

[31] Centre for the Protection of National Infrastructure – Information exchanges: http://www.cpni.gov.uk/about/Who-we-work-with/Information-exchanges/ (last access date: 4 September 2015)

[32] Information Sharing and Analysis Centres (ISACs): https://www.ncsc.nl/english/Cooperation/isacs.html (last access date: 4 September 2015)

[33] European FI-ISAC: https://www.enisa.europa.eu/activities/cert/support/information-sharing/european-fi-isac-a-public-private-partnership (last access date: 29 May 2015)

[34] Centre for the Protection of National Infrastructure – Information exchanges: http://www.cpni.gov.uk/about/Who-we-work-with/Information-exchanges/ (last access date: 4 September 2015)

[35] *Ibidem.*

[36] NIS Public-Private Platform: https://resilience.enisa.europa.eu/nis-platform (last access date: 15 May 2015)

[37] ACDC: http://acdc-project.eu (last access date: 15 May 2015)

[38] The Austrian Trust Circle (ATC): http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=56982 (last access date: 7 July 2015)

[39] Cyber Security Coalition: https://www.cert.be/docs/press-release-cyber-security-coalition (last access: 7 July 2015)

[40] Cyber Threat Intelligence Research Project (CTISRP): http://www.politiestudies.be/userfiles/20141202%20BISC%20Luc%20Beirens%20voor%20verspreiding.pdf (last access date: 15 May 2015)

[41] *Kooperation zwischen Betreibern Kritischer Infrastrukturen* (UP KRITIS): http://www.kritis.bund.de/SubSites/Kritis/EN/Home/home_node.html;jsessionid=3D1238A4F91961A3082D7BBD88E60C61.1_cid320 (last access date: 10 June 2015)

[42] Conference on Information Security and Cyber Defence (ISCD): http://www.nbf.hu/whitepaper.html (last access date: 7 July 2015)

[43] Foro ABUSES: http://www.abuses.es/ (last access date: 7 July 2015)

4 Areas of Cyber Security Relevant for the Identified Sectors

This chapter aims to present the main areas of cyber security that are relevant for the selected sectors. For this purpose, and for the clarity of the readers, the two key concepts of 'cyber space' and 'cyber security' have been used. The definitions can be found in Chapter 1.6 'Key Concepts and Definitions'. According to the EU CSS, major cyber incidents are likely to have an impact on EU governments, business and individuals. However, the response mechanisms will differ depending on the nature, magnitude and cross-border implications of the incident. A number of categories of major incidents are defined in the EU CSS in the context of EU support in case of a major cyber incident or attack. These are visible in the left column of the table below (Table 6). Some cyber security areas can relate to multiple categories of cyber incidents.

CATEGORIES OF CYBER INCIDENTS	AREAS OF CYBER SECURITY
Incidents having a serious impact on business continuity of **networks and services**.	✓ Critical Infrastructure Protection (CIP)
	✓ Critical Information Infrastructure Protection (CIIP)
Incidents relating to a **crime** that would require the preservation of evidence, identification of the perpetrators and ultimately assurance that they are prosecuted.	✓ Cyber crime
	✓ Cyber safety
Incidents compromising **personal data**.	✓ Privacy breaches
	✓ Cyber crime (identity theft, fraud, ransomware…)
	✓ Cyber safety

Table 6: Areas of cyber-security related to cyber incidents (European Commission, 2013) (Council of the European Union, 2013)

Furthermore, cross-sector information sharing communities are usually established based on some common interest, such as the nature of the shared information. For this reason, we have identified relevant areas of cyber security that apply per category of cyber incidents - visible in the right column of the table. Critical Infrastructure Protection is considered as an area of cyber security because the protection of infrastructure can also be achieved via the information sharing on cyber incidents. For example, it seems that the members of the Thematic Network Critical Energy Infrastructure Protection (TNCEIP) initiative[44] share information on relevant cyber issues that are related to the operational security of their physical assets. Moreover, incidents relating to a crime and incidents involving personal data are both related to cyber safety. Indeed safety and security are required in cyber space and these can be achieved by sharing these two types of incidents. It is also important to note that cyber security builds upon information security, application security, network security, and Internet security, all of these being considered its fundamental building blocks (International Organization for Standardization (ISO), 2012b). However, cyber security is not strictly speaking synonymous with Internet security, network security, application security or information security. Therefore, for the purpose of this study, these are not considered areas of cyber security. Moreover, other criteria could have been chosen to identify areas of cyber security. Nevertheless, the approach derived from the EU CSS seems to be the most suitable

[44] TNCEIP: http://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure (last access date: 15 June 2015)

approach to follow for the purpose of this study because in the context of the EU CSS, ENISA is tasked to support Strategic priority 1 - Achieving cyber resilience (see Chapter 1.4 Policy Context). In addition,

anther reason to justify the use of the EU CSS in determing the criteria is the fact that the EU CSS is aligned with other EU policy intiatives, and is also a reference for other national and European policy intitiatives.

5 Possible Regulatory and Non-regulatory Approaches to Sharing Information on Cyber Incidents

This chapter addresses possible regulatory and non-regulatory approaches that EU Member States and EEA and EFTA countries may adopt to regulate information sharing about cyber incidents. Taking stock of international studies and initiatives, including an OECD report (OECD, n.d.), we distinguish between three main clusters:

1) Traditional regulation
2) Alternative forms of regulation, such as self-regulation and co-regulation, and
3) Other approaches to enable information sharing, such as information and education schemes.

Each approach is illustrated in this study by examples at EU, national or international level. However, these examples constitute here a representative, but non-exhaustive, list of initiatives or approaches that were identified during the project analysis.

In particular, it is not always easy to make a clear distinction between the co-regulatory trend, self-regulation and other approaches to enable information exchange. The main reason for this is that, in general, there are no widely-accepted and formal criteria to distinguish between them. In addition, the concepts of co-regulation and self-regulation are constantly evolving in practice, under the influence of market practices and the regulatory culture of each region or country. Therefore, the difference between co-regulation and self-regulation seems quite small as these approaches often comprise a regulatory basis.

5.1 Traditional Regulation

A response of governments to a policy issue is often to regulate by setting legally binding rules that all citizens or companies, or indeed a subset thereof, need to comply with. A general definition of 'regulation' is "A rule or order prescribed for management or government; a regulating principle; a precept. [It is a] rule of order prescribed by superior or competent authority relating to action on those under its control" (InterActive Terminology for Europe, 2014). 'Command-and-control'[45] is one of the most well-known examples of traditional regulation approaches (Baldwin, Cave, & Lodge, 2012). Traditional regulation is commonly referred to in the EU as 'hard law' (European Commission, 2015), implying the adoption of coercive rules by an authority, which has the competence and power to enforce compliance.

Traditional regulation might not be the most effective or cost-efficient solution to policy issues (European Commission, n.d.) (OECD, n.d.). The OECD (OECD, 2012), the EU, and US regulators such as the Federal Trade Commission (FTC) (Federal Trade Commission, 1998) therefore advocate wherever possible the use of alternative forms of regulation, which is referred to in the EU's recently published Better Regulation package as 'soft' regulation (European Commission, 2015).

In the EU, the proportionality (Bradley, 2011) and subsidiarity (Eur-Lex, 2010) principles[46] govern the choice of instrument, leaving traditional regulation as the preferred option only in case this is proportionate to the policy goal and this goal cannot be achieved at a lower level of government (e.g.

[45] 'The essence of command and control (C & C) regulation is the exercise of influence by imposing standards backed by criminal sanctions. The force of law is used to prohibit certain forms of conduct, to demand some positive actions, or to lay down conditions for entry into a sector' (Baldwin, Cave, & Lodge, 2012).
[46] On the topic of principles regulating information security see (Mitrakas & Portesi, 2007)

Member State, regional, municipal level) or through alternative forms of regulation. In reality, this has led to a proliferation of alternative soft forms of regulation. In Chapter 6.1 we list the main forms these approaches can take - by no means an exhaustive list or strict typology.

5.2 Alternative Forms of Regulation

5.2.1 Co-regulation

Co-regulation is “a mechanism whereby the legislator entrusts the attainment of specific policy objectives set out in legislation or other policy documents to parties which are recognised in the field (such as economic operators, social partners, non-governmental organisations, or associations)” [underlining added] (European Commission, 2015). As such, the degree of legislative backing and involvement of government is the main element that differentiates co-regulation from self-regulation (OECD, n.d.).

A representative example of co-regulation can be found in standardisation within the Information and Communication Technologies sector (ICT) which stemmed from the EU Regulation 1025/2012 on European Standardisation (European Parliament and the Council, 2012b). This sets the legal framework in which the different actors in the standardisation system can operate. These actors are the European Commission, the European standardisation organisations (CEN/CENELEC, ETSI), industry, small and medium-sized enterprises (SMEs) and societal stakeholders.

EU Regulation 1025/2012 aims at setting up an effective and efficient standardisation system within the EU “which provides a flexible and transparent platform for consensus building between all participants and which is financially viable” (European Parliament and the Council, 2012b). Given that standards can have a broad impact on society, in particular on the safety and wellbeing of citizens, the efficiency of networks, the environment, workers’ safety and working conditions, accessibility and other public policy fields, the EU legislator deemed it “necessary to ensure that the role and the input of societal stakeholders in the development of standards are strengthened, through the reinforced support of organisations representing consumers and environmental and social interests” (European Parliament and the Council, 2012b).

5.2.2 Self-regulation

Self-regulation “typically involves a group of economic agents, such as firms in a particular industry or a professional group, voluntarily developing rules or codes of conduct that regulate or guide the behaviour, actions and standards of its members” [underlining added] (OECD, n.d.). In self-regulation, this group is also responsible for enforcement and compliance amongst its members.

There are different forms of self-regulation, but it usually takes the form of market-driven initiatives. A non-governmental organisation, a representative body or a professional association may take such an initiative, without specific regulation having foreseen the creation of such a group. It may take the shape of codes of conduct, or ethical codes or industry protocols. The main challenge for self-regulation is ensuring that the desired policy outcome is achieved. The lack of a legal basis means that conventional enforcement mechanisms associated with regulation are not available to enforce compliance.

Thus, in all self-regulatory initiatives which lead to the adoption of certain rules, such as the ones described in the next chapter, the adoption of such rules by the market stakeholders remains voluntary. When the market stakeholders are members of the self-regulatory group/forum/community having produced the said rules, then, in principle, members are committed to abide by the rules. However, the enforcement power (or the power to ban) of the self-regulatory instruments upon their members is generally low (e.g. relevant sanctions in terms of non-compliance or in case a member breaks the rules are either not specified or generally weak).

5.3 Other Approaches (Information and Education)

This cluster covers approaches embedding educational and awareness-raising elements aiming to enhance the knowledge of a stakeholder community on a specific subject matter and, hence, to improve coordination of actions and information sharing. Information and education instruments "work to change behaviour through the provision of greater information or by changing the distribution of information; that is, making information that may be available to some businesses and consumers available to others" (OECD, n.d.). It is worth mentioning that in the field of this study, stakeholders targeted by this kind of approach are organisations, cyber security experts, ISPs, CSIRTs, companies but also any group of citizens willing to share information on cyber incidents.

There are cases where information sharing under this stream remains informal and voluntary although it is organised in a quite practical and interactive manner. Interesting examples in this area are cooperative work and stakeholders' initiatives that are taking shape under the guidance and training support of ENISA.[47] Cyber crisis cooperation[48], relevant training exercises and incident simulations that stakeholders undertake with the objective to test and foster the resilience of communications networks, including against IT/cyber threats, fall therefore under this stream of 'other approaches' (see also Chapter 6.3 for relevant examples).

