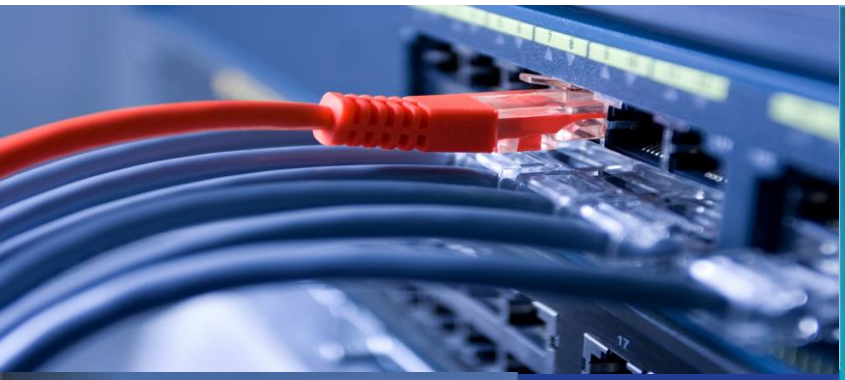

Stocktaking, Analysis and Recommendations on the Protection of CIIs

JANUARY 2016

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

Sarri Anna, Secure Infrastructure & Services Unit, ENISA

Moulinos Konstantinos, Secure Infrastructure & Services Unit, ENISA

Contact

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

Acknowledgements

This study was contacted under contract with KPMG Germany.

Special thanks to **Pillokeit Pascal Dustin** and **Weissmann Paul** from KPMG for their continuous efforts and great work!

We would like to acknowledge all the experts that provided input for this report and especially:

Andreas Reichard, Federal Chancellery, AT

Anita Tikos, National Electronic Information Security Authority, HU

Anna Passeggia, Ministry of Economic Development, IT

Antonis Antoniades, Electronic Communications and Postal Regulation, CY

Barend Sluijter, Ministry of Interior, NL

Daniel Bagge, National Security Authority, CZ

Elīna Neimane, Ministry of Defence, LV

Illes Solt, National Information Security Authority Ministry of Interior, HU

Krzysztof Silicki, NASK Institute, PL

Liina Areng, Estonian Information System Authority (RIA), EE

Maciej Pyznar, Government Centre for Security, PL

Magdalena Wrzosek, Ministry of Administration and Digitization, PL

Martin Konečný, National Security Authority, CZ

Peter Knøster, Danish Defense Intelligence Service Centre for Cyber Security, DK

Peter Wallström, The Swedish Post and Telecom Authority (PTS), SE

Sápi Gergely, National Information Security Authority,

Sandro Mari, Ministry of Economic Development, IT

Stefanie Frey, MELANI, CH

Timo Mischitz, Federal Chancellery, AT

Timo Kievari, Ministry of transport and communications, FI

Urmo Sutermäe, Estonian Information System Authority (RIA), EE

Uwe Jendricke, German Federal Office for Information Security (BSI), DE

Vereckei Béla Ferenc, National Information Security Authority Ministry of Interior, HU

Yann Salamon, French Network and Information Security Agency (ANSSI), FR

ISBN 978-92-9204-136-6, doi: 10.2824/534303

Table of Contents

Executive Summary

The internet and other digital technologies as well as its underlying network and information systems are the backbone of the European Society and the Digital Single Market. Many critical sectors operating in the European Member States such as the energy, transportation or financial sectors rely on critical information infrastructure (CII). The Threats to CII, which stem from different sources ranging from national actors to criminal hackers, have increased in recent years. In order to fully meet the emerging threats to CII, ENISA offers assistance to EU Member States and the EU Commission.

This study contributes to the improvement of the protection of critical infrastructure in Member States by taking stock of and analysing existing measures deployed in the field across several EU Member States. The goal is to provide a set of good practices and recommendations to national authorities and lawmakers which will contribute to stronger and more resilient CII in EU Member States and decrease the risk of disruption or failure of critical infrastructure.

The introduction identifies six action areas for Member States, which contribute to an effective national protection of CII (CIIP). These action areas include comprehensive policies and legislations, but also effective national governance structures during day-to-day operations and in cases of emergency. Information sharing between the private and the public sector and threat intelligence constitute important elements in CIIP, since critical information infrastructure is mainly owned by the private sector.

This study presents some key findings, uncovers the different governance structures for CIIP in seventeen EU Member States and one EFTA country along with different good practices. In addition, it presents general findings, based on collected information via interviews and online surveys:

- Surveyed EU Member States have delegated responsibility to **cyber security authorities, emergency agencies or national regulators**. Only a minority of the examined Member States have tasked intelligence agencies or information security forums with CIIP
- **Almost all national authorities for CIIP are responsible for operational tasks** (for example: PoC for incident reporting, organising exercises, incident response). Two thirds of the authorities are responsible for **additional tasks on the strategic or political level**, such as the development of strategy papers, supervision of the national CSIRT or the proposing legislation.
- **Cooperation with the private sector tends to be high**, but only around 56 Percent of the examined Member States have established institutionalised forms of cooperation in forms of public-private partnerships
- **Legalisation and corresponding obligations for CII-operators vary across sectors**. The critical sectors with the strongest regulations across all analysed Member States are the **Telecommunications, Finance and Energy sectors**
- **The majority of countries have conducted a risk assessment on a national level** (or are planning to do so). Other countries have decided that risk assessment is the responsibility of sector-specific agencies or of the individual operators.
- Three profiles of CIIP-governance have been identified: A **centralised, a decentralised and a co-regulation approach**.

Finally, the study makes general recommendations to EU Member States and the EU Commission on how to improve CIIP in the European Union. The recommendations are the following:

Member States

- Recommendation 1: Increase institutionalised cooperation with private stakeholders
- Recommendation 2: Align management structure for CIIP with existing national crisis and emergency management structures
- Recommendation 3: Participate in or host international exercises
- Recommendation 4: Establish mandatory security incident reporting
- Recommendation 5: Conduct national risk assessment
- Recommendation 6: Utilize best legal framework practices for CIIP across critical sectors
- Recommendation 7: Examine if positive incentives can be provided to operators of CII to invest in security measures

European Commission

- Recommendation 8: Define baseline requirements in order to support the development of CIIP in MS
- Recommendation 9: Develop and conduct a maturity assessment of Member States' CIIP readiness
- Recommendation 10: Support information sharing and the exchange of knowledge between EU Member States' national CSIRTs
- Recommendation 11: Identify European Critical Information Infrastructure

List of Figures

List of Abbreviations

ABBREVATION	DESCRIPTION
ANSSI	Agence nationale de la sécurité des systèmes d'information (France)
CERT	Computer Emergency Response Team
CII	Critical Information Infrastructures
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CIWIN	Critical Infrastructure Warning Information Network
Crisis Act	Act no. 240/2000 Coll., on Crisis Management
CSIRT	Computer Security Incident Response Team
ECI	European Critical Infrastructure
EFTA	European Free Trade Association
ENISA	European Network and Information Security Agency
EPCIP	European Programme for Critical Infrastructure Protection
EU	European Union
ICS	Industrial Control Systems
ICT	Information and Communication Technology
ISAC	Information Sharing and Analysis Centre
IWWN	International Watch and Warning Network
LPM	Military Programming Law (France)
MS	Member States (EU)
MSB	Swedish Civil Contingencies Agency (Sweden)
NASK	The Research and Academic Computer Network (Poland)
NCSC	National Cyber Security Centre (Netherlands)
NCTV	National Coordinator for Security and Counterterrorism (Netherlands)
NIS	Network and Information Security
OIV	Operators of vital importance (France)
PoC	Point of Contact
PPPs	Public-private partnerships
PTS	Swedish Post and Telecom Agency
SAMFI	Cooperation Group for Information Security (Sweden)
SCADA	Supervisory Control and Data Acquisition

1. Introduction

Overview

The internet and other digital technologies as well as its underlying network and information systems are the backbone of the European Society and the Digital Single Market. Millions of EU citizens and many businesses rely on the information and communication infrastructure for a variety of services. These range from energy and telecommunications to e-government, healthcare, and logistics. That is why disruption or failure of this "critical infrastructure" can have dire consequences, ranging from the loss of money and reputation for companies to the disruption of the provision of goods and essential services to the general population.

In order to fully meet the emerging threats to critical information infrastructures (CII), ENISA offers assistance to EU Member States and the EU Commission. The agency helps to understand the current threat landscape with regard to CII, Smart Grids and ICS-SCADA (Industrial Control Systems-Supervisory Control and Data Acquisition) among others. Furthermore, Cyber Europe has become an important multi-national and multi-stakeholder cyber exercises for EU Member States. Many Member States in the European Union have started to develop and implement different measures for the protection of critical information infrastructure in their country. These measures range from the establishment of national coordinating bodies to the development of national emergency plans or the adoption of specific legal frameworks. ENISA has supported these efforts in the past by defining good practices in areas like cyber security strategies and national contingency plans or by analysing different methods for the identification of critical infrastructure[1][2][3].