Last but not least, we may integrate in this cluster bilateral discussions on cyber security and information exchanges that take often place between two stakeholders or within the members of informal stakeholder groups. These bilateral or multilateral exchanges of information happen on a completely informal basis with no external communication (e.g. no formal website exist presenting the initiative) and the information sharing is based on mutual trust between the participants and without any expectation of taking up any formal action unless in cases where activities have been agreed upon based on a 'closed user group' contract or under 'gentlemen's agreement'. Although it is difficult to formally measure the effectiveness of such informal, 'closed user group' approaches in the study, we deem it worth to mention them here, in the cluster of 'other approaches', for the sake of completion of this report.

[47] For more information on ENISA work in the field of training, see https://www.enisa.europa.eu/activities/cert/training

[48] For more information on ENISA's work in the field of Cyber Crisis Cooperation and Exercises, see https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation

5.4 From Regulatory to Non-regulatory Approaches: a Summarising Table

Table 7 below illustrates the main possible approaches to regulate or promote information sharing about cyber incidents, and shows the range of possibilities that exists between regulatory and non-regulatory approaches (see arrow at the end of the table). As stated before, due to the difficulty to draw a clear line between co- and self-regulation, certain initiatives may be considered to be qualified as both self- and co-regulatory. Some examples of initiatives mentioned in the Table 7 are described in more detail in Chapter 6.

TRADITIONAL REGULATION	ALTERNATIVE FORMS OF REGULATION	OTHER APPROACHES
Command-and-control legislation, legally binding rules: coercive rules are implemented and organisations need to comply with these legally binding rules. • e.g. Electronic identification and trust services (eIDAS) Regulation • e.g. Telecom laws in Belgium, Lithuania, Spain • e.g. Electronic Communication Act in Slovenia • e.g. Information Society Code in Finland • e.g. Security measures acts in Estonia, Germany	**Co-regulation:** the regulatory body gives power and entrusts market stakeholders to achieve a policy objective**.** • e.g. Information Sharing and Analysis Centres (ISACs) in the Netherlands • e.g. Information Exchanges (IEs) in the United Kingdom • e.g. UP KRITIS in Germany • e.g. Austrian Trust Circle (ATC in Austria • e.g. Threat indicators sharing platform for private sector (MISP) in Luxembourg • e.g. Forum for information sharing (FIDI) in Sweden	**Information and education:** enhance the knowledge of the community on a certain topic to change its behaviour. • e.g. workgroups held by Czech CSIRT in Czech Republic • e.g. Belgian Network and Information Security (BELNIS) in Belgium • e.g. (ISC)² Ireland Chapter in Ireland • e.g. Cyber Security Research Center from Romania (CCSIR) in Romania
	Self-regulation: market stakeholders agree and create on a voluntary basis rules to regulate their actions. • e.g. Industrial Cybersecurity Centre (CCI) in Spain • e.g. n6 Network Security Incident Exchange and ABUSE Forum in Poland • *Club des directeurs de sécurité des entreprises* in France • *Associazione italiana esperti in infrastructure critiche* (AIIC) in Italy • e.g. Bulgarian Association of Information Technologies (BAIT) e.g. Information Technology and Information Systems Security Experts Group (DEG) in Latvia	

REGULATORY
NON-REGULATORY
APPROACHES

Table 7: Summarising regulatory and non-regulatory approaches to share information on cyber incidents

6 Member States Regulatory and Non-regulatory Approaches for Cyber Security and Practices of Member States

Based on the high-level review that was carried out, a number of initiatives per approach were identified. The initiatives identified were collected based on several criteria.

First of all, we targeted the 28 EU Members States and the EEA/EFTA countries, namely Iceland, Liechtenstein, Norway, and Switzerland. We also focused on relevant initiatives being shaped beyond the local territories, notably at EU and global level.

Secondly, we looked into initiatives that focus on information related to incidents, threats, vulnerabilities and all other topics related to this specific part of cyber security.

Thirdly, we selected to include in this overview the initiatives or organisations presenting a certain level of maturity (at least two years of existence).

As explained in Chapter 5, certain initiatives might fit into more than one approach due to the difficulty to always clearly distinguish between the different approaches. The initiatives listed in this chapter have been classified based on their main characteristics. However, they might also find similarities with another approach.

6.1 Traditional Regulation in Practice

Based on the findings of our analysis it appears that only a few EU Member States (approximately one quarter of them) have set up traditional regulation in the field of cyber security information sharing.

In particular, in light of the findings of our research, it appears that a substantial part of traditional regulation which triggers information sharing stems from notification requirements enshrined in the European[49] and local regulation.

A first example in this regard is a European legislative act, the **EU Directive on the protection of personal data in the electronic communications sector**, known as the *ePrivacy* Directive which aims at protecting the privacy of personal data in the sector of electronic communications (European Parliament and the Council, 2012a). Based on a requirement of this directive, electronic communications service providers are required by law in all EU Member States having transposed the directive to empower their respective Data Protection Authorities (DPAs) and, under certain circumstances also their citizens in case of security breaches affecting personal data. Accordingly, all EU Member States have passed legislation to bring their laws in line with the notification requirement of the ePrivacy Directive. Illustrations of national measures taken in this respect are the following:

- In **Slovenia**, based on the **Electronic Communication Act** (Information Commissioner, 2015), the Communications Networks and Services Agency (AKOS) is obliged to notify security incidents and cyber violations to the national and governmental CSIRT (SI-CERT).
- **Legislative Act in the form of the Telecommunications Law** of 10 July 2012 of **Belgium** states that providers of public electronic communications services are obliged to report any security breach or

[49] For a summary of different security articles in EU legislation which mandate cyber incidents and cyber security measures, see (ENISA, 2012)

damage of integrity to the national regulator of electronic communications. (belgiquelex.be - Banque Carrefour de la législation, 2012)

Secondly, **sector-specific European regulation applicable to electronic communications** has defined a notification duty similar to the one described above. Accordingly, based on the Framework Directive (Article 13a) (European Parliament and the Council, 2009), "Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services. Where appropriate, the national regulatory authority concerned shall inform the national regulatory authorities in other Member States and the European Network and Information Security Agency (ENISA). Moreover, ENISA and the European Commission should receive a report summarising the measures taken to resolve the issues".[50]

As a third example in the area of incident reporting, there is the **upcoming NIS Directive** (European Commission, 2013a) which is expected also to provide an obligation for market operators in scope of the directive to notify incidents having a significant impact on the security (or continuity) of the core services they supply. The proposed NIS Directive is now under negotiation between the EU legislative bodies.[51]As with the ePrivacy directive, the NIS directive – once adopted – will need to be transposed in national laws, through primarily a legislative act (being a law, a decree or other regulatory act) for the notification obligation to become enforceable upon operators.

A fourth example related to notification obligations derives from **another European legislative act that has been enacted recently, the Electronic identification and trust services (eIDAS) Regulation** (European Parliament and the Council, 2014). Article 19 of this regulation stipulates that trust service providers should report "any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data" to the relevant supervisory bodies (e.g. national security authority or data protection authority) and in some cases, to ENISA. As the regulation is directly applicable at Member State level without need of transposition, the notification rule enshrined in this legislative act (the eIDAS Regulation) is directly enforced at national level.

Apart from these non-exhaustive examples, many other relevant regulatory texts can be cited in the context of mandatory incident reporting, such as the EU General Data Protection Regulation (GDPR) (legislative procedure towards its adoption currently ongoing)[52] and the EU Directive 2013/40/EU on attacks against information systems (European Parliament, Council, 2013).[53] Besides the above examples of legislative acts with a cross-border impact being imposed by the European legislative bodies, more and

[50] For more information on the ENISA work in the field of article 13a of the Framework Directive, see: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting

[51] To follow the status of the procedure, including proposed amendments to the proposal, see: http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2013/0027(COD)#basicInformation

[52] General Data Protection Regulation: Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) of the European Commission [2012/0011 (COD) - initial Commission's proposal as amended]. The legislative procedure towards the adoption of the GDPR is currently ongoing. At the time of drafting this study, the negotiations between the European Commission, the Council and the Parliament (trilogue negotiations) are in progress and the GDPR is expected to be adopted by end of this year (2015). Once adopted, the GDPR will replace the EU core regulation on personal data protection being currently in force (Directive 95/46/EC).

[53] Relevant work of ENISA relating to this directive: https://www.enisa.europa.eu/media/news-items/attacks-against-information-systems-good-practice-collection-for-certs

more countries are putting in place command-and-control legislation in the field of information sharing on cyber incidents at national level. We can mention the following indicative examples:

- The **Finnish Communications Regulatory Authority (FICORA)**[54], which the National Cyber Security Center (NCSC-FI) is part of. NCSC-FI is the home of the national and governmental CSIRT in Finland, the CERT Finland (CERT-FI). According to the Information Society Code 917/2014 (Ministry of Transport and Communications, Finland, 2014), FICORA is "responsible for the coordination of incident response and information security measures for both government institutions and the private sector" (BSA - The Software Alliance, 2015). Section 304 of the same act lays down the special duties of the authority which are, among others, to "collect information on violations of and threats to information security […] as well as on defects and interference situations in communications networks and services" and to "disseminate information security matters as well as communications network and service matters" (Ministry of Transport and Communications, Finland, 2014).
- The Communications Regulatory Authority of the Republic of **Lithuania** was "established under the **Law on Telecommunications and the provisions of the European Union Directives"** (RTT, 2015) and "is an independent institution which, among other tasks, is responsible for the regulation of cyber security activities".
- Another case of traditional national regulation is the case of **Estonia's "security measures for information systems of vital services and related information assets**" (Estonian Ministry of Interior, 2013) based on the Emergency Act of 2009 (Estonian Ministry of Interior, 2009). The Estonian government requires providers of vital services to report "any security incidents with significant impact" to the Estonian Information System's Authority. In addition, this regulation stipulates that the Estonian Information System's Authority will distribute the information to the institution in charge of this vital service and vice versa.
- Germany has also recently put in place local regulation in the field of incident reporting. In February 2015 the **German** parliament voted a **law to improve IT systems safety** (German Parliament, 2015). According to this law, all CIIP organisations are obliged to report serious incidents to the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, BSI).
- INCIBE, the **Spanish** national CSIRT, helped in modifying the 'Second Final Provision 9/2014' **Telecommunications Law**. This amendment obliges Spanish Internet Service Providers and administrators from the telecommunications sector to report and liaise with the competent CSIRT in case of cyber incidents.
- In **France** the **Law on Military Programing** (*Loi de Programmation Militaire* (Legifrance, 2013)) requires the Operators of Vital Importance (OVIs) to inform the National Agency for Information Systems Security (ANSSI) on incidents that could endanger the functioning of respective IT system. The OVIs can be part of several sectors, such as the health, water, energy, telecommunication, transportation and finance sectors. In this context, several working groups have been set up per sector, in order to define efficient and compatible rules.[55]

[54] FICORA: https://www.viestintavirasto.fi/en/cybersecurity/ficorasinformationsecurityservices/cert-fi/rfc2350.html (last access date: 10 June 2015)

[55] This example primarily refers to the defence sector which is out of scope of this project D-COD-15-T13. However, it is mentioned here as this law concerns other sectors in scope and has an influence on the intra-sector information sharing.

6.1.1 Challenges of Traditional Regulation and Approaches to Address Them

The examples above show that several EU Member States as well as EEA and EFTA countries have put in place their own legislation to regulate information sharing related to cyber incidents. Based on the interviews that were carried out we understood, that the differences between these national legislations may hinder information sharing between organisations coming from the different countries in scope, if no EU-wide mechanisms are in place.