This study contributes to the improvement of the protection of critical infrastructure in Member States by taking stock of and analysing existing measures in this field across several EU Member States. The goal is to provide a set of good practices and recommendations to national authorities, lawmakers and the European Commission which will contribute to a stronger and resilient CII in EU Member States and decrease the risk of disruption or failure of critical infrastructure.

Policy context

The EU aims to support its Member States in the protection of critical infrastructure. In order to align efforts and foster cooperation, the EU has adopted specific programmes and directives:

The protection of critical infrastructure was first put on the agenda in June 2004, when the European Council asked for the preparation of an overall strategy. At that time, the main concern was the protection against terrorist attacks. In November 2005, the Commission adopted a Green Paper on a European Programme for Critical Infrastructure Protection (EPCIP) (European Commission 2005). On request of the Justice and Home Affairs Council in December 2005, the EU Commission made a proposal for an EPCIP (European Commission 2006): Purpose of the EPCIP is the improvement of the protection of critical infrastructure in the EU against

[1] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide
[2] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber_exercises/national-exercise-good-practice-guide
[3] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/Methodologies-for-identification-of-ciis

different types of threats (all-hazard approach). The legislative framework of the EPCIP consists of measures designed to facilitate the implementation of EPCIP. This includes an EPCIP action plan, the Critical Infrastructure Warning Information Network (CIWIN), the setting up of Critical Infrastructure Protection (CIP) expert groups at EU level, CIP information sharing processes, and the identification and analysis of interdependencies. A key component is the procedure for identifying and designating European Critical Infrastructure (ECI). This has been implemented by means of the 2008 Directive on European Critical Infrastructures (Council of the European Union 2008)[4], which however only applies to the energy and transport sectors. An updated approach to the EU CIP policy is currently under development and preliminary results have been summarised in the 2013 Staff Working Document[5] on a new approach to the European Programme for Critical Infrastructure Protection (European Commission 2013a).

In order to strengthen the critical infrastructure against the various threats and to uphold the trust of the EU citizens, the European Commission has proposed the Network and Information Security Directive (NIS Directive) in 2013 (European Commission 2013b). The NIS Directive is currently in negotiations between the European Parliament and the Council. The aim is to improve the EU Member States' national cybersecurity capabilities, enhancing the cooperation between the Member States, the public and the private sector while also requiring companies in critical sectors to report major incidents to national authorities and to adopt risk management practices.

A legal framework for attacks against information systems has been set by the Council Framework Decision 2005 (Council of the European Union 2005) and its replacement Directive 2013/40/EU (European Parliament, Council of the European Union 2013)[6]. The objectives of this frameworks are to approximate the criminal law of the EU Member States in this area. For this purpose the Directives establish definitions of criminal offenses and sanctions. Furthermore, cooperation between law enforcement agencies and EU Agencies and bodies such as Eurojust, Europol and its European Cyber Crime Centre, and ENISA shall contribute to this improvement through measures such as the exchange of information.

Scope of the document

This study focuses on Critical **Information** Infrastructure Protection (CIIP), rather than Critical Infrastructure Protection (CIP). Both terms are often used interchangeably, which creates difficulties for researchers and policy makers to clearly distinguish between them. In general, CIIP can be seen as an essential part of the comprehensive efforts for CIP. While CIP covers the protection of a nation's infrastructure across various sectors, CIIP focusses on the protection of the underlying information infrastructure. CII is comprised of a physical component (networks, wires, satellites, computers etc.) and an immaterial component, which is the actual information transported by and through the physical components.

CIIP is also an integral part of many cyber and information security strategies. Cybersecurity covers a broad spectrum of ICT-related security issues, of which the protection the CII is an integral part (Myriam Dunn Cavelty 2012).

[4] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008L0114&from=EN

[5] http://ec.europa.eu/dgs/home-affairs/pdf/policies/crisis_and_terrorism/epcip_swd_2012_190_final.pdf

[6] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32013L0040&from=EN

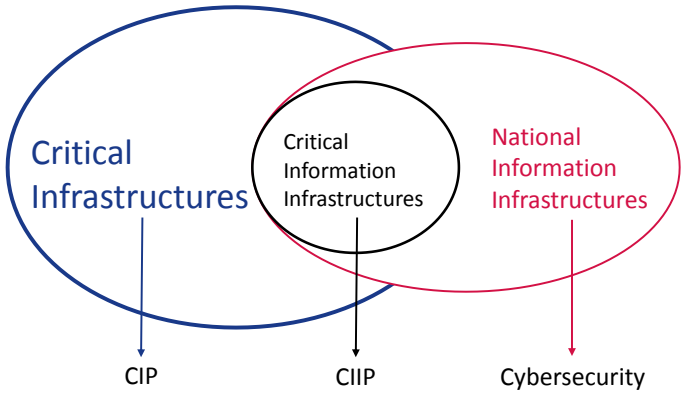

Figure 1-1 – CIP/CIIP/Cybersecurity. Adapted from: Dunn Cavelty, The Art of CIIP Strategy 2012. p. 20[7]

Because of the conceptual overlap between CIP, CIIP and cyber/information security, data gathering and analysis of policies and documents was conducted in all areas.

In order to analyse CIIP, this study makes use of a holistic understanding of CIIP that includes different aspects. CIIP in a national context is understood as an interplay of different areas of action that contribute to an effective national CIIP. These action areas are:

- Policy
- Governance structure
- Legislation
- Risk management and mitigation measures
- Emergency preparedness
- Threat intelligence and information sharing

Policy means the development of strategic, policy or other white papers that outline strategic priorities, focal points, goals, measures and defined roles and responsibilities of public and private stakeholders.

The Governance structure refers to the implementation of the defined roles and responsibilities in the area of CIIP. This includes the development of public agencies with responsibility for CIIP or the extension of existing authorities. It also includes the establishment of communication channels and cooperation mechanisms between public and private agencies.

Legal obligations and requirements are an important tool for Member States to ensure that public and private operators of CII adhere to a certain security standard. These can include mandatory security standards, incident reports or audits.

Emergency preparedness refers to different measures to ensure appropriate incident handling in case of national information security incidents. Regular exercises for CIIP, national risk assessments and national incident management systems are all part of appropriate emergency preparedness. Computer Emergency Response Teams are an essential pillar of CIIP on an operational level and offer expertise and advise to operators of CII.

[7] In the study we are trying to understand how CIIP is conceived on a national level. Nevertheless, critical information infrastructures are not only national infrastructures.

Threat intelligence and information sharing is carried out by the respective national authorities and the asset owners and refers to the monitoring of the threat landscape with regards to the cyber threats and threats to CI. Information about threats have to be disseminated to the relevant stakeholders such as operators of CII.

All action areas contribute to strong national CIIP.

The goal of this study is twofold: The first step is to take stock of existing practices and policies in the different described areas of CIIP amongst Member States. The second step is to analyse the data with the goal of identifying good practices and to create different profiles of the national CIIP measures. Based on the analysis, a list of recommendations on how to improve national CIIP will be created. The overall goal is to contribute to the improvement of CIIP amongst Member States and thus of the European Union.

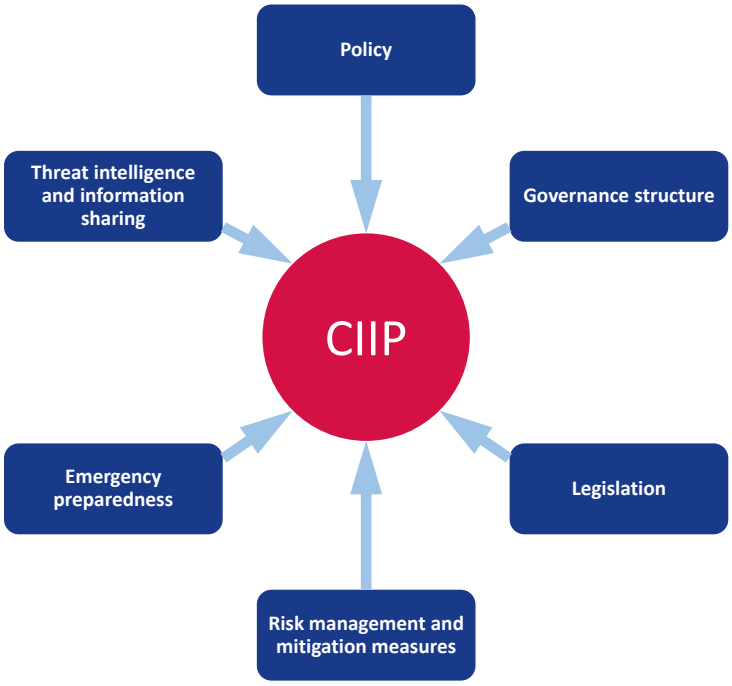

Figure 1-2 – Action Areas of CIIP

Target audience

The target audience is governmental authorities, the European Commission and the CIIP community at large. This document is specifically aimed at Member States that are at the beginning of CIIP structure development or are looking to further improve existing structures. Decision makers in mandated national agencies with responsibilities in the area of CIIP and lawmakers in charge of drafting legal frameworks with the goal of protecting critical information infrastructure can benefit from the insights and results offered by this study.