Moreover, based on a number of interviews carried out during this study, as well as the practical experience of the experts who contributed to this analysis, it appears that local regulations imposing data localisation requirements, information storage restrictions, as well as information secrecy and non-disclosure rules are often perceived by the stakeholders affected as considerable obstacles to an efficient information exchange. In addition, certain countries or sectors consider that information sharing on cyber incidents may at the end be interpreted, on the grounds of the local or European regulation, as an anti-competitive behaviour and hence is likely to infringe competition rules. On the other hand, the national laws on personal data protection seem to be one of the biggest barriers in the information sharing process. For example, in several cases the national laws that consider IP addresses as personal data do not allow organisations to exchange this type of information, even if it could be helpful for other companies (ENISA, 2011).

To tackle these challenges, many organisations and initiatives engage in discussions with the law makers and regulators to make them aware of the issues encountered and the improvements that could be made. Examples in this direction could for instance be to raise stakeholders' education on the correct interpretation of the regulations concerned and enhance market (including public sector) awareness of which information sharing practices are actually permitted and which not. These organisations set up working groups and panel discussions; they draft publications, position papers and other materials to highlight the practical advantages of information sharing. An illustrative example in this area is FS-ISAC. Starting originally as a US initiative, FS-ISAC has become global and is now all the more active in EMEA (Continental Europe, Middle East and Africa). This forum works continuously on the review of European regulatory restrictions and legal requirements to enable information exchange in the financial sector at an international level. To meet their objective, FS-ISAC created a working group called the Joint Working Group Initiative (JWGI), which, amongst other activities, is currently compiling an analysis of legal obstacles and regulatory requirements around sharing of threat intelligence in Europe. Part of this effort is also the design of a report to the attention of companies' management, to explain the positive impact of information exchange for companies. Moreover, a second working group was tasked to create a regional and per-country 'landscape map' of national, sector-specific, and regional threat intelligence sharing initiatives and related organisations in Europe to give practitioners a better overview of who is doing what in this area.

Another practice was identified in the Czech Republic, where the NSA CZ engages in bilateral and case-by-case discussions with the different Internet Service Providers (ISPs) when it is not allowed to share certain types of information. However it seems that this process is time-consuming and not really transparent to other community members (ISPs) who could probably benefit from this information (e.g. by learning from others' experiences without necessarily getting hold of confidential or detailed information about an event). Thus, NSA CZ is trying to automate or improve this process. It is expected that with the adoption of the NIS Directive (European Commission, 2013a), notification requirements will be aligned across the EU and also encourage harmonised implementation across the sectors in the scope of the directive.

Last but not least, the findings of this stock-taking exercise confirmed that quite a lot of rule-making on information sharing in the area of information security actually stems not only (and not so much) from formal regulation, but from contractual arrangements, bilateral or multilateral agreements and framework contracts governing the provision of a service. A variety of contracts or agreements can be found both in the private and public sector between the parties involved in the provision of these services (e.g. software agreements). In the majority of cases, all these contracts incorporate high-level or detailed provisions on information reporting and information sharing obligations of the said service providers. Non-disclosure agreements are often included in this contractual framework imposing on their parties (service providers or the organisations requesting their services) which type of information (e.g. on a security breach) could be disclosed, to whom and under which circumstances.[56]

[56] A detailed overview of the categories and types of contractual tools (agreements, boiler-plate provisions, model contracts, etc.) that are used in the public and private sectors relevant to information sharing in the IT area, though it might be interesting for the purpose of this study, was not in the scope of the current stock-taking.

6.2 Alternatives Forms of Regulation (Co-regulation and Self-regulation) in Practice

Many different alternative regulatory initiatives to enable information sharing exist beyond the realm of traditional regulation in the EU/EEA today. Based on this, one can conclude that organisations tend to initiate information sharing by using a co- or self-regulatory approach, meaning that organisations establish common rules among each other either with or without the intervention of the regulatory bodies.

6.2.1 Co-regulation in Practice

Co-regulation differs from self-regulation in that it implies active government involvement and/or legislative backing of the initiative.

A common example of a co-regulatory set-up in this area are **Information Sharing and Analysis Centres (ISACs)**.[57] In the **Netherlands**, ISACs are established by the government's National Cyber Security Centre (NCSC) on a sector-by-sector basis (Water, Energy, Finance, etc.). The NCSC facilitates ISACs by providing them with a secretariat. ISACs meetings are held six or seven times per year, but some ISACs meet more regularly than others. There are also regular teleconferences, bilateral meetings between ISAC members, information shared via chats or closed channels/email lists.

All Information in ISACs is shared on a voluntary basis, but ISAC members are subject to certain rules. In order to become a member of an ISAC, organisations usually need to be accepted by the other members and have to sign an agreement/Memorandum of Understanding (MoU). This agreement/MoU states, for example, that the information shared within the ISAC cannot be shared onwards with other parties. While the contract is not legally enforceable, a violation of it may result in a warning or the organisation being banned from the ISAC.

The instruments and regulatory mechanisms used within co-regulatory initiatives are similar to those of self-regulatory initiatives. All ISACs in the Netherlands use the Traffic Light Protocol (TLP) - a mechanism widely used in information sharing communities - to indicate the permitted distribution of information. In addition, some ISACs limit the number of members of the group, in order to build trust, which is considered as crucial to foster information sharing.[58]

In the **United Kingdom**, a very similar set-up exists, organised by the government's Centre for the Protection of National Infrastructure (CPNI).[59] For thirteen different sectors[60], the CPNI organises **Information Exchanges (IEs)**, along the same lines as the Dutch ISACs. Information exchanges are free to join, but like in ISACs their membership is determined by the existing members. The CPNI typically provides a co-chair and a coordinator to facilitate the meetings of the IEs. Since trust amongst the members is regarded as crucial here as well, identity and employment verification checks are performed on all

[57] Information Sharing and Analysis Centres (ISACs): https://www.ncsc.nl/english/Cooperation/isacs.html (last access date: 4 September 2015)
[58] On the topic of trust, see also (ENISA, 2014a)
[59] Centre for the Protection of National Infrastructure – Information exchanges: http://www.cpni.gov.uk/about/Who-we-work-with/Information-exchanges/ (last access date: 4 September 2015)
[60] Current IE's: Aerospace and Defence Manufacturers, Communications Industry Personnel Security, Civil Nuclear IE, Financial Services IE, Managed Service Providers IE, Northern Ireland Cross-Sector IE, Network Security IE, Pharmaceutical Industries IE, SCADA and Control Systems IE, Space Industries IE, Security Researchers IE, Transport Sector IE and Water Security IE.

applicants as well as checks against official records. Member representatives are expected to attend all meetings, and only a limited number of members from the same organisation are usually allowed.

In **Germany**, **UP KRITIS**[61] is a large co-regulatory initiative in which critical infrastructure organisations participate (both private and public entities). It is organised by the *Bundesamt für Sicherheit in der Informationstechnik* (BSI) and the *Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe* (BBK). UP KRITIS facilitates working groups related to a certain sector or subject. Members do not need to be part of a working group to receive information. The working groups can be intra- or cross-sector related. Information that is only related to certain sectors will however not be shared with others (e.g. banking related-information will not be shared with water sector organisations).

Within UP KRITIS, information is shared based on the Traffic Light Protocol (TLP) as the information cannot always be made public. Information is shared via emails and standard templates provided by the Federal Office for Information Security (BSI).

Other relevant examples were observed during the research at Member State and EU level. We mention some of them in the list below:

- The Dutch Telecommunications Act imposes obligations upon network operators when encountering a state of emergency. However, the practical guidelines on how to comply with these obligations are primarily conceived, prepared and decided on by the market stakeholders themselves. This happens in the framework of a permanent group, the **(Dutch) National Continuity Telecommunications Forum** (NCO-T), whereby operators meet under the auspices of the Ministry of Economic Affairs (Ministerie van Economische Zaken, 2008).
- In the UK, the **Energy Emergencies Executive Committee Cyber (E3CC)**[62] is in an information sharing roundtable of senior information security professionals across UK electricity generation, transmission and distribution operators. The government participates to this initiative through DECC, CPNI and Ofgem. Via individual membership of CiSP and other communications the group shares information on security incidents in the energy sector.
- The **Austrian Trust Circle (ATC)**[63] founded in 2010 is an initiative of CERT.at and the Federal Chancellery. The primary goal is to build confidence between the responsible persons and organisation in individual sectors of strategic infrastructures so as to facilitate the exchange of security - related experience and ensure that swift and joint action will be taken when appropriate.
- The National CSIRT of **Luxembourg**, CIRCL, operates among others the **Threat indicators sharing platform for private sector (MISP)**.[64] They act as a platform for sharing threat indicators within private and public sectors. Their objective is to improve automated detection and response to targeted cyber attacks in Luxembourg and beyond.

[61] *Kooperation zwischen Betreibern Kritischer Infrastrukturen* (UP KRITIS): http://www.kritis.bund.de/SubSites/Kritis/EN/publications/Fortschreibungsdokument_engl..html (last access date: 10 June 2015)

[62] Energy Emergencies Executive Committee Cyber (E3CC): https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386626/E3C_Annual_Report_2014.pdf (last access: 4 September 2015)

[63] Austrian Trust Circle (ATC): https://www.cert.at/about/atc/content.html (last access date: 7 July 2015)

[64] Threat indicators sharing platform for private sector (MISP): https://www.circl.lu/services/misp-malware-information-sharing-platform/ (last access date: 4 September 2015)

- In **Sweden**, several industry stakeholders and the government have launched a public-private initiative named the **Forum for information sharing (FIDI)**[65] - in several sectors, such as finance and banking, health, energy and others.
- The **Thematic Network on Critical Energy Infrastructure Protection (TNCEIP)**[66] is an initiative of the European Commission, and is assembling European owners and operators of energy infrastructure in the electricity, gas and oil sectors. Members of the initiative meet four times a year and have access to a shared platform to exchange information on cyber incidents, attacks, vulnerabilities and threats relevant to information security.
- In **Norway**, the National Security Authority (NSM) has launched the **Warning system for digital infrastructure (*Varslingssystem for digital infrastruktur* – VDI)**[67] which operates a 'sensor network' to detect attempts of hacking against critical infrastructure across sectors. VDI cooperation is largely based on openness and trust between NSM and participating companies and agencies.
- The **MELANI (GovCERT.ch)**[68] **and SwitchCERT**[69] are two **Swiss** CSIRTs. GovCERT.ch is responsible for the safeguard of critical infrastructure in the public administration and finance and banking sectors. SwitchCERT handles security, fraud detection and elimination. Both organisations are mandated ad interim to provide their services for certain sectors also in **Liechtenstein**.
- At the European level, in the context of Article 13a of the Framework Directive (European Parliament and the Council, 2009), **ENISA** has launched several initiatives in the field of information sharing on cyber incidents.[70] Noteworthy cases are the ‘Article 13a meetings’ where the **Article 13a Expert Group** meets three times a year to discuss about recent incidents, lessons learned and measures that might be taken to prevent incidents[71]; the **Electronic Communications Reference Group (ECRG),** being composed of Chief Information Security Officers (CISOs) of the main electronic communications operators that addresses security topics across the broad subject area of electronic communications - including security measures, incident reporting and data protection[72]; the **European Public-Private Partnership for Resilience (EP3R)** [73] - which existed between 2009 and 2013[74] - to encourage the private sector to share information, discuss good practices to be followed, policies, objectives, measures and other initiatives that could be undertaken to strengthen the robustness of network resilience.