Structure of this document

This document is structured as follows:

- Chapter 1 – Introduction and general overview

- Chapter 2 – Describes the analytical framework and the process of data gathering
- Chapter 3 – Presents the key findings: The governance of CIIP and good practices in EU MS
- Chapter 4 – Identifies different CIIP profiles among the EU MS
- Chapter 5 – Presents the lessons learnt and final recommendation of the study

Methodology

In accordance with the methodology named above, stock taking and information gathering has been performed for seventeen different EU Member States and one EFTA country by the use of desk research, online surveys and personal interviews. To facilitate comparison, the protection of CII has been analysed by means of the following categories:

- Framework for CIIP
- Preparation for emergencies on a national level
- Governmental authorities and other relevant actors
- Computer Security Incident Response Team (CSIRT)
- Legal obligations and requirements

“Framework for CIIP” includes research on national strategies or comparable policy papers for CIIP that have been developed and put in place. It is assessed whether threats and risks to CII are outlined in an official document and if strategic goals and objectives are set out on an official basis. In addition, a methodology for the identification of CII should have been developed and applied and a framework for CIIP, i.e. through regulations, guidelines, measures good practices etc., should have been established.

“Preparation for emergencies on a national level” examines if a risk assessment plan for CII-related security incidents on a national level has been developed. It is also checked whether the roles and responsibilities of various actors during a national crisis or security incident are defined and if regular trainings and exercises for CIIP are carried out. To support information exchange on a national level, a multisource information platform for CII awareness, crisis management and emergency response could be used.

“Governmental authorities and other relevant actors” evaluates if roles and responsibilities of governmental agencies and the private sectors are defined. A governmental agency should have been designated to act as the main national authority for CIIP, which includes authorisation to issue binding instructions to companies and governmental authorities. In addition, it is assessed whether institutionalised forms of cooperation between the public and private sector as well as between different authorities or institutions with a role in CII protection have been established. Beyond this, awareness raising or similar training programmes related to CIIP should also have been developed and put in place.

“Computer Security Incident Response Team (CSIRT)” determines if CIIP has been assigned to a national or governmental CSIRT or if one has been set up for this purpose, as well as if the CSIRTs are under the supervision of a national authority.

“Legal obligations and requirements” focuses on the operators of CII and analyses whether they are obligated to notify an authority about security incidents as well as to implement appropriate technical and organisational security measures. It is also evaluated if they are pledged to undergo an external security audit and/or conformity or compliance tests and if incentives could be given to CII operators to invest in security.

Key findings: The collected data will be analysed and interpreted. We will look for similarities and differences in measures for CIIP. The focus will be on measures in the described action areas (see Figure 2).

Profile development: The focus here is on the governance structure of CIIP in the individual Member States. We will analyse roles and responsibilities of public and private actors, as well as modes of governance and steering in the issue area of CIIP.

Online Survey

ENISA developed an online survey to assess protection measures for CII in different EU Member States. The survey consists of fifteen questions, which are to some extent dependant on one another. The survey covers similar broader topics like the organisational structure of authorities or agencies, mechanisms for incident reporting and investigation, national exercises for CIIP, cooperation mechanisms and obligations and incentives. For the full survey form, refer to Appendix A.

The survey took place between May and July 2015. It was made available via an online platform provided by EUSurvey, and has been answered by representatives of thirteen EU Member States.

Interview Questionnaire

ENISA has developed an interview questionnaire to assess protection measures for CII in different EU Member States. The questionnaire contains seventeen questions which cover the five described categories. For the full interview questionnaire, refer to Appendix B.

Interviews were conducted between May and August 2015. They took place in the form of personal conversations or were answered in written form. In total, representatives of the national authorities for CIIP of sixteen EU Member States were interviewed.

2. Key Findings

The key findings are the result of a detailed analysis made on the different governance structures for CIIP in fifteen EU Member States and one EFTA country. The specific analysis can be found on a separate report under the title: "CIIP Governance in the EU Member States".

2.1 Good Practices

This chapter identifies exemplary good practices in CIIP among EU Member States in the areas of information sharing schemes between public and private actors, CII emergency preparations, and obligations and requirements for operators of CII.

Examples of Member States that have developed good practice in a certain area or field will be provided. The list of examples is not exhaustive and should only serve as an inspiration for other EU Member States.

2.1.1 Partnership with Private Stakeholders

ICT structures across sectors are mostly owned by private companies, which means that cooperation of public institutions with CII operators is essential in order to ensure the knowledge on current threats is up to date and to ensure quick support in incident response, if needed.

The Netherlands are a good example for strong partnership with the private sector. The National Cyber Security Centre (NCSC) serves as a focal point for a number of public-private partnerships. Within the NCSC, several partnerships have been established for the purpose of Detection, Response and Analysis of threats. In addition, the Cyber Security Council, made up of representatives from public and private parties, serves as an independent advisory board. Thereby, the NSCS ensures a close partnership with private stakeholders on a strategic and operational level (2015h).

Another example for close collaboration with the private sector is Austria. Austria has set up a Cyber Security Platform, which is comprised of representatives of private and public operators of CII as well as relevant public agencies. It aims to facilitate communications between its participants. On an operational level, GovCERT has been set up as the main governmental CSIRT. It is run by the Federal Chancellery in cooperation with CERT.at (a private initiative) (2015a).

2.1.2 Information Sharing Schemes

Many EU Member States have developed information sharing schemes in order to disseminate important information between relevant public agencies and private operators. However, forms of cooperation can differ between countries. Information sharing schemes ensure that all relevant stakeholders are informed on current threats and risks and can take appropriate measures. It can also strengthen cooperation and coordination of actions and thus foster the effective usage of resources.

Germany has established a number of wide-ranging information sharing schemes between public and private sector agencies. Information sharing between law enforcement and intelligence agencies is realised through the National Cyber Response Centre[8], where the participants inform each other in daily meetings and workshops. Information sharing with the private sector is fostered through UP KRITIS and the Alliance for Cyber Security: UP KRITIS[9] is a public-private partnership and its main task is to establish CIIP related

[8] http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/Cyberabwehrzentrum/cyberabwehrzentrum_node.html
[9] http://www.kritis.bund.de/SubSites/Kritis/EN/Home/home_node.html

communication and cooperation between the private and public stakeholders on strategic and operational level. While UP KRITIS focuses on cooperation with companies of the critical sectors, the Alliance for Cyber Security has a broader scope and includes all relevant institutions in the area of cyber security. In order to strengthen the security of all stakeholders, the alliance offers a general "information pool", regular threat reports and knowledge exchange between its participants (Federal Office for Information Security 2013, 2015a).

Sweden's Cooperation Group for Information Security (SAMFI)[10] is another example for a good practice in information sharing. Unlike Germany, the focus is not on law enforcement and intelligence agencies but rather on authorities with responsibilities in societal information security. Within SAMFI, the different authorities not only share information on recent threats but also discuss strategical issue as well as national and international developments. Representatives from the different authorities meet several times a year and work together in working groups on current issues (Swedish Civil Contingencies Agency (MSB) 2015).

2.1.3 Development of a CSIRT-Community

In most countries a variety of CSIRTs with different competencies exist. Developing a strong community between the different national CSIRTs, including the division of responsibilities and sharing of information, can lead to mutual benefits, such as increased knowledge and a more efficient use of resources.

A good example for a strong community between CSIRTs is Poland. In Poland, no CSIRT has been designated as the national CSIRT. Instead, a community of different CSIRTs shares the responsibilities. CERT.gov.PL is the main CSIRT for public agencies, but also offers its services to CI operators based on formal agreements. CERT Polska was the first CSIRT in Poland and is part of the Research and Academic Computer Network (NASK). It holds special expertise in the analysis and research of security incidents and provides information on threats and incidents. The information is available on a database that can be used by private and public entities. CERT.gov.PL and CERT Polska work together closely, for example in operating a database dedicated to honeypots. Furthermore, they cooperate with a number of sectorial CSIRTs, such as MilCERT and CERT Orange (telecommunications sector) (2015b).

Other examples for good practices in the development of CSIRT-communities are the Netherlands or Germany. In Germany, the "CERT-Verbund" is an alliance of different German public CSIRTs (CERT-Bund, the military CERTBw and several CERTs of the federal states), private CSIRTs of major companies, and CSIRTs of private information security providers, among others. Every CSIRT is still responsible for its own constituency, but participants share information and support each other in incident handling. CERT-Verbund is the institutional foundation for this cooperation. The organisation is open to all kinds of German CSIRTs. The participants have defined standardised technical and organisational interfaces for the exchange of information. A key part is the statistical evaluation of the shared data and the provision of strategic insights (Federal Office for Information Security 2015b).

2.1.4 Risk Assessment

Risk Assessment includes the identification of potential threats, consequences of these threats (impact) and their likelihood.[11] The analysis of risks is a necessary step for crisis and incident preparation and management. In some countries, a national risk assessment is conducted by a national authority across all

[10] http://rib.msb.se/Filer/pdf/26177.pdf

[11] For an analysis of approaches to national-level risk assessment see: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/nlra-analysis-report

relevant sectors. Other countries, especially those with a more decentralised approach in CIIP, leave risk assessment the sector-specific authorities or to the operators of CI.

Examples for centralised national risk assessments are Sweden. The Swedish MSB has been commissioned to continue the work on a national risk assessment which began in 2011. It developed a risk assessment methodology, identified 27 particularly serious (national) events and developed eleven scenarios based on a selection of these events (2015c).

Denmark does not follow a national risk assessment plan, because sectoral risk management is seen as a more successful way to mitigate risks. A Cyber Threat Assessment Unit has been set up, which consists of personnel from the different sectoral public authorities. The Unit's goal is to conduct risk assessments for the different sectors (2015d).

An example for a decentralised approach is Switzerland. Switzerland uses an approach with a strong focus on individual self-responsibility. The critical subsectors are in charge of identifying the cyber-risks for their processes and systems. It is believed that the subsectors have the best knowledge on their own processes and systems. The government supports this process if requested (2015e).

2.1.5 Cyber Crisis Management

Good cyber crisis management includes the definition of roles and responsibilities in cases of cyber emergencies and coordination and decision-making procedures between relevant stakeholders with the necessary competencies and expertise. Furthermore, cyber crisis management needs to be aligned with other existing national emergency and crisis management systems.[12]

A good example for good practice in this field is the cyber crisis management structure in the Netherlands. For decision-making, the National Manual on Decision-making in Crisis Situation is applied (National Coordinator for Security and Counterterrorism 2013). In case of emergency related to ICT the national crisis organisation is handled by the Director of Cyber Security of the National Coordinator for Security and Counterterrorism (part of the Ministry of Security and Justice). Operational coordination and crisis response measures are offered by the National Cyber Security Centre.

Cyber crisis management is conducted in close cooperation with the private sector. In case of a cyber-related crisis the ICT Response Board becomes activated. The Board is set up as a public-private partnership and includes ICT experts from the affected sectors. It offers advice and recommendations. In addition, the NCSC has established agreements with public and private stakeholders on the method of crisis cooperation (National Cyber Security Centre 2015a).

2.1.6 Comprehensive Legal Framework

Some countries have drafted new laws and regulation in order to tackle the problem of increasing threats to CII. These legal frameworks are often tailored for operators of CI across all relevant sectors and are not limited to specific ones.

These legal frameworks often include mandatory implementation of technical and organisational security measures according to national or international standards. Other requirements can include mandatory incident notification and regular external security audits. These laws ensure a consistent security level across sectors and, in cases of mandatory security reporting, give governments the possibility to analyse the

[12] For a comparative study on cyber crisis management and general crisis management, see ENISA's Report on Cyber Crisis Cooperation and Management ENISA 2014.

incoming incidents reports, monitor threats levels, issue warnings to threatened operators of CI and offer support if necessary

An example of good practice in this area is France. The Military Programming Law (LPM[13]) obliges "operators of vital importance" (OIVs) to report cybersecurity incident to the Agence nationale de la sécurité des systèmes d'information (ANSSI) and implement technical and organisational measures for information security. In addition, OIVs are obligated to undergo cybersecurity audits, performed either by ANSSI or a service provider qualified by ANSSI (French Senate 2013).

Similar obligations can be found in Germany which has recently enacted the IT Security Act[14]. The newly passed law obligates operators to implement adequate organisational and technical measures for information security as far as it is necessary for the availability of their critical services. Furthermore organizations are to conduct security audits, to establish a contact point within their organisation and to report major IT security incidents if they could possibly affect the availability of their critical services (Federal Office for Information Security 2015c).

13 http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=D18929C424710499FAE3092CB887BD8D.tpdjo09v_2?cidTexte=JORFTEXT000028338825&categorieLien=id

14 http://dip21.bundestag.de/dip21/btd/18/040/1804096.pdf

2.2 Key Findings

Based on information collected (interviews and online surveys), some key findings have been identified. The key findings are presented along the different categories of the analytical framework. The total number of analysed countries per category can vary between twelve and eighteen depending on the feedback we received via the interviews and online survey.

Some of the key findings refer to critical sectors. Not all countries identify the same sectors as critical. The table below gives an overview of the mapping of the critical sectors identified by each country. The table is adapted from ENISA's study "Methodologies for the identification of Critical Information Infrastructure assets and services" from December 2014 (ENISA 2014). Please note that the table only covers a portion of the countries, which have been examined in this study.

SECTORS	ENERGY	ICT	WATER	FOOD	HEALTH	FINANCIAL	PUBLIC & LEGAL ORDER	CIVIL ADMIN.	TRANS-PORT	CHEMICAL & NUCLEAR INDUSTRY	SPACE & RESEARCH
AU	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
CZ	✓	✓	✓	✓		✓		✓	✓		
DK	✓	✓		✓	✓				✓		
EE	✓	✓	✓	✓	✓	✓	✓	✓	✓		
FI	✓	✓	✓	✓	✓	✓	✓		✓		
FR	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
DE	✓	✓	✓	✓	✓	✓	✓		✓		
HU	✓	✓	✓	✓	✓	✓	✓		✓		
IT	✓								✓		
NL	✓	✓	✓	✓		✓	✓	✓	✓	✓	
PL	✓	✓	✓	✓	✓	✓		✓	✓	✓	
ES	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓
CH	✓	✓	✓	✓	✓	✓		✓	✓		

Table 1 – Critical Sectors per Country. Adapted from: ENISA, Methodologies for the Identification of Critical Information Infrastructure Assets and Services 2014. p. 5-6

2.2.1 Types of National Authorities

In order to cope with the issue of CIIP, EU countries have either developed new authorities or extended the area of responsibility and powers of existing agencies. National authorities fall within the following categories:

- EMR: Emergency or CIP agency
- INT: Intelligence or security service
- ISA: Information security agency
- ISF: Information security forum
- NRA: National regulator or agency
- MIN: Ministry

Most of these categories are self-explanatory, however some remarks on the distinction between ISA and ISF are necessary. Information security agencies are public agencies with a strong focus on the security of information and telecommunications infrastructure. In many cases, they are the host of the national or governmental CSIRT. They are usually either independent agencies or subdivisions of ministries with a high degree of autonomy. Information security forums in comparison with ISAs, are set up as institutions where different agencies can cooperate closely together. With this model, the responsibilities and competencies of each existing agency largely remains intact. The ISF itself is usually not authorised to issue binding instructions to operators of CII. ISFs are often developed in countries that follow the principle of subsidiarity or decentralisation.

It should be noted that not all countries have developed a main or leading authority for CIIP. Especially Member States that follow a principle of subsidiarity leave responsibility with the individual ministries and operators of CII. In these cases we have identified the agency with the most responsibility or the strongest involvement in CIIP. In some Member States, responsibility for CIIP is shared between two agencies. In these cases, both agencies have been considered separately.

The following figure shows the number of the different types of governmental authorities for CIIP in 17 EU Member States and one EFTA country.

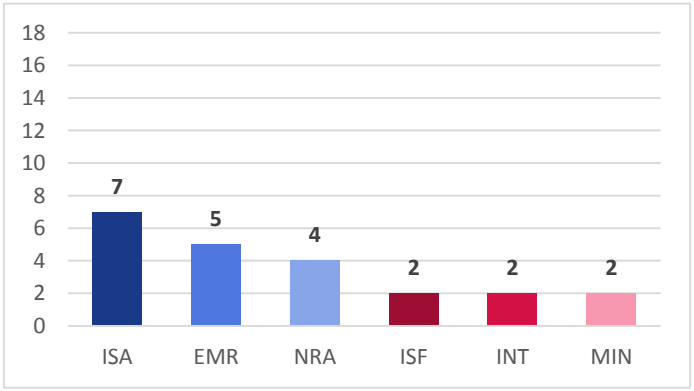

Figure 2-1 – National Authorities

Countries examined have assigned responsibility for CIIP to various national authorities. However, the figure shows that most countries tend to task their Information Security Authorities with CIIP. This seems to indicate that CIIP is seen as closest related to the issue of information security. CIIP is also a subcategory of general CIP, which might be the reason why five countries have decided to let their national EMR take

responsibility for it. CIIP also requires strong knowledge of information technology and the "landscape of private operators". Usually, NRAs combine these two traits, which could be the reason why four countries have assigned CIIP to them. Only a small minority of countries has assigned INT with the responsibility for CIIP. In two cases Ministries are complementing the tasks of another national authority.