[65] Forum for information sharing – FIDI: https://www.msb.se/Upload/Produkter_tjanster/Publikationer/KBM/Information%20Security%20in%20Sweden.pdf (last access date: 4 September 2015)

[66] Thematic Network on Critical Energy Infrastructure Protection (TNCEIP): http://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure (last access date: 15 June 2015)

[67] *Varslingssystem for digital infrastruktur* (VDI): http://nsm.stat.no/tjenester/varslingssystem-for-digital-infrastruktur-vdi/ (last access date: 15 June 2015)

[68] MELANI (GovCERT.ch): https://www.melani.admin.ch/melani/de/home.html (last access date: 7 September 2015)

[69] SwitchCERT: https://www.switch.ch/security/ (last access date: 7 September 2015)

[70] For information on ENISA’s work in the field, see: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting

[71] Article 13a Expert Group: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting (last access date: 15 September 2015)

[72] Electronic Communications Reference Group (ECRG) https://resilience.enisa.europa.eu/ecrg (last access date: 10 June 2015)

[73] European Public Private Partnership for Resilience (EP3R): https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r (last access date: 15 September 2015)

[74] See (ENISA, 2015c)

- In March 2012, the **US Federal Communication Commission (FCC)**[75], working with communications companies including Verizon, Cox, and Comcast, passed a voluntary code that spells out the steps participating Internet Service Providers (ISPs) must take to combat botnets. ISPs agreeing to follow the code must "take meaningful action" in each of the following areas: education, detection, notification, remediation, and collaboration. Those who follow the code are added to a 'safe list' maintained by the FCC.

6.2.1.1 Challenges of Co-regulation and Approaches to Address Them

Although co-regulatory initiatives like the examples discussed above are increasingly expanding and grow in popularity, they still have to address a number of challenges: lack of, or weak, enforcement and trust, the voluntary nature of membership and, quite often, the voluntary (or not really monitored) nature of information sharing.

On the point of enforcement, it seems that the exclusion of a member can be considered as a strong deterrent only if the co-regulatory platform has proved to bring a real added value to their stakeholders to such an extent that stakeholders who are deprived from membership will consider this as a major loss (e.g. loss of or missing access to knowledge, missing networking opportunities, loss of reputation, etc.). As far as trust is concerned, the view of the authors of this report is that there are means the co-regulatory (as well as self-regulatory) schemes could use to inspire confidence to their members in order to exchange information in a meaningful way without causing any prejudice to the wrongful party. Such means can be, for instance: the mandatory application of the Traffic Light Protocol restrictions, the exchange of information that stakeholders may consider as potential harmful only on a non-named basis and through the use of a trusted third party (e.g. the platform's co-ordinator), the mandatory execution of strict Non-Disclosure Agreements (NDA) which will, in itself, provide sanctions in terms of inappropriate disclosure of information, the creation of temporary, closed sub working groups relying on an infrastructure which prevents the sharing of the information with anybody outside of the closed working group.

Regarding the voluntary nature of membership, a point of discussion that seem to raise concerns within such initiatives is how to strike the right balance between limiting the number of participants (in order to always keep information under control) and taking the risk of not including new stakeholders whose contribution might be valid to their organisation. According to statements and proposals of stakeholders who contributed in the study, a collective design of a Memorandum of Undestanding within the group of existing participants could for example identify ways and ideas on how the group could accept new applications for membership whilst motivating new and existing members to effectively share information (e.g. via meetings, group activities, interactive information sessions, organisation of open events with the aim of attracting new members).

On the topic of the voluntary information sharing, the day-to-day operations of the co-regulatory (as well as self-regulatory) fora mentioned herein also demonstrate that stakeholders are in practice more comfortable with sharing information if they know that the objective of the information exchange is to enhance market intelligence and disseminate good practices rather than to spot actions of non-compliance, which may lead to reputational damage, court action and so far.

In the light of the suggestions made during the survey, it may be worthwhile examining whether the initiatives based on co-regulation could adopt a 'modus operandi' that convince their participants that information exchange does not aim at the sanctioning of bad examples and does not to be perceived as a notification strictly speaking (to the regulator or the 'market'). The members of such initiatives may need

[75] US Federal Communication Commission (FCC): https://www.fcc.gov/ (last access date: 20 May 2015)

to consider their participation in the group as a unique opportunity to learn from the experiences of peers and participate in the shaping of good practice that reflects the same concerns and, ideally, a common approach to risk.

In other words according to a number of experts having contributed in this study, it would be more beneficial to try to better incentivise the market in joining the existing co-regulatory initiatives than to take the effort to enact new regulation that would render mandatory the exchange of information.

Moreover, the representative cases outlined in this study seem to address the above hurdles - lack of, or weak, enforcement and trust, the voluntary nature of membership and, quite often, the voluntary (or not really monitored) nature of information sharing -via different measures: agreement on ad hoc rules, focusing on trust-building and using the Traffic Light Protocol (TLP) to regulate how information can be disseminated. A number of initiatives have recourse to other mechanisms, such as fostering a continuous working relationship and regular interactions between their participants, encouraging recurrent meetings and mutual help. Interesting to note, however, is the evolution in Germany, where members' potential reluctance to share information about vulnerabilities may be overcome through the entry into force of traditional regulation. A new law that obliges critical infrastructure providers (CIPs) to report serious incidents to the BSI was established in 2015 (German Parliament, 2015).

6.2.2 Self-regulation in Practice

Through our research we found around thirty examples of self-regulatory efforts. These initiatives can be limited to one sector or can operate across sectors and also national borders.

A first illustration of a self-regulatory initiative is **Spain's Industrial Cybersecurity Centre (CCI)**[76], an industry-led centre that operates without subsidies, independently and as a non-profit organisation. Its mission is to boost and improve 'Industrial Cybersecurity' in Spain and Ibero-America, defining it as "the set of practices, processes and technologies, designed to manage cyber space's risk associated to the management, process, storage and transmission of information used by industrial infrastructures, from the points of view of people, processes and technologies".

We found further self-regulatory practices in **Poland**. The **n6 Network Security Incident Exchange**[77] is a free platform for collection and transmission of information on threats and incidents. The platforms includes malicious URLs, malware, scanning, IP addresses or the names of malicious software, depending on the availability of specific information. The platform is aimed at the national and private sector. Next to this, the **ABUSE Forum**[78] is an initiative of NASK and operates within the NASK CERT Polska team. The forum meets quarterly and also maintains closed email list dedicated to sharing of information about threats and incidents. Participants come from many sectors including Internet services, banking and public administrations.

Other noteworthy cases of self-regulation are listed below:

- The **French *Club des directeurs de sécurité des entreprises* (CDSE)**[79] (Chief Security Officers Club) is an organisation established more than 25 years ago to federate security experts' experiences working in the major French companies.

[76] Industrial Cybersecurity Centre (CCI): https://www.cci-es.org/en/home (last access date: 20 May 2015)
[77] n6 Network security incident exchange: http://n6.cert.pl/ (last access date: 30 June 2015)
[78] ABUSE Forum: http://www.abuse-forum.pl/ (last access date: 7 September 2015)
[79] *Club des directeurs de sécurité des entreprises* (CDSE): https://www.cdse.fr/ (access date: 26 August 2015)

- The **Spanish Association for the Advancement of Information Security (ISMS Forum Spain)**[80] is a non-profit organisation founded in January 2007 to promote the development, knowledge-sharing and culture of Information Security in Spain and to act for the benefit of the entire sector. It was created with a plural and open vocation, that is set up as a specialised debate forum for companies, public and private organisations, researchers and professionals as a place where to collaborate, share their experiences and know the latest advances and developments with regard to Information Security. The Association activity is carried out from a perspective of transparency, independence, objectivity and a neutral stance.
- In **Italy**, the ***Associazione italiana esperti in infrastructure critiche* (AIIC)**[81] (Italian association of critical infrastructure experts) aims at exchanging experiences and knowledge related to critical infrastructure to create an interdisciplinary and inter-sectoral shared approach among experts of different fields. Their goal is to share knowledge about cyber incidents related to CIIP.
- In December 2012, Deloitte Belgium initiated the **Cyber Threat Intelligence Sharing Research Project (CTISRP)**[82]: an initiative bringing together a number of major public and private organisations from across Europe to discuss sharing of cyber threat information between these organisations. The goal was to understand better the benefit of exchanging information on cyber security incidents across countries, sectors, and industries.
- The **Bulgarian Association of Information Technologies (BAIT)**[83] has the mission to protect the general interests of its members by actively working for the establishing of information society in this country, for the development of the Bulgarian ICT industry and of the ICT market in general. Established in 1995, the association registers currently 135 member companies and organisations. The Association includes companies in the trend of hardware, software, system integration, networks, telecommunications, Internet suppliers, etc.
- The **Information Technology and Information Systems Security Experts Group (DEG)**[84] in **Latvia** is the former LV CSIRT and is composed by IT and systems experts from various organisations in the country. One of the main goals of the group is to facilitate information exchange among members. DEG has created statutes and a code of ethics to rule the information exchanges. In addition, members meet on a monthly basis.

The **European Financial Institutes - Information Sharing and Analysis Centre (EU FI-ISAC)**[85] is a forum consisting of ‘country representatives coming from the financial sector, national CSIRT's (GovCerts) and Law Enforcement Agencies (LEA’s). Other organisations participating in it are: ENISA, Europol, the European Central Bank (ECB), the European Payments Council (EPC) and the European Commission’ (ENISA, n.d.(b)). The members exchange information on vulnerabilities, threats and incidents and are obliged to use the Traffic Light Protocol (TLP), which ensures that sensitive information is shared according to requirements defined by the source individual/organisation. TLP guides the members’ behaviour on how to share information with the entire sector (provided that there is no use of publicly accessible channels).

[80] ISMS Forum Spain: https://ismsforumspain.wordpress.com/about-us/ (last access date: 27 July 2015)
[81] AIIC : http://www.infrastrutturecritiche.it/aiic/index.php?option=com_content&view=article&id=14&Itemid=39
[82] Cyber Threat Intelligence Research Project (CTISRP): http://www.politiestudies.be/userfiles/20141202%20BISC%20Luc%20Beirens%20voor%20verspreiding.pdf (last access date: 15 May 2015)
[83] Bulgarian Association of Information Technologies (BAIT): http://www.bait.bg/about-bait/about-bait (last access date: 7 July 2015)
[84] DEG: https://www.cert.lv/section/show/17 (last access date: 7 July 2015)
[85] European FI-ISAC: https://www.enisa.europa.eu/activities/cert/support/information-sharing/european-fi-isac-a-public-private-partnership (last access date: 29 May 2015)

6.2.2.1 Challenges of Self-regulation and Approaches to Address Them

The challenges faced by self-regulatory initiatives are very similar to those faced in co-regulation set-ups: as noted above, one of the main challenges that is inherent to the use of self-regulatory initiatives is that membership, as well as adherence of their members to agree upon rules is entirely voluntary. Especially in the area of cyber security information sharing, this can pose a problem, as companies and governmental actors are hesitant to share information about their vulnerabilities, given that such sharing can lead to reputational loss especially when the information becomes public. A major deterrent to the voluntary sharing of information is a lack of trust between participants in any given sector, especially in a cross-border context. To address this challenge, many of the self-regulatory initiatives this study has identified regularly organise face-to-face meetings to build trust and encourage sharing amongst participants. In addition, most initiatives regulate the use, and onwards distribution, of information shared using the Traffic Light Protocol (TLP).

As stated during the interviews performed during this study, the use of TLP in itself can pose issues as well. In cross-border sharing, country-specific legal requirements may still oblige the receiver of information to pass it on, to a regulator or within a sector, effectively overriding the TLP-level attached to it. In addition, members do not always fully understand that TLP aims to clarify how information can be used and disseminated beyond the group. Furthermore, there seem to be various interpretations of AMBER in various information sharing communities. Some CSIRTs for example, may share information labelled as AMBER downwards with their own constituencies while others would not consider their own constituencies as part of their own organisation. Based on some interviews with experts in the topic, it also appears that some sharing schemes seem to take a more open interpretation than others of AMBER data in some cases, which permits information to be shared with responsible, concerned, external organisations and stakeholders on a case-by-case basis. Some CSIRT experts are of the opinion that TLP should be formalised towards becoming an international standard. According to these experts, it would be helpful for national and governmental CSIRTs to negotiate towards a common TLP standard. Towards this end, the challenge is to find all TLP interpretations currently in use by all information sharing communities and to find a representative translation (Millar, 2015).