2.2.2 Responsibilities of National Authorities

We examined the responsibilities and tasks assigned to national authorities in the area of CIIP for 12 countries (11 EU MS and one EFTA country):

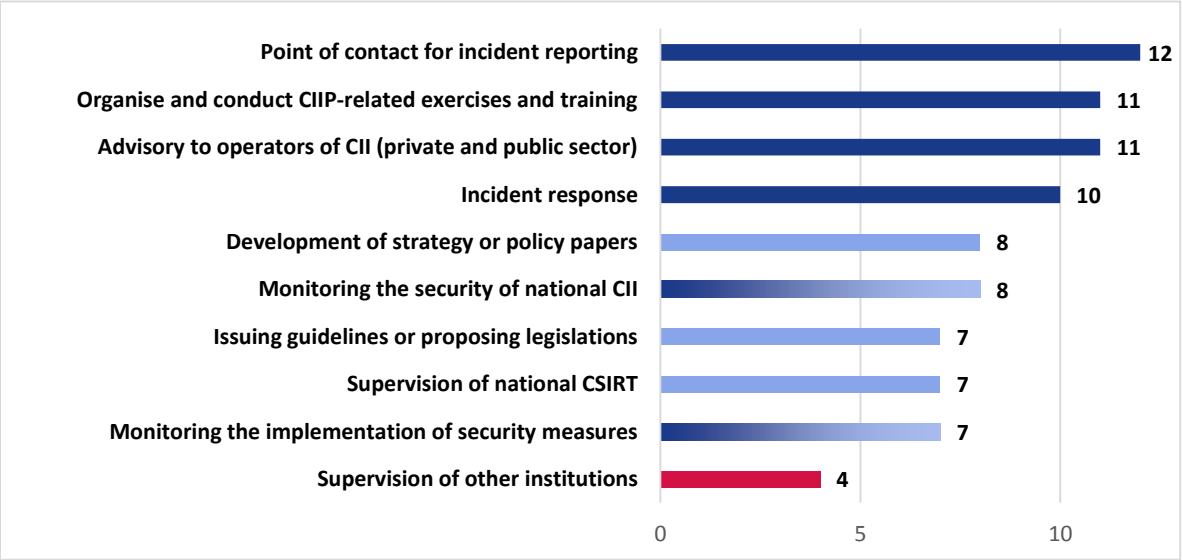

Figure 2-2 – Responsibilities of National Authorities

The figure shows that the majority of tasks are on the operational level (dark blue). Only seven to eight countries have additional responsibilities on a strategical or political level, such as the development of strategies, proposing legislations or the supervision of the national CSIRT (light blue). Only one third of the examined countries has been tasked with the supervision of institutions other than CSIRTs (red). These include mainly regulatory tasks.

2.2.3 Forms of Cooperation between Public and Private Stakeholders

The Member States examined have developed different forms of cooperation with the private sector with varying degrees of institutionalisation. Public-Private partnerships are an institutionalised form of cooperation between public and private actors. They are usually characterised through a long-term commitment of the different stakeholders, a contractual agreement or a joint statement, which defines the goals and responsibilities of the partnership, and shared responsibility for the produced output. A less institutionalised form of cooperation are working groups and contact forums, which are often temporary and demand less resources and commitment from the different stakeholders.

The following figure shows how many countries have developed different forms of cooperation with private stakeholders. Eighteen countries (seventeen Member States and one EFTA country) have been examined in total:

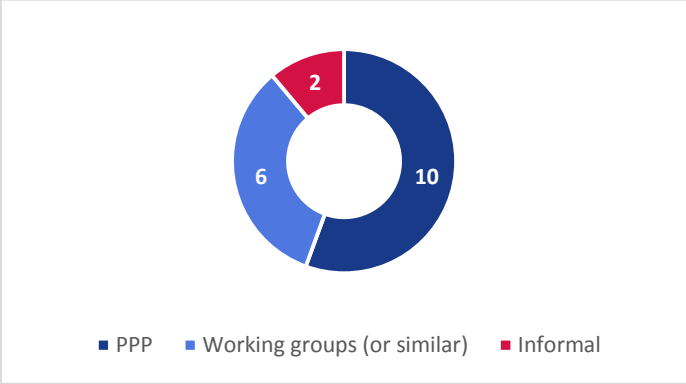

Figure 2-3 – Forms of Cooperation between Public and Private Stakeholders

Ten of the eighteen examined countries have established formal Public-Private Partnerships for the purpose of CIIP. Six countries are relying on less institutionalised forms of cooperation such as working groups or networks. Some of these countries are currently in the process of developing PPPs as required by their cyber security strategies. Two countries communicated with private stakeholders via informal ways.

2.2.4 Institutionalised Forms of Cooperation between Public Agencies

All of the sixteen examined countries have established some form of institutionalised cooperation between public agencies for the purpose of CIP beyond the usual communication channels. The institutional settings range from advisory boards, steering groups, forums, councils, cyber centres or expert meeting groups. However, the purpose is always to share information and to coordinate the actions of the different agencies. The majority of countries have developed new kinds of cooperation mechanism for the specific purpose of CIP. Some countries have instead extended the scope of existing institutions, which are responsible for emergency management or the security of the supply of infrastructure and services.

2.2.5 Risk Assessment

Risk Assessment includes the identification of threats, potential consequences of these threats (impact) and their likelihood. In some countries, a national risk assessment is conducted by a national authority across all relevant sectors. Other countries, especially those with a more decentralised approach in CIIP, leave risk assessment the sector-specific authorities or to the operators of CI.

The following figure shows how many countries are conducting what kind of risk assessment, or a leaving risk assessment to the individual operators.

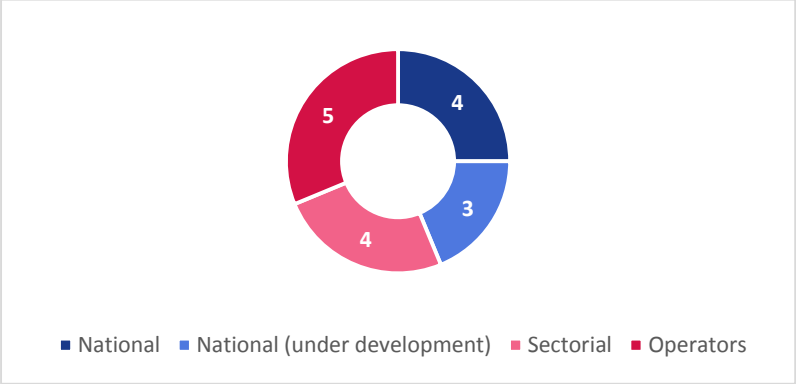

Figure 2-4 – Risk Assessment

The majority of the sixteen examined countries (fifteen Member States and one EFTA country) have conducted risk assessments on a national level or are planning to do so in the future. In four countries, risk assessment is conducted by the sector-specific agencies or ministries. In five countries, no national or sectorial risk assessment is being conducted. Instead, risk assessment is seen as the responsibility of private operators. However, this does not necessarily mean that governments are obligating operators to conduct risk assessments. This can be seen as an indicator on which level a government believes the problem should be best tackled: On the national level, the sectorial or the operator level.

2.2.6 Cyber Security Exercises

All of the examined countries are conducting regular CIIP-related exercises. There a three different kinds of CIIP-related exercises:

- Sector-specific exercises
- Cross-sectorial exercises
- International exercises

Most sector-specific and cross-sectorial exercises are being conducted in the financial, energy and the telecommunications sector. Other important sectors are public administrations, transport and logistics and healthcare.

The international exercises which were most commonly visited were NATO's exercises Locked Shields and Cyber Coalition and exercises of ENISA's Cyber Europe program. Other international exercise of importance were Cyberstorm IV (International Watch and Warning Network (IWWN)), ENISA's table top exercise Cyber Atlantic, NATO's Crisis Management Exercise CMX and the Nordic Cyber Security Exercise.

2.2.7 National Computer Security Incident Response Team

CSIRTs can be distinguished by their constituencies. Governmental CSIRTs usually offer their services to the public administration and agencies. National CSIRTs have a wider scope, because their constituency consists of operators of critical infrastructure and sometimes individual citizens. However, in some cases responsibilities between both types of CSIRTs might exist.