Another concern raised about TLP relates to the fact that more and more CSIRTs are connecting with the intelligence community which is used to employ government classification schemes (such as SECRET and TOP SECRET). However, according to some CSIRT experts, it would be challenging to combine the use of TLP and classic classification. The first reason for this is that not all of the intelligence community is used to the TLP logic. A second reason may be that TLP has no formal legal value thereby possibly disallowing the intelligence community to use it.[86]

Another challenge of self-regulation compared to traditional regulation is the lack of mechanisms to enforce agreed upon rules. We found that this can be overcome by warning and excluding members in case of non-compliance to the set rules. In the EU FI-ISAC initiative for instance, members sign up to Membership Guidelines through which they commit, inter alia, to regularly attending physical meetings. Even though there is no legal recourse to non-compliance with this rule, members may get excluded from the initiative and lose the benefits that come with participation if they do not attend three successive meetings.

[86] Content based on a presentation of the FIRST conference (Millar, 2015) and the comments made by CSIRTs experts during the presentation.

6.3 Other Approaches (Information and Education) in Practice

Our desktop research identified approaches implying awareness raising and education on cyber security and incidents. These approaches do not seem to be defined by either a regulatory body or by a group of organisations. They seem to be voluntary initiatives that have as main objective to disseminate information towards others and to educate the community on the current threats, vulnerabilities and other cyber security related challenges.

A first example of this type of approach are the **working groups**[87] held by the Czech CSIRT (**CSIRT.CZ**). CSIRT.CZ organises regular meetings with the members of the security community of the Czech Republic. Events are held twice or three times a year. During the meetings, members can discuss topics related to current trends in the field of safety, security threats, and the development of cooperation between security teams. Moreover, the meetings also represent the opportunity to mutually exchange experience in the field of prevention and resolution of security incidents.

A second example is the **Alliance for Cybersecurity**[88] launched by the German BSI and the Federal Association for Information Technology, Telecommunications and New Media. This cross-sector and voluntary initiative aims to ‘inform and report on cyber incidents’ at national level (Jones Day, 2014). The objective of this organisation is to share information related to cyber security and incidents to help the community in being prepared to encounter them.

A third example, the **Cyber-security Information Sharing Partnership** (**CiSP**)[89] in the United Kingdom is also a representative example of the awareness raising approach. This cross-sector initiative launched by CERT-UK has the objective to ‘share cyber threat and vulnerability information in order to increase overall situational awareness of the cyber threat and therefore reduce the impact on UK business’ (CERT-UK, n.d.). Information can be exchanged among members but they also receive reports from the CERT-UK concerning the current situation of the network. Moreover, the initiative has been extended to the Northern Ireland region (Northern Ireland CiSP) since January 2015. The goal of this regional community is to share information with local members on cyber security threats.

Another example is the **Belgian Network and Information Security (BELNIS)** [90], established in 2005, which acts as a coordinating workgroup that includes representatives from government agencies engaged in cyber security. It provides advice to the government on cyber security incidents and cyber security in general. Other relevant examples that came up during this study are listed below.

- In Slovakia, **the Slovak Office for Personal Data Protection** started to publish information on the official website (as reports, guides, magazines and in other formats) to organise events (seminars, conferences) or propose advisory services related to the issue. The Office collaborated in that regard with companies from the IT sector and other public and private institutions (FRALEX, 2009).

[87] Working groups CSIRT.CZ: https://www.csirt.cz/page/886/spoluprace/ (last access date: 7 September 2015)
[88] Alliance for Cybersecurity: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html (last access date: 7 July 2015)
[89] CiSP: https://www.cert.gov.uk/cisp/ (last access date: 4 September 2015)
[90] Belgian Network and Information Security (BELNIS): http://www.senate.be/www/?MIval=/Vragen/SchriftelijkeVraag&LEG=5&NR=8213&LANG=fr (last access date: 15 June 2015)

- The National Security Authority of **Hungary** organises a yearly **'Conference on Information Security and Cyber Defence (ISCD)'**.[91] Started in 2011, this conference aims at exchanging information related notably to security and cyber defence, cyber challenges and cyber threats.
- The **(ISC)² Ireland Chapter**[92] is an organisation that aims at raising awareness and educating the Irish community by organising seminars. Their goal is to share information and knowledge and market collaboration.
- The **Cyber Security Research Center from Romania (CCSIR)**[93] is a non-governmental organisation with the objective to promote and support research related to cyber security in Romania and encourage market partnerships in this area.
- Under the Commission's Safer Internet Action Plan (2004), the **Safer Internet Forum**[94] was established to act as 'a discussion forum including representatives of industry, law enforcement authorities, policymakers and user organisations (e.g. parent and teacher organisations, child protection groups, consumer protection bodies and civil and digital rights organisations). It provides a platform for national co-regulatory or self-regulatory bodies to exchange experience and an opportunity to discuss ways in which industry can contribute to the fight against illegal content (European Parliament and the Council, 2015).
- The **European Cyber Security Protection Alliance** (CYSPA)[95] focuses on a sector-by-sector approach to evaluate the impact of cyber risks and to create a community of stakeholders interested in sharing knowledge to improve their level of cyber protection.
- Based on existing industry standards, guidelines and practices, the US National Institute for Standards and Technology (NIST) issued the first version of the **NIST Framework for Improving Critical Infrastructure Cybersecurity**[96] in 2014. The Framework only intends to promote the protection of critical infrastructure and can be used as a handbook by operators across sectors and borders.

With the goal of educating and sharing information with the community, ENISA issues many reports and often organises workshops or exercises. Noteworthy cases are the guidelines for CSIRTs collaboration (ENISA, 2009), studies to encourage exchange between CSIRTs (ENISA, 2011) or to present the advantages of information sharing (ENISA, 2010).[97]

6.3.1 Challenges of Information and Education and Approaches to Address Them

In the light of the interviews conducted, it appears that the trust element is equally important in this stream as in the co- and self-regulatory set-ups. The measure of "success" of education and similar

[91] Conference on Information Security and Cyber Defence (ISCD): http://www.nbf.hu/iscd/2014-hu.html (last access date: 7 July 2015)

[92] (ISC)² Ireland Chapter: http://isc2irelandchapter.org/ (last access date: 7 July 2015)

[93] Cyber Security Research Center from Romania (CCSIR): http://ccsir.org (last access date: 7 July 2015)

[94] Safer Internet Forum: http://www.saferinternet.org/sif (last access date: 7 July 2015)

[95] European Cyber Security Protection Alliance (CYSPA): http://www.cyspa.eu/default.aspx?page=home (last access date: 15 April 2015)

[96] NIST Cybersecurity Framework, http://www.nist.gov/cyberframework/ (last access date: 30 April 2015)

[97] To be noted also the role of ENISA as facilitator for Member States by supporting the exchange of good practices in the area of Cyber Crisis Cooperation and Exercises. It appears that ENISA is the driving force behind the series of pan-European cyber exercises Cyber Europe as well as the joint EU-US cyber exercise (Cyber Atlantic). Along the same lines, ENISA published a 'Good Practice Guide on National Exercises' with the aim to assist European stakeholders to design, plan, execute and monitor a national exercise on the resilience of public communication networks. Third, ENISA is organising the series of the annual International Conferences covering topics in the area of Cyber Crisis Cooperation and Exercises (ENISA website at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation)

approaches largely depends on how eager the members are to share information and be transparent regarding their needs, the practices they follow (e.g. in case of a cyber incident) and the experiences they have. As the primary objective of this type of information sharing initiative is to reach and educate as many members as possible, trust building might be difficult to achieve among large groups of people/participants.

In particular, interviewees noted that members might hesitate to exchange information when they are not acquainted with most participants. However, the example of the Cyber-security Information Sharing Partnership (CiSP) shows how this challenge may be addressed by insisting on the fact that the applications to become a member are "assessed fairly and independently" (CERT-UK, n.d.). In this case, the organisation assures the members that the used information sharing platform is secure, frequently monitored and tested.

Furthermore, based on the literature reviewed during this study, other challenges and the appropriate measures to address them may be highlighted in this type of approach. Firstly, it might be challenging if the objective of the community is opposed to, or not in line with, the goal of another regulatory instrument. In this case, the initiative should be incorporated or aligned with the other policy tools. Secondly, it might be hard to measure and to verify whether the behaviour of the community has changed or the degree at which the awareness has been raised as a result of an initiative under this cluster. Moreover, it might take time to meet the objectives of this approach (i.e. education and awareness raising) as the goal is to reach a wide community. Therefore, this type of tool should be used in situations where there is enough time to diffuse the message and to evaluate the results of the initiative (OECD, n.d.).

7 Conclusions and Recommendations

7.1 Conclusions

This report aims at identifying the regulatory and non-regulatory approaches that EU Member States as well as EEA and EFTA countries use, in order to share information on cyber incidents and to address the challenges of sharing information. Based on desk research and the conduct of interviews, and with the support of the of National Liaison Officers (NLOs) of ENISA, more than eighty (80) initiatives and organisations and more than fifty (50) national and governmental CSIRTs involved in information exchange on cyber incidents were identified at EU and EEA level. More information on this list of identified initiatives and relevant organisations (including national and governmental CSIRTs) as well as on the possible access to it can be requested by contacting cert-relations@enisa.europa.eu.

Some of these initiatives have been discussed in this study based on the distinction between three different clusters of regulatory/non-regulatory approaches, being: 1) traditional regulation; 2) alternative forms to regulation, such as co- and self-regulation; and 3) other approaches, such as information and education.

7.1.1 Geographical Distribution of Initiatives

In light of our findings, we understand that there are countries - such as for example the Netherlands and the United Kingdom - where the co-regulation approach is used the most. This is mainly due to the relatively high number of ISACs (Information Sharing and Analysis Centres) and/or IEs (Information Exchanges) that exist in these countries. Examples of self-regulation can be found in Poland and Spain. Furthermore, at EU and global level, the co- and self-regulatory approaches are preferred to share information or launch new initiatives. Besides the Netherlands and the United Kingdom, a relatively high number of initiatives exist in France. These initiatives are usually based on other non-regulatory approaches, such information and education schemes.

Furthermore traditional regulation does not seem to be the most used approach among the countries in scope, but the use of this approach is spread geographically across EU, EEA and EFTA.

Finally, some countries have less information sharing initiatives or do not run them by themselves. Some countries join forces with larger countries: a recent illustration of this is the case of Liechtenstein which mandated the Swiss CSIRTs – MELANI and SwitchCERT – to provide ad interim their services for certain sectors in Liechtenstein too.

7.1.2 Prevalence of Alternative Types of Regulatory Initiatives

Although national legislators in EU Member States seem to increasingly issue traditional regulation in the cyber security space, most information sharing initiatives identified in this study are still based on self- or co-regulation. In addition, traditional regulation, triggered especially from European legislative texts which aim at harmonising notification requirements, has so far not moved beyond imposing incident reporting obligations on electronic communications and critical service providers. Although other sector communities will be concerned in the near future by notification obligations that are foreseen in European legislation that is currently in preparation (see the upcoming NIS directive for example), this extension will not change the fact that regulation is perceived by the market as a ‘one-way street’ since information sharing is actually ‘directed’ without necessarily implying the real involvement of the wider cyber security community.

Based on desk research and the interviews conducted, we understood that most initiatives do not only share information on cyber incidents. Their missions and objectives seem to be broader than just concentrating on this type of events. For example, besides incidents, vulnerabilities and threats, organisations are willing to share information such as strategies related to cyber security, operational methods and best practices in the information security area.

It appears that a substantial part of the information is shared across sectors, this means that organisations coming from different sectors are part of the same group and share with other members, regardless of their sector. However, this trend seems to change with the level of maturity of the initiative and of the sector. The finance and banking sector and the public administration sector seem also more developed in terms of intra-sector information exchange.