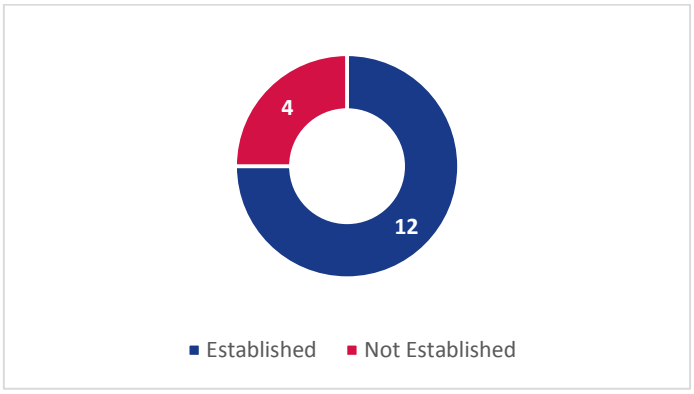

Figure 2-5 – National Computer Security Incident Response Team

Fourteen of the examined countries have established National CSIRTs. In two of these cases, the national CSIRT also serves as the Governmental CSIRT. Four countries have not developed dedicated national CSIRTs, however, either a national CSIRT is under development or the responsibility is shared by a community of private and sector-specific CSIRTs (as it is the case in Germany for example).

2.2.8 Security Incident Reporting

The majority of the examined countries have implemented mandatory incident reporting in the telecommunications sector,[15] but only a minority has implemented it across all sectors. The scope of reporting schemes vary greatly. Some countries obligate operators of CII to report security incidents regardless of the sector, as long as they have been assessed to be critical. Other countries have implemented mandatory reporting only for specific sectors.

The following figure shows the scope of mandatory security incident reporting across the examined countries (Sixteen Member States and one EFTA country):

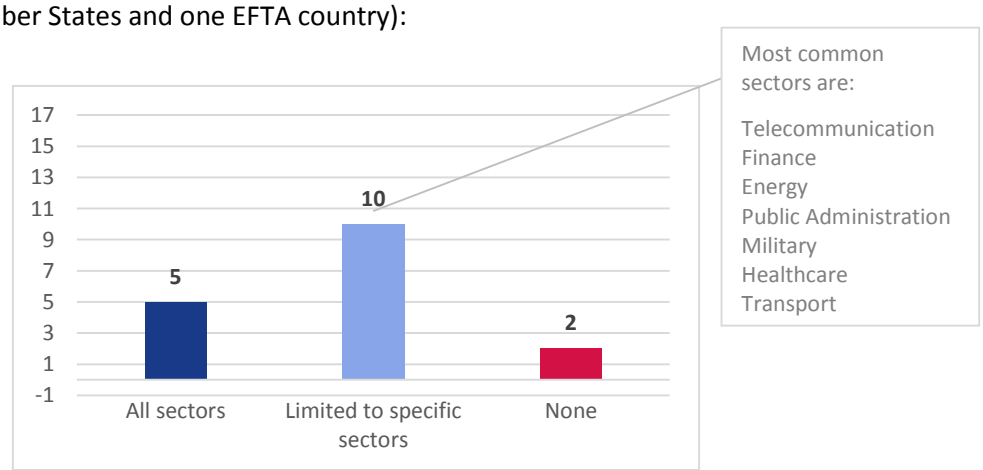

Figure 2-6 – Security Incident Reporting

[15] All Member States have implemented mandatory incident reporting in the telecommunications sector to be in line with the article 13a requirements. Moreover, Sweden intends to introduce mandatory incident reporting for the public institutions

Five countries have established mandatory security incident reporting across all sectors, with Germany being the most recent one. Most EU Member States have only developed mandatory incident reporting for some sectors. All of the ten countries that are limiting incident reporting to specific sectors, have established such obligations for the telecommunications sector. Other important sectors are Finance, Public Administration and Energy. Only two countries have not established mandatory reporting in any sector. The Netherlands are currently preparing a new law which will include obligatory incident reporting. The details of the law (e.g. the installation of enforcement mechanisms) depend on the content of the final NIS-Directive.

2.2.9 Security Measures

A similar picture can be observed for mandatory security measures.[16] The same five Member States that have implemented mandatory incident reporting across all sectors, have also implemented mandatory security measures across all sectors.

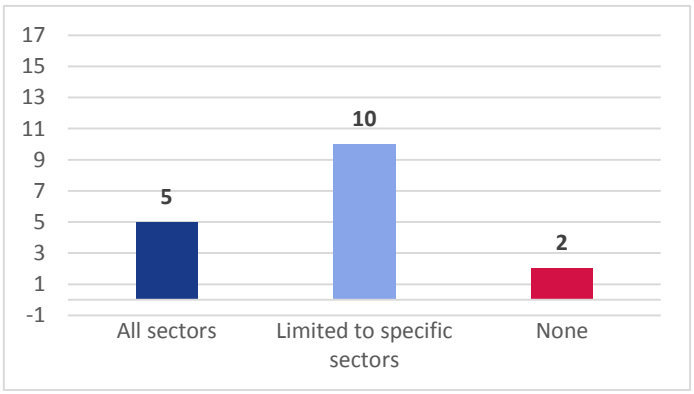

Figure 2-7 – Security Measures

Before CIIP became an important part of the political agenda, most countries had already established mandatory security measures in some sectors. Specifically sectors, which were already strongly relying on information technology or were providing crucial services to the population (for example the telecommunications, energy or finance sector). This explains why most countries have only implemented mandatory security measures in specific sectors. Countries with no mandatory security measures, usually consider security as the responsibility of private companies. However, there seems to be a slight tendency of countries to establish more comprehensive legislation for CIIP that covers all critical sectors.

2.2.10 Security Audits

Security audits seems to be either of the lowest priority or the hardest to implement for EU countries: Six countries have not implemented mandatory security audits and only five are obligating operators across all sectors to undergo audits.

[16] Article 13a also implies mandatory security measures for the telecommunications sector.

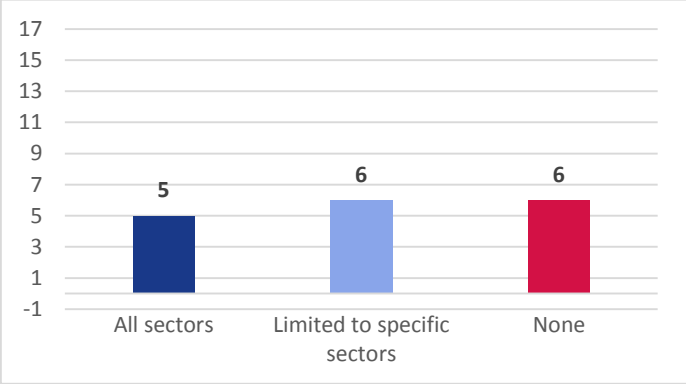

Figure 2-8 – Security Audits

The same five countries that have implemented mandatory security measures, have also implemented mandatory security audits. The analyses indicates that security audits are either of less a priority or harder to implement for the Member States' governments.

2.2.11 Incentives to Invest

In theory, countries can give an impetus to operators of CII to invest in security by creating incentives, such as subsidies or tax benefits. In areas such as environmental and ecological issues, tax benefits have proven to be successful in creating incentives for companies to implement environmental standards. However, almost none of the examined Member States have such incentives for CIIP-security in place. Some countries believe that market pressure will, in the long run, give operators of CII enough incentive to invest in additional security measures. An exception is Finland, where companies that invest in operational security measures are eligible for tax breaks under certain conditions.

2.3 CIIP Governance Profiles

This chapter describes three profiles of CIIP governance among the examined sixteen EU Member States. CIIP governance refers to all structures and processes associated with the steering in the area of CIIP undertaken by public (e.g. public administration or law enforcement agencies) or private actors (e.g. associations, operators of CII, sectorial CSIRTs). It can refer to the decision-making processes, but also the operational measures in the protection of CII.

The different profiles illustrate specific forms of CIIP governance, which are defined by their shared characteristics. The profiles are not exclusive types, but are rather points on a spectrum. For example, the centralism of CIIP-governance displayed by a country will vary and while some countries can be described as either centralised or decentralised, others fall in between these two points. The same is true for the degree of private-sector involvement. In the following section examples of Member States that fit a profile or the defining characteristics of it are presented.

These profiles can help to understand how CIIP is organised in the individual Member States and what CIIP-measures and actions can possibly be transferred from one Member State to another. Some measures undertaken by Member States with a centralised approach in CIIP might not work in countries that follow a decentralised approach (and vice versa), because of different responsibilities, processes and relations between relevant stakeholders. Likewise, measures undertaken by Member States with a high degree of private sector participation might not be transferable to states in which CIIP is primarily steered by emergency or law enforcement agencies (and vice versa). However, Member States with similar characteristics in CIIP-governance might be better suited for the exchange of good practices and effective CIIP-measures.

The governance of CIIP is a key feature in understanding how CIIP is organised in different Member States and to what degree measures are transferable between them.

2.3.1 Profile 1: Decentralised Approach

The decentralised approach is characterised by:

- Principle of subsidiarity
- Strong cooperation between public agencies
- Sector-specific legislation

Sector-Responsibility

Instead of establishing a strong CIIP-agency with responsibility across all or several critical sectors, the decentralised approach follows the principle of subsidiarity. This means that the responsibility for CIIP is either in the hands of the sector-specific authority or the companies and operators of the CII themselves.

Therefore, many Member States that fit this profile are lacking a centralised authority for the purpose of CIIP, but have placed the responsibility for CIIP on the sector-specific authorities.

Strong Cooperation between Public Agencies

Because of the variety of public agencies involved in CIIP, many Member States have developed cooperation schemes in order to coordinate the work and efforts of the different stakeholders. These cooperation schemes can take the form of informal networks or more institutionalised forums or councils. However, these cooperation schemes only serve the purpose of information exchange and coordination between the different public agencies, but have no authority over them.

Sector-specific Legislation

The countries that follow the decentralised approach often refrain from drafting legislation for the purpose of CIIP across critical sectors. Instead, the adoption of laws and regulations remains sector-specific and therefore can vary greatly between sectors.

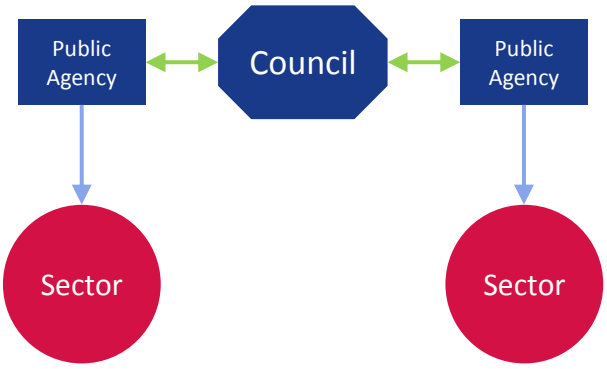

Figure 2-9 – Decentralised Approach

Examples for the Decentralised Approach

Sweden is a good example for a country that follows a decentralised approach in CIIP. The country uses a "system perspective", which means that the main tasks of CIIP, such as the identification of vital services and critical infrastructures, the coordination and support of operators, regulatory tasks as well as measures for emergency preparedness are the responsibility of different agencies and municipalities. Among these agencies are the Swedish Civil Contingencies Agency (MSB), the Swedish Post and Telecom Agency (PTS), and several Swedish Defence, Military and law enforcement agencies (2015c).

In order to coordinate the actions between the different agencies and public entities, the Swedish government has developed a cooperative network comprised of authorities "with specific societal information security responsibilities". This Cooperation Group for Information Security (SAMFI), consists of representatives of the different authorities and meets several times a year to discuss issues related to national information security. SAMFI's subject areas are mainly to be found in political-strategic areas and cover topics such as technical issues and standardization, national and international development in the field of information security, or management and prevention of IT incidents (Swedish Civil Contingencies Agency (MSB) 2015).

Sweden has not published a central law for CIIP applicable for operators of CII across sectors. Instead, issuing legislation with obligations for companies within specific sectors is the responsibility of the respective public authorities. For example, the MSB has the right to issue regulations for government authorities in the area of information security, while the PTS can obligate operators to implement certain technical or organisational security measures based on secondary legislation.

Another example for a country that display characteristics of this profile is Ireland. Ireland follows a "doctrine of subsidiarity", where each Ministry is responsible for the identification of CII and risk assessment within its own sector. Furthermore, no specific regulations for CIIP at the national level have been enacted. Legislation remains sectorial and exists mainly for the energy and telecommunications sector (2015f). Other examples are Austria, Cyprus, Finland and Switzerland.

2.3.2 Profile 2: Centralised Approach

The centralised approach is characterised by:

- Central authority across sectors
- Comprehensive legislation

Central Authority across Sectors

Member States that follow a centralised approach have developed authorities with responsibilities and wide competencies across several or all critical sectors, or have extended the powers of existing authorities. These main authorities for CIIP combine several tasks such as contingency planning, emergency management, regulatory tasks and supporting private operators. In many cases, the national or governmental CSIRT is part of the main CIIP-authority.

Comprehensive Legislation

A comprehensive legislation creates obligations and requirements for all operators of CII across all sectors. This can be achieved through new comprehensive laws, or through complementing existing sector-specific regulations.

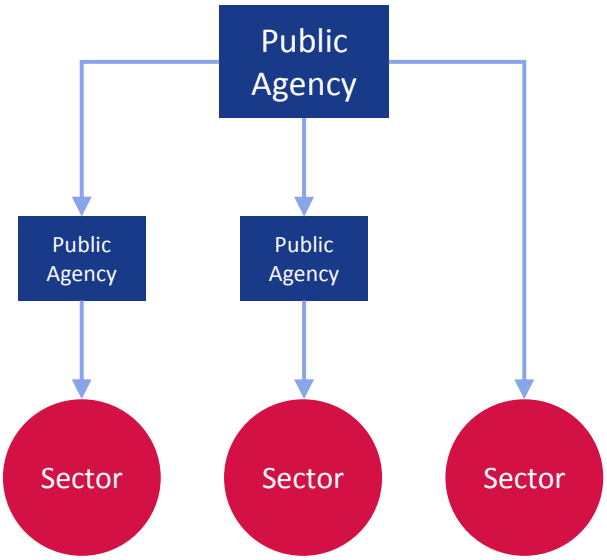

Figure 2-10 – Centralised Approach

Examples for the Centralised Approach

France is a good example for an EU Member State with a centralised approach. France's ANSSI has been declared the main national authority for the defence of the information systems in 2011. ANSSI has a strong supervisory role for "operators of vital importance" (OIVs): The agency can order OIVs to comply with security measures and is authorised to perform security audits on them. Furthermore, it is the main Single Point of Contact for OIVs, which are obligated to report security incident to the agency (2015g).

In cases of security incidents, ANSSI acts as a contingency agency for CIIP and decides on the measures that operators must take to respond to the crisis. The government's actions are coordinated within ANSSI's

operations centre. Detection of threats and incident response on an operational level is performed by CERT-FR, which is part of ANSSI.

France has established a comprehensive legal framework for CIIP. In 2006, the Prime Minister ordered to establish a list of sectors of critical infrastructure. Based on this list, which identified twelve vital sectors, the government has defined around 250 OIVs. In 2013, the Military Programming Law (LPM) was promulgated, which sets different obligations for OIVs, such as incident reporting or implementation of security measures. These requirements are mandatory for all OIVs across all sectors (French Senate 2013).

Among the analysed EU Member States, the centralised approach is the exception. Most countries are following a cooperative, decentralised approach. However, France is not the only country, which displays characteristics of a centralised approach. Other examples of countries with characteristics of the centralised approach are the Czech Republic (central authority) and Germany (comprehensive legislation).

2.3.3 Profile 3: Co-Regulation with the Private Sector

The co-regulation approach is characterised by:

- Institutionalised cooperation with the private sector
- Horizontal relationship between public and private parties

Institutionalised Cooperation with the Private Sector

A typical form of institutionalised cooperation between the public and private sector are public-private partnerships (PPPs) which are usually based on contractual agreement between the parties. Public and private actors can provide different resources to the partnerships: For example, the government can offer political legitimacy and funds, while private actors can add special expertise and efficiency. Through PPPs, governments have the possibility for regulation in areas where it is lacking expertise.

Horizontal Relationship between Public and Private Parties

Although not exclusively, PPPs are often characterised by a horizontal relationship between the public and private parties, meaning that both are on equal footing and make joint decisions. The decision making process is based on negotiations rather than hierarchical command structures.[17]

In some cases, this kind of relationship is also reflected in a compliance structure which is not based on a strong regulatory framework and enforcement mechanisms but is based on voluntary action and trust.

[17] For a good practice guide on Cooperative Models for Effective PPPs see: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/good-practice-guide-on-cooperatve-models-for-effective-ppps

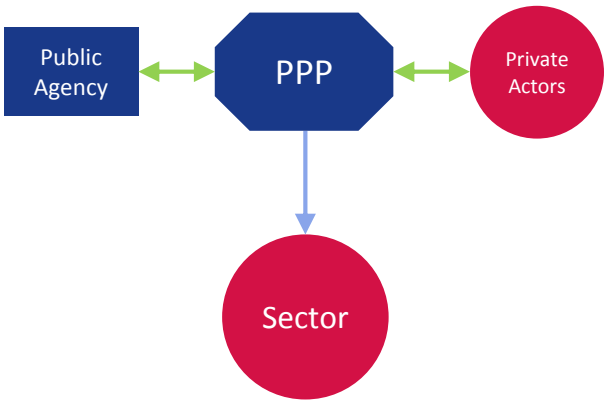

Figure 2-11 – Corregulation

Examples for Co-Regulation with the Private Sector

An example for co-regulation in the area of CIIP can be found in the Netherlands. The major CIP agency is the National Cyber Security Centre (NCSC). It is set up as a central information hub and a centre of expertise for cyber security within the National Coordinator for Security and Counterterrorism (NCTV). The NCSC consists of several partnerships between public and private actors, such as various Information Sharing and Analysis Centres (ISACs) and the ICT Response Board which analyses the situation during a large-scale IT crisis or threat. The NCSC emphasises that cooperation with private stakeholders is based on equality and trust (National Cyber Security Centre 2015b).