The initiatives appear to be relatively open to welcoming new members. Only few organisations follow strict entry criteria or request a membership fee. Finally, when the initiative does not stem from traditional regulation, the information is in many cases shared on a voluntary basis. In the majority of cases information is exchanged informally (e.g. during face-to-face meetings, conferences, etc.), as well as virtually (via platforms, email lists, teleconferences, etc.).

7.1.3 Challenges to Sharing Information on Cyber Incidents

Different regulatory and non-regulatory approaches bring different challenges with them.

In the case of traditional regulation, we understood that legislation related to mandatory reporting varies from Member State to Member State and is sometimes vague. It is however expected that recently-enacted European regulation (e.g. the eIDAS Regulation) and other acts being currently shaped (e.g., proposed NIS Directive (European Commission, 2013a)) will streamline notification requirements cross-border and will promote harmonisation of the practices that have already been deployed at national level around security breach reporting, cyber incident preparedness and reaction. Consequently, organisations do not know exactly what they need to share. Conversely, in voluntary information sharing initiatives, some members may hesitate to share personal or internal information with other members. In the case of educational or awareness raising approaches, as the primary objective of this type of information sharing initiative is to reach and educate as many members as possible, trust building might be difficult to achieve among large groups of people. As a result, members might hesitate to exchange information when they are not acquainted with most participants.

7.1.4 Trust as a Key Element for Information Sharing

As many other studies pointed out, trust is a key success factor for information exchange in the field of cyber security and incidents. Members of a community want to know with whom they share data and whether the data will be handled appropriately. Throughout the interviews that were carried out, we understood that trust building has become one of the main objectives of the initiatives as it facilitates the exchanges, especially when the initiatives are based on voluntary information sharing.

In this context, trust building seems to be a process where participants need to prove that they can be trusted and that they share the same objectives, ethical principles, and views of their counterparts. It must be noted that the dialogue and information sharing within the co- and self-regulatory schemes discussed herein does not primarily aim at revealing stakeholders’ weaknesses or gaps in terms of cyber security but rather to create a climate of confidence and trust to share between the stakeholders concerned good and bad practices, exchange experiences around events, discuss preparedness measures and even reactions from citizens or regulators in the information security broad subject area. Along these lines, it is noteworthy to state that the climate of trust is built more easily when the purpose of the information exchange is ‘intelligence’ (communicate knowledge and best practices) rather than ‘evidence’ (use information as proof in order to take action before a regulator or court). Ideally, the success of the co- or self-regulatory approach is not only to bring forward rules made by the market but also create a trusted environment which will encourage awareness raising and participants’ education.

Interviews suggested several methods to build trust: informal meetings, small group meetings, transparency, teleconferences, use of TLP or of other standards establishing some rules on how information should be communicated.

7.1.5 Important role of National and Governmental CSIRTs

In the context of the information sharing initiatives, it is worth mentioning the important role of national and governmental CSIRTs that was already presented for instance in the study ‘A flair for sharing – encouraging information exchange between CERTs’ (ENISA, 2011).

It seems that certain CSIRTs have launched activities to promote information exchange among their constituents. Noteworthy cases are: INCIBE-CERT (Spain) which took actively part in the change of the national regulatory framework on incident reporting and, based on this regulatory change, it follows a collaborative approach towards sharing useful information with Internet Service Providers (ISPs) and the private sector in general; the NASK Polska team which launched the ABUSE Forum, being a cross-sector initiative to share information on cyber security incidents and threats amongst ISPs, financial operators and the public sector; the Luxembourg CSIRT running, amongst others, the threat indicators sharing platform aiming at improving the public and private sectors’ response to cyber attacks within the country and beyond; or the Czech CSIRT.CZ organising working group meetings for security teams. By developing these activities, CSIRTs contribute and share their experience with other organisations willing to exchange information. They can share best practices and potentially serve as examples for future initiatives.

7.2 Recommendations

In the light of the practices discussed in this report and the conclusions above, the following recommendations may be considered as follow-up steps to this study. Where possible, tentative action owners are proposed. Accordingly, the relevant communities to take certain action in order to enhance the landscape of information sharing are primarily: law makers and regulators, governmental institutions; the owners, founders, initiators or co-ordinators of the different initiatives discussed herein (collectively named sometimes here as 'initiatives' or 'approaches'); the market stakeholders in general or a specific community, as well as European bodies such as ENISA.

7.2.1 Leverage Existing Self-Regulatory and Co-regulatory Initiatives

A number of areas for improvement can be suggested in order to fully benefit from the co- and self-regulatory schemes, in particular trust, enforcement, as well as transparency and promotion.

In a nutshell, following challenges and areas of improvement have been identified based on the findings of this study:

- **Trust:** To foster trust, information sharing founders, coordinators and/or facilitators could use following alternatives:

  1) limit the number of participants to better control the channels and boundaries of information exchange;

  2) use the Traffic Light Protocol to regulate information sharing and ensure that members are aware of how to use it in practice; and

  3) set rules (and adequate mechanism to enforce them) to prevent absenteeism and to further encourage regular information sharing by each member.

- **Enforcement**: Voluntary approaches naturally suffer from the lack of legal basis and strict enforceability of any agreed upon rules. To overcome this challenge, the initiatives should build up sets of rules and exclude members who do not adhere to the rules of the initiative.

- **Transparency and promotion**: For co- and self-regulatory initiatives to grow efficiently, it is essential to clearly inform the participants of the relevance and real added-value of such initiatives as well as to be transparent regarding the rules and practices followed. These initiatives (if necessary, with the backing of the competent authorities overseeing them) should emphasise more dynamically the assets and benefits that members of such initiatives will draw by their active participation in such fora. The founders or facilitators of the co- or self-regulatory groups such as the ones identified in this study, should ideally design a 'go to market' plan to better highlight to their members and potential joiners the advantages, added-value elements and the incentives of participating in the group.

For law makers and regulators or any other stakeholder willing to launch new programs or initiatives for strengthening information exchange, it is highly recommended to look first at the lessons learned and the experiences gained within the currently existing initiatives and then leverage on the existing successful initiatives. It may be more worthwhile and cost effective to first check to what extent the current initiatives can be complemented rather than spending additional effort (operational, financial and technical means) to launch new initiatives.

Recommendation for:

- EU and national policy makers, law makers and regulators;
- Governmental institutions and administrative bodies as they have an influence and control on the policy and legislative framework; and
- The actors of the initiatives as such, being indicatively the initiatives' founding or supporting bodies being CSIRTs or other.

7.2.2 Harmonise Regulation Rather than Enact New Mandatory Rules

Traditional regulation related to cyber incidents reporting does not seem to be harmonised at EU level and remains a vague notion in certain Member States. This might be confusing for organisations willing to share information and can, in some cases, hinder information exchange. Member States law makers and regulators should therefore be more precise in terms of what is allowed or must be reported; they should clearly define the situations in which mandatory reporting is needed or what constitutes personal data. Moreover, they should establish laws and guidance to the attention of stakeholders involved in information sharing initiatives, in order to orientate them on how to minimise the exchange of personal information or on how to share this kind of data in case of real necessity. With the adoption of the NIS Directive, cyber security might be at the centre of discussions in the EU, therefore, law makers and regulators or other interested stakeholders should take this recommendation into account when implementing mandatory reporting rules at EU level. Regulatory bodies could also provide guidelines with the purpose to harmonise the different notification requirements established by the eIDAS Regulation, the Personal Data Regulation and the proposed NIS Directive. Finally, public administrations should take actions and be involved in the field of information sharing as they have an important influence on the legislative framework of law makers and regulators and their behaviours.

Recommendation for:

- European oversight and regulatory bodies, competent by sector;
- European policy and law makers;
- National regulatory and oversight bodies; and
- Standard-setting bodies.

7.2.3 Further Develop Intra- and Cross-sector Exchange with Government Intervention

As intra-sector information exchange seems to be more developed under the co-regulation approach (e.g. ISACs in the Netherlands or IE's in UK), national governments should back up and help national initiatives to develop themselves, to become more mature and increase the number of exchanges. Governments and information sharing initiatives facilitators can use different approaches and solutions to encourage organisations to share information (mutual contracts or agreements, terms and conditions to sign, protocols, secretary support, etc.).

Recommendation for:

- National governmental institutions; and
- Information sharing initiatives' facilitators (e.g. CSIRTs or administrative body supporting an initiative financially or in another way).

7.2.4 Take Advantage of the Practice Developed by National and Governmental CSIRTs

As CSIRTs seem to be experienced in information sharing, the governments, information sharing facilitators or any other stakeholder willing to engage in a new initiative should base themselves on the examples of and on the lessons learnt from CSIRTs. CSIRTs could also be involved by facilitators in more information sharing initiatives so that they can actively share information, best practices and knowledge with other organisations.

Recommendation for:

- National governmental institutions;
- Information sharing facilitators with the support of CSIRTs; and
- Any stakeholder willing to engage in a new information sharing initiative.

7.2.5 Build upon Existing Work Performed by EU Institutions and Bodies – including ENISA – and by the Member States in the Field of Information Sharing on Cyber Security Incidents

A number of examples outlined in this study have shown that initiatives active in the area of critical infrastructure protection can already demonstrate a good record of information sharing. On top of that, mandatory European regulation related to incident reporting that is already enforceable in the electronic communications sector incite the relevant operators to adopt a ‘culture of sharing’ (towards the regulators but also towards their peers and the public at large). The national and European regulatory bodies in these areas could help build upon the best practices followed by the market in incident reporting and, based on the practical experience gathered, back the initiatives identified herein and, to a certain extent, help disseminate to the market good examples, tools and, at the end, a *modus operandi* on information sharing.

Along the same lines, being the European Union Agency for Network and Information Security ENISA gained a long and deep experience in the field of this study. Several initiatives of information sharing have been launched by ENISA related to notification requirements and electronic communications network resilience, many ideas and propositions have been sketched and good practices have already been produced related to information sharing.[98]

The European Commission and ENISA should find ways to boost the interactive dissemination of the knowledge that have already been produced by identifying the appropriate channels to distribute this know-how to the appropriate communities and reach the initiatives identified here and the stakeholders of them. Last but not least and according to ENISA’s Work Programme, the goal of supporting CSIRTs in the area of information security could take a concrete dimension if ENISA helps these organisations in the information sharing initiatives they take or may plan to take in the future. Such a supporting role could specifically take the form of, indicatively: 1) creation of CSIRTs working group that will tackle the matters of incident reporting and information sharing; 2) awareness raising, for example by the organisation of educational and training events around information sharing within the CSIRTs community; 3) dissemination of good practice on information sharing; 4) support the CSIRTs practically in the design of tools necessary to enhance the communication of information and transparency towards the stakeholder communities having to cooperate with the CSIRTs (model cyber-threat/cyber-incident notification forms, sample confidentiality/Non-Disclosure Agreements – NDAs, etc.).

A first step towards this direction could notably be the elaboration of a more in-depth study aiming at assessing the way of functioning, current results and working programmes of national and cross-border information sharing initiatives starting with the ones identified here. In tandem, or as next step, ENISA

[98] Relevant ENISA’s initiatives include, *inter alia*: Article 13a Expert Group; Electronic Communications Reference Group, as well as reports such as: ‘A flair for sharing – encouraging information exchange between CERTs’ (ENISA, 2011),and ‘Incentives and Challenges for Information Sharing in the Context of Network and Information Security’ (ENISA, 2010).

could envisage the launch of a project or initiative (in partnership with CSIRTs but also with other expert groups and market stakeholders) to build upon existing working tools related to information exchange (membership forms, contracts, NDAs, virtual tools, etc.) or to initiate work in this direction (as per point number 3) above). The output of such work could consequently benefit not only the CSIRT community but any initiatives, especially the less mature ones, in the information exchange and information sharing area.

On the other hand, public administrations and regulatory bodies should build upon the work produced in the field by EU institutions and bodies – including ENISA – and by the Member States, and leverage it while taking into account the national specificities, stakeholders' experiences, as well as the existence and performance of initiatives in their respective countries.

Recommendations for:

- EU and national policy makers (including administrative institutions as they have an influence and control on the policy and legislative framework of the law makers and regulators' behaviour);
- Regulatory and oversight bodies; and
- European Commission (e.g. DG Communications Networks, Content and Technology (DG CONNECT), DG Research and Innovation (DG RTD)) and ENISA as far it concerns to find ways to boost the interactive dissemination of the knowledge and good practices.

7.2.6 Encourage Cross-border Cooperation and Build Joint Initiatives at EU level without excluding an international reach whenever possible

The desk research and interviews conducted throughout this study have demonstrated that similar information sharing initiatives exist in several Member States. Dutch ISACs and UK IEs, or the Spanish *Foro ABUSES* and the Polish ABUSE Forum are noteworthy cases.

Member States and their respective organisations which have supported the set-up of the initiatives discussed herein (as well as the ones that may be in their infancy now in some Member States or the ones which will emerge in the future), such as CSIRTs, shall expand the competence of those initiatives, as well as procure them with the necessary financial and funding means, to liaise with their counter-parts cross-border, extend their memberships beyond the national borders and attract multinational participants (e.g. global corporations). Furthermore it appears that it would be more beneficial for organisations having a global footprint to engage in information sharing initiatives at international level instead of spreading funds, time and effort on many geographically dispersed and different local initiatives.

The exchange of knowledge, good practices and experience amongst the initiatives across borders could enhance information sharing in the cyber security area and create the foundations of pan-European or international information exchange schemes.

An interesting example for consideration will be the launch of the Connecting Europe Facility (CEF) Core Cooperation Platform / Core Service Platform for CSIRTs that is envisaged by the European Commission (DG CONNECT). Another illustration is represented by the cyber-related Coordinated and Support Actions[99]

[99] A Coordination and Support Action is "An action consisting primarily of accompanying measures such as standardisation, dissemination, awareness raising and communication, networking, coordination or support services, policy dialogues and mutual learning exercises and studies, including design studies for new infrastructure and may also include complementary activities of networking and coordination between programmes in different countries". See http://ec.europa.eu/research/participants/portal/desktop/en/support/reference_terms.html (last access 5 October 2015).

foreseen under the Horizon 2020 work programmes[100] by the European Commission (DG Research & Innovation).

Recommendation for:

- Member States;
- European Commission (e.g. DG Communications Networks, Content and Technology (DG CONNECT), DG Research and Innovation (DG RTD), DG Internal Market, Industry, Entrepreneurship and SMEs (DG GROW), DG Migration and Home Affairs (DG HOME), DG Joint Research Centre (DG JRC) and DG Energy (DG ENER));
- ENISA; and
- Current and future initiators, founders and facilitators of initiatives.

[100] See http://ec.europa.eu/programmes/horizon2020/en/what-work-programme (last access date: 5 October 2015)

8 Bibliography

Baldwin, R., Cave, M., & Lodge, M. (2012). Understanding Regulation: Theory, Strategy and Practice. *Oxford University Press*, p. 106. Retrieved April 25, 2015

belgiquelex.be - Banque Carrefour de la législation. (2012, July 10). *Loi portant des dispositions diverses en matière de communications électroniques (cité comme : loi Télécom).* Retrieved September 9, 2015, from http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2012071004&table_name=loi

Bradley, C. (2011, April 23). *EU Law: What is the Principle of Proportionality & Subsidiarity?* Retrieved April 15, 2015, from European Law Monitor: http://www.europeanlawmonitor.org/eu-legal-principles/eu-law-what-is-the-principle-of-proportionality-a-subsidiarity.html

BSA - The Software Alliance. (2015, January 1). *EU Cybersecurity Dashboard.* Retrieved April 16, 2015, from Finland: http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_finland.pdf

CERT-UK. (n.d.). *Cyber-security Information Sharing Partnership (CiSP).* Retrieved July 27, 2015, from CERT-UK: https://www.cert.gov.uk/cisp/

Council of the European Union. (2013, July 22). *Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Retrieved September 23, 2015, from http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012109%202013%20INIT

Deloitte. (2013, October 2015). *Cyber Security - The Perspective of information sharing*. Retrieved 13 April, from https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/The-perspective-of-information-sharing.pdf

Department for Business Innovation & Skills. (2015, March). *Better Regulation Framework Manual - Practical Guidance for UK Government Officials*. Retrieved April 13, 2015, from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/421078/bis-13-1038-Better-regulation-framework-manual.pdf

ENISA. (2009, June 13). *Good Practice Guide - Network Security Information Exchanges.* Retrieved April 15, 2015, from https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/good-practice-guide

ENISA. (2010, September 8). *Incentives and Challenges for Information Sharing in the Context of Network and Information Security.* Retrieved April 15, 2015, from https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/incentives-and-barriers-to-information-sharing

ENISA. (2011). *A flair for sharing – encouraging information exchange between CERTs.* Retrieved March 30 2015, from https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing/legal-information-sharing-1

ENISA. (2012). *Cyber Incident Reporting in the EU.* Retrieved from https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu

ENISA. (2014, October 28). *Work Programme 2015 - Including Multi-Annual Planning (ENISA Management Board Decision of 28 Ocotber 2014).* Retrieved March 16, 2015, from https://www.enisa.europa.eu/publications/programmes-reports/enisa-work-programme-2015

ENISA. (2014a). *Scalable and Accepted Methods for Trust Building in Operational Communities*. Retrieved from https://www.enisa.europa.eu/activities/cert/support/information-sharing/scalable-and-accepted-methods-for-trust-building

ENISA. (2014b). *Report on Cyber Crisis Cooperation and Management.* Retrieved from https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/ccc-management/ccc-study

ENISA. (2015a). Tender Specifications - Re-Opening of competition under multiple framework contracts "Supporting the CERT community" F-COD-13-C22. p.6.

ENISA. (2015b, September). *ENISA – CERT Inventory.* Retrieved September 9, 2015, from Inventory of CERT teams and activities in Europe: https://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

ENISA. (2015c). *EP3R 2009-2013 Future of NIS Public Private Cooperation.* Retrieved from https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r/ep3r-2009-2013

ENISA. (n.d.). *Glossary.* Retrieved April 13, 2015, from https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary

ENISA. (n.d.(a)). *National/governmental CERTs - Baseline Capabilities.* Retrieved September 9, 2015, from ENISA website: https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities

ENISA. (n.d.(b)). *European Financial Institutes – Information Sharing and Analysis Centre, A Public-Private Partnership.* Retrieved September 3, 2015, from ENISA website: https://www.enisa.europa.eu/activities/cert/support/information-sharing/european-fi-isac-a-public-private-partnership

Estonian Ministry of Interior. (2009, June 15). *EMERGENCY ACT.* Retrieved April 13, 2015, from http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXXXX26&pg=1&tyyp=X&query=H%E4daolukorra+seadus&ptyyp=RT&keel=en

Estonian Ministry of Interior. (2013, March 14). *Security measures for information systems of vital services and related information assets.* Retrieved July 14, 2015, from https://www.ria.ee/public/KIIK/Security_measures_for_information_systems_of_vital_services_and_related_information_assets.pdf

Eur-Lex. (2010, March 3). *The principle of subsidiarity.* Retrieved April 15, 2014, from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:ai0017

European Commission - DG Enterprise and Industry. (2008, December 8). *Standardisation mandate to the European standardisation organisations CEN, CENELEC and ETSI in the field of Information and Communication Technologies applied to Radio Frequency Identification (RFID) and systems*. (European Commission) Retrieved April 24, 2015, from ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Fields/ICT/RFID/M436.pdf

European Commission. (2013, February 07). *Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Retrieved March 27, 2015, from JOIN(2013) 1 final: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

European Commission. (2013a, February 7). *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*. Retrieved March 25, 2015, from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013PC0048&from=EN; Latest official version available on European Parliament Legislative Observatory at http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0244&language=

European Commission. (2013b, February 07). *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 NIS across the Union*. Retrieved March 25, 2015, from EU Cybersecurity plan to protect open internet and online freedom and opportunity: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1669

European Commission. (2014a, Novembre 25). *CONNECTING EUROPE FACILITY (CEF) - TRANS-EUROPEAN TELECOMMUNICATIONS NETWORKS - WORK PROGRAMME 2015.* Retrieved September 9, 2015, from http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/1_en_annexe_acte_autonome_part1_v2.pdf

European Commission. (2014b, December 18). *CONNECTING EUROPE FACILITY (CEF) - TRANS-EUROPEAN TELECOMMUNICATIONS NETWORKS - WORK PROGRAMME 2014.* Retrieved September 9, 2015, from http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=8329

European Commission. (2014c, September 16). *Preparatory activities for the launch of the connecting Europe facility (CEF) core cooperation platform for computer emergency and response teams in the European Union - SMART 2014/1079 - Tender Specifications.* Retrieved September 9, 2015, from http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=6834

European Commission. (2015, May 19). *Better Regulation - Tool #15: The choice of policy instruments*. Retrieved April 30, 2015, from http://ec.europa.eu/smart-regulation/guidelines/tool_15_en.htm

European Commission. (n.d.). *Better Regulation "Toolbox".* Retrieved from http://ec.europa.eu/smart-regulation/guidelines/docs/br_toolbox_en.pdf

European Parliament and the Council. (2002, July 12). *DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).* Retrieved September 21, 2015, from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:HTML

European Parliament and the Council. (2009, November 27). *DIRECTIVE 2009/140/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 amending Directives 2002/21/EC.* Retrieved September 15, 2015, from http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/140framework_5.pdf

European Parliament and the Council. (2012a, July 12). *DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.* Retrieved September 9, 2015, from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:HTML

European Parliament and the Council. (2012b, October 25). *REGULATION (EU) No 1025/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 October 2012 on European standardisation.* Retrieved September 9, 2015, from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:316:0012:0033:EN:PDF

European Parliament and the Council. (2013, June 18). *REGULATION (EU) No 526/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 (Text with EEA relevance)*. (Official Journal of the European Union) Retrieved April 27, 2015, from http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:JOL_2013_165_R_0041_01&qid=1397226946093&from=EN

European Parliament and the Council. (2014, July 23). *REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.* Retrieved September 15, 2015, from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN

European Parliament and the Council. (2015, May 11). *DECISION No 854/2005/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2005 establishing a multiannual Community Programme on promoting safer use of the Internet and new online technologies (Text with EEA relevance).* Retrieved September 9, 2015, from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005D0854&from=EN

European Parliament, Council. (2013, August 12). *Directive on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.* Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:en:PDF

Eurostat. (2008). *METADATA - Statistical Classification of Economic Activities in the European Community, Rev. 2 (2008).* Retrieved April 3, 2015, from RAMON - Reference And Management Of Nomenclatures: http://ec.europa.eu/eurostat/ramon/nomenclatures/index.cfm?TargetUrl=LST_NOM_DTL&StrNom=NACE_REV2

FARLEX. (n.d.). *The Free Dictionary.* Retrieved April 13, 2015, from http://www.thefreedictionary.com/regulatory

Federal Trade Commission. (1998, July 21). *FTC Tells House Subcommittee that Self-regulation Is the Preferred Method of Protecting Consumers' Online Privacy.* Retrieved April 13, 2015, from https://www.ftc.gov/news-events/press-releases/1998/07/ftc-tells-house-subcommittee-self-regulation-preferred-method

FRALEX. (2009, March). *Thematic Study on the assessment of data protection measures and relevant institutions in Slovakia.* Retrieved September 9, 2015, from http://fra.europa.eu/sites/default/files/role-data-protection-authorities-2009-sk.pdf

FS-ISAC. (n.d.). *About FS-ISAC.* Retrieved April 30, 2015, from Financial Services - Information Sharing and Analysis Center: https://www.fsisac.com/about

German Parliament. (2015, February 25). *Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz).* Retrieved July 17, 2015, from http://dip21.bundestag.de/dip21/btd/18/040/1804096.pdf

Information Commissioner. (2015, January 13). *Electronic Communications Act - Official Gazette RS, no 109/12, 110/13, 40/14 - ZIN-B, and 54/14 - Decision of the Constitutional Court no. U-I-65/13.* Retrieved September 9, 2015, from https://www.ip-rs.si/index.php?id=504

InterActive Terminology for Europe. (2014, November 25). *Regulation - Source of law*. Retrieved June 15, 2015, from http://iate.europa.eu/FindTermsByLilId.do?lilId=48635&langId=en

Internation Organization for Standardization (ISO). (2012). *Information technology — Security techniques — Guidelines for cybersecurity (BS ISO/IEC 27032:2012).* Retrieved April 25, 2015, from http://www.iso.org/iso/catalogue_detail?csnumber=44375

International Organization for Standardization (ISO). (2011, September 1). *Information technology — Security techniques — Information security incident management (ISO/IEC 27035:2011)*. (International Organization for Standardization (ISO)) Retrieved April 13, 2015, from http://www.iso.org/iso/catalogue_detail?csnumber=44379

International Organization for Standardization (ISO). (2012a, April 01). *Information technology - Security techniques - information security management for inter-sector and inter-organizational communications (BS ISO/IEC 27010:2012)*. (British Standards Insitution (BSI)) Retrieved April 25, 2015, from http://shop.bsigroup.com/ProductDetail/?pid=000000000030204594

International Organization for Standardization (ISO). (2012b, August 15). *Information technology - Security techniques - Guidelines for cybersecurity (ISO/IEC 27032:2012)*. Retrieved April 25, 2015, from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44375

ITIL (IT Service Management). (2007, May 30). *Glossary of Terms, Definitions and Acronyms*. (ITIL) Retrieved April 2015, 2015, from http://www.best-management-practice.com/gempdf/itil_glossary_v3_1_24.pdf

Jones Day. (2014, January). *Europe Proposes New Laws and Regulations on Cybersecurity.* Retrieved April 23, 2015, from http://m.jonesday.com/europe-proposes-new-laws-and-regulations-on-cybersecurity-01-02-2014/

Latvian Presidency of the Council of the European Union. (n.d.). *Latvian Presidency reaches a breakthrough in talks with EP on network and information security.* Retrieved September 21, 2015, from https://eu2015.lv/news/media-releases/2489-latvian-presidency-reaches-a-breakthrough-in-talks-with-european-parliament-on-network-and-information-security

Legifrance. (2013, December 23). *LOI n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale (Article 22).* Retrieved September 9, 2015, from Legifrance: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825

Millar, T. (.-C. (2015, June 17). *Traffic Light Protocol (TLP) - BoFReturn to TOC.* Retrieved September 14, 2015, from FIRST (Berlin) - Conference Program: https://www.first.org/conference/2015/program#ptraffic-light-protocol-tlp-bof

Ministerie van Economische Zaken. (2008, August 28). Handboek - Nationaal Continuïteitsoverleg - Telecommunicatie - Bijlagen. *http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/wob-verzoeken/2013/08/12/handboek-nationaal-continuiteitsoverleg-telecommunicatie-versie-1-3/handboek-nco-t-bijlagen-versie-1-3.pdf*, p.8. Retrieved from http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/wob-verzoeken/2013/08/12/handboek-nationaal-continuiteitsoverleg-telecommunicatie-versie-1-3/handboek-nco-t-bijlagen-versie-1-3.pdf

Ministry of Transport and Communications, Finland. (2014). *Information Society Code (917/2014).* Retrieved June 15, 2015, from https://www.finlex.fi/fi/laki/kaannokset/2014/en20140917.pdf

Mitrakas, A., & Portesi, S. (2007). Regulating Information Security: A Matter of Principle? *ISSE/SECURE 2007 Securing Electronic Business Processes*, 3-17.

OECD. (2012). *Recommendation of the Council on Regulatory Policy and Governance.* Retrieved April 20, 2015, from http://www.oecd.org/gov/regulatory-policy/49990817.pdf

OECD, G. H. (n.d.). OECD Report - Alternatives to traditional regulation. p.6.

Republic of Estonia - Information System Authority. (2014). *Annual Report Cyber Security - Branch Of the Estonian Information System Authority.* Retrieved June 15, 2015, from https://www.ria.ee/public/Kuberturvalisus/RIA-Kyberturbe-aruanne-2014_ENG.pdf

Robinson, N., & Disley, E. (2010, September 08). *Incentives and Challenges on Information Sharing*. Retrieved March 30, 2015, from http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/incentives-and-barriers-to-information-sharing

RTT. (2015). *About RTT.* Retrieved June 27, 2015, from RTT - Communications Regulatory Authority of the Republic of Lithuania: http://www.rrt.lt/en/about_rrt.html

Stupp, C. (2015). *Oettinger: Deal on cybersecurity directive close*. Retrieved from http://www.euractiv.com/sections/digital/oettinger-deal-cybersecurity-directive-close-319325

Annex 1 - Acronyms

Key acronyms used:

- **CEF:** Connecting Europe Facility
- **CERT:** Computer Emergency Response Team
- **CIIP:** Critical Information Infrastructure Protection
- **CIP:** Critical Infrastructure Protection
- **CSDP:** the Common Security and Defence Policy
- **CSIRT:** Computer Security Incidents Response Team
- **CSS:** Cyber Security Strategy
- **DG:** Directorate-General
- **EEA:** European Economic Area
- **EFTA:** European Free Trade Association
- **ICT**: Information and Communication Technologies area
- **IEs:** Information Exchanges
- **ISAC:** Information Sharing and Analysis Center
- **MS:** Member State
- **n.d.:** no date
- **NACE:** *Nomenclature des Activités Économiques dans la Communauté Européenne*
- **NIS:** Network and Information Security
- **NLO:** National Liaison Officer
- **PIIE**: Pharmaceutical Industries Information Exchange
- **SMEs**: Small and Medium-sized Enterprises
- **TLP:** Traffic Light Protocol
- **WSIE**: Water Security Information Exchange

Other acronyms found – some used only once, often names of organisation and explained fully within text:

- **ACDC:** European Advanced Cyber Defence Centre
- **ATC:** Austrian Trust Circle
- **ANSSI:** National Agency for Information Systems Security, France
- **AIIC:** Associazione italiana esperti in infrastructure critiche
- **BAIT:** Bulgarian Association of Information Technologies
- **BBK:** Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe
- **BELNIS:** Belgian Network and Information Security
- **BSI:** Bundesamt für Sicherheit in der Informationstechnik
- **DEG:** Information Technology and Information Systems Security Experts Group
- **CCSIR:** Cyber Security Research Center
- **CIP:** Critical Infrastructure Providers
- **CCI:** Industrial Cybersecurity Centre
- **CDSE:** Club des directeurs de sécurité des entreprises
- **CEPOL:** European Police College
- **CiSP:** Cyber-security Information Sharing Partnership
- **CPNI:** Centre for the Protection of National Infrastructure

- **CTISRP:** Cyber Threat Intelligence Research Project
- **CYSPA:** European Cyber Security Protection Alliance
- **CZ NSA:** national authority for cybersecurity in the Czech Republic
- **DENSEK:** Distributed Energy Security Knowledge
- **DG CONNECT:** European Commission DG Communications Networks, Content and Technology
- **DG RTD:** European Commission DG Research and Innovation
- **DG GROW:** European Commission DG Internal Market, Industry, Entrepreneurship and SMEs
- **DSI:** Digital Service Infrastructure
- **E3CC:** Energy Emergencies Executive Committee Cyber
- **ENISA:** European Union Agency for Network and Information Security
- **EU:** European Union
- **EC3:** Europol/European Cybercrime Centre
- **EDA :** European Defence Agency
- **EEAS:** European External Action Service
- **EIDAS:** Electronic identification and trust services (eIDAS) Regulation
- **EMEA:** Europe, Middle East and Africa
- **ECRG:** ENISA Electronic Communications Reference Group
- **FCC:** Federal Communication Commission, US
- **FICORA:** Finnish communications regulatory activity authority
- **FIDI:** Forum for information sharing
- **FTC:** Federal Trade Commission
- **INCIBE:** Instituto Nacional de Ciberseguridad
- **(ISC)^{2}®:** International Information System Security Certification Consortium, Inc.
- **ISCD:** Conference on Information Security and Cyber Defence
- **ISO:** International Organization for Standardization
- **ISMS:** Association for the Advancement of Information Security
- **ISP:** Internet Service Providers
- **JWGI:** Joint Working Group Initiative
- **MoU**: Memorandum of Understanding
- **NCSC:** Nationaal Cyber Security Centrum
- **NDA:** Non-Disclosure Agreements
- **OECD:** Organisation for Security and Cooperation in Europe
- **OVI:** Operators of Vital Importance
- **TISAC:** Telecommunications Industry Security Advisory Council
- **TNCEIP:** Thematic Network on Critical Energy Infrastructure Protection
- **TSIE:** Transport Sector Information Exchange
- **UK NSIE:** UK Network Security Information Exchange
- **UP KRITIS:** Kooperation zwischen Betreibern Kritischer Infrastrukturen
- **VDI:** Varslingssystem for digital infrastruktur
- **WPK:** Work Package

Annex 2 - Sample Questionnaire Used for the Interviews with a Selected Group of Stakeholders Involved in Information Sharing Initiatives

The below represents the questionnaire that was used as a basis to conduct the interviews. This questionnaire was further customised based on the experience and the activity sector of the interviewee.

NR.	QUESTION
1.	**a) With whom do you share information on cyber incidents?** Do you share information on cyber incidents with private companies, public organisations, government agencies, peers, etc.? *An cyber incident might be:* ▪ *Cyber attack* ▪ *identity theft* ▪ *fraud* ▪ *cyber disruption* Answer: **b) Are you and these organisations part of the same sector?** Is the shared information sector-related? Answer:
2.	**Do you share information on cyber incidents with other sectors?** *Possible other sectors might be:* ▪ *Energy* ▪ *Transportation* ▪ *Health* ▪ *Finance and banking* ▪ *Internet Services* ▪ *Public administration* ▪ *etc.* Answer:
3.	**Which regulatory approaches/legal bases do you use to share information on cyber incidents?** **In which circumstances do these apply?** **Are these approaches sector-specific?** *Regulatory approaches might be:* ▪ *Mandatory disclosure (e.g. you are obliged to share information in certain situations)* ▪ *Administrative measures (e.g. you receive a subsidy that makes you share information with peers or you pay taxes/charges if you don't share information)* ▪ *Co-regulation (e.g. your organization and your peers help the government to create a regulatory environment by sharing information)* Answer:
4.	**Which non-regulatory approaches do you use to share information on cyber incidents?**

NR.	QUESTION
	Are these approaches sector-specific? *Non-regulatory approaches might be:* - *Voluntary approach (e.g. you are committed to share information beyond what the regulation requires)* - *Awareness-raising (e.g. your organization tries to educate the public on the different ways to share information and the benefits of it)* Answer:
5.	**What challenges do you face to share information on cyber incidents in your sector?** **What approach do you use to face these challenges?** Answer:
6.	**Do you know any other stakeholders to could be contacted in the field of our study?** **Could you share relevant links with us?** Answer:

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 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

TP-04-15-690-EN-N

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

ISBN: 978-92-9204-131-1
DOI: 10.2824/43639