In addition, the Dutch Cyber Security Council offers advice on a strategic and political level. The council is comprised of representatives from different Ministries, academia and the private sector and has a strong public-private character.

Participation in the various Information Sharing and Analysis Centres is based on confidentiality, meaning that members are not forced or obligated to share information with the other participants but do so on a voluntary basis. All representatives are expected to respect the mutual agreement and treat information on threats, risks and other sensitive issues in a confidential manner.

Legal obligations and requirements in the Netherlands tend to be stronger for the telecommunications and nuclear sector. However, Dutch companies are not obliged to report security incidents and a lot of incident notification is done voluntarily (2015h).

3. Recommendations

Based on the key findings of this study, ENISA presents the following recommendations for the European Member States and the European Commission.

3.1 Member States

Recommendation 1: Increase institutionalised cooperation with private stakeholders

EU Member States have established different kinds of cooperation with private stakeholders. These primarily include the private operators of CII, but also private associations, sectorial CSIRTs or academia. Some countries are relying on public-private partnerships while others are cooperating with the private actors in less formalised, temporary working groups and similar formats.

Threats to CII are likely to increase in the coming years and therefore the necessity for cooperation with private stakeholders will increase as well. Member States should establish institutionalised and long-term partnerships or equivalent cooperation schemes with private stakeholders for different tasks such as detection, response and analysis of threats to CII. Existing working groups or forums can provide a good starting point to develop stronger cooperation.

Related to this is the development of a strong CSIRT-community. Member States should foster the cooperation between government and sectorial CSIRTs in order to distribute tasks and responsibilities and gain from increased knowledge and a more efficient use of existing resources.

Recommendation 2: Align management structure for CIIP with existing national crisis and emergency management structures

Most Member States have general management structures for emergencies or incidents on a national level in place. The issue of CIIP should be integrated into the existing management structures. Alternatively, CIIP-management structures should be aligned and made compatible with existing management structures. This includes the definition of roles and responsibilities of the different public agencies in cases of emergency, but also in day-to-day operations.

Recommendation 3: Participate in or host international exercises

Threats to CI are not bound by national borders and often transcend them. This means that Member States and private actors often need to cooperate with their counterparts in other Member States or countries beyond the European Union. In order to strengthen international cooperation, Member States should maintain participation in international CIIP-related exercises and consider hosting equivalent exercises in their home country.

Recommendation 4: Establish mandatory security incident reporting

In order to gain an overview of the national risk situation and on potential threat scenarios, the state is dependent on the input from operators of CII. Only with comprehensive data are governments able to gain knowledge on current dangers to CII. This data constitutes the basis for a national risk assessment (see Recommendation 5) and for the development and adjustment of strategies, policies, the drafting of legislation and the allocation of resources.

For this purpose, Member States should establish mandatory security incident reporting for all operators of CII. ENISA could play a significant role in this process by providing support in the execution of aligned reporting schemes at EU level. With the help of ENISA a consistent implementation of incident reporting would make it easier for providers and users to operate across the different Member States. Monitoring of IT-infrastructure can be conducted by the operators themselves or, in cases of smaller operators with limited financial resources, by third parties. If needed, operators should be supported in the development of the capacities for monitoring and incident reporting by public agencies.

Mandatory security incident reporting should also include obligations for public agencies to report back to the affected operators and inform about security threats and other CIIP-related issues. This will create additional incentives for operators to cooperate with the government on incident reporting and ensure that vulnerable operators are informed quickly about potential threats.

Operators of CI are often reluctant to report incidents to public agencies because they fear that public disclosure of these incidents will damage their companies' reputation. A means of increasing trust between the government and private operators could be the installation of "clearing houses". These institutions could receive incidents reports and other threat-related information from operators and anonymise them, before forwarding them to the responsible public agencies.

Recommendation 5: Conduct national risk assessment

Member States currently conduct risk assessments on different levels. Some governments believe that the risk assessments should be conducted by the individual operators, since they have the best knowledge of their processes and structures. However, the results of the identification and assessment of risks conducted by a national government and a private company can differ. National governments are responsible to ensure that the population has access to all necessary services and goods. A private companies' focus is limited to its own business and the interests of their stakeholders.

Because of these different perspectives, the government should conduct risk assessments from a national perspective, which identifies and assesses risks and impacts for a nation's general population. Furthermore, Governments should adopt an open, transparent and collaborative approach to national risk assessment, involving all relevant stakeholders.

Recommendation 6: Utilize best legal framework practices for CIIP across critical sectors

Some sectors, like the financial or the energy sector, are stronger regulated than others. This means that obligations and requirements can vary greatly across the sectors and thus for the different operators of CI. Furthermore, mandatory security measures are not always compatible with certain companies or sectors.

Member States should evaluate and asses their legal frameworks for CIIP in different critical sectors. This will ensure that all operators of CII are facing applicable risk based obligations and will contribute to the alignment of security standards across sectors.

Recommendation 7: Examine if positive incentives can be provided to operators of CII to invest in security measures

Almost none of the examined Member States in this study have implemented incentives to invest in CIIP-related security measures for operators of CII. Incentives like tax breaks or financial subsidies have been used by some governments in other policy areas as a "soft" steering tool. The goal is to refrain from laws or regulations, but to encourage companies through positive incentives to implement certain policies. This

strategy has been used successfully in other areas such as environmental issues. Such incentives should not be limited to the capital expenditures of security measures, but also include the operational expenditures of processes and continuing operations.

Other possible forms of positive incentives include supporting measures by government institutions, such as post-incident support. Public agencies could help operators with forensic investigations and recovery measures.

3.2 European Commission

Recommendation 8: Ensure that MS collectively agree baseline requirements in order to support the development of CIIP in MS

The European Commission should require the MS to collectively define baseline requirements for an adequate level of national CIIP-capabilities. These baseline requirements can serve as a guideline for the EU Member States that are in the process of developing or extending CIIP. The baseline requirements should be comprehensive and cover all relevant action areas: Policy, governance structure, legislation, risk management and mitigation measures, emergency preparedness, threat intelligence and information sharing. The baseline requirements should be generic and contain objectives and controls. Ideally, they can be used to evaluate the maturity level of CIIP in EU Member States and help to identify gaps.

The Network and Information Security Directive, proposed by the Commission in 2013, is expected to fill this gap. It is currently in the final stages of negotiations between the European Parliament and the Council and will lay down different measures to ensure a high common level of network and information security within Member States (European Commission 2013b).

The EU Commission should actively promote the different measures outlined in the NIS Directive and support implementation efforts.

Recommendation 9: Develop and conduct a maturity assessment of Member States' CIIP readiness

The European Commission should develop a method for maturity assessment of Member States' critical information infrastructure protection and conduct those assessment on a regular basis.

The defined baseline requirements (see recommendation 8) can serve as a basis for the development of key process areas and defined goals. Development of such a model will allow the EU Commission to assess the national CIIP measures of the individual EU Member States and compare them with each other.

Based on these results, the EU Commission can make individual recommendations to EU Member States on how to improve national CIIP.

Recommendation 10: Support information sharing and the exchange of knowledge between EU Member States' national CSIRTs

The EU Commission should foster information sharing and the exchange of knowledge between EU Member States' national CSIRTs. If a CII-related incident occurs in a certain country, other CSIRTs should be notified about the risk and possible incident solutions in order to take appropriate operational preparations. Permanent forums and working groups, as well as technical platforms and interfaces for threat information

sharing should be developed. Since threats to CII often transcend national borders, information sharing platforms can also serve to coordinate actions of the different national CSIRTs.

Similar EU-wide information sharing networks for national CIIP-authorities as well as private operators should be considered.

Recommendation 11: Identify European Critical Information Infrastructure

A part of EU Information Infrastructure is potentially critical, such as the information and communications systems of the institutions and agencies of the European Union or assets such as the global navigation satellite system Galileo, which is currently under development.

The EU should identify EU Critical Information Infrastructure and take appropriate security measures. CIIP-measures of EU assets can also be delegated to hosting Member States.

List of References

Council of the European Union (2005): Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. Available online at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32005F0222&from=EN.

Council of the European Union (2008): Council Directive 2008/114/EC. On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Available online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

ENISA (2014): Methodologies for the identification of Critical Information Infrastructure assets and services - Annex A. Draft, V1.0, checked on 04.06.15.

(2015a): CIIP in Austria. Interview with Timo Mischitz-Schilcher. Andreas Reichard. Phone conference.

(2015b): CIIP in Poland. Interview with Krzysztof Silicki, Maciej Pyznar, Magdalena Wrzosek. Phone conference.

(2015c): CIIP in Sweden. Interview with Peter Wallström. Phone conference.

(2015d): CIIP in Denmark. Interview with Peter Knøster. Phone conference.

(2015e): CIIP in Switzerland. Interview with Dr. Stefanie Frey. Phone conference.

(2015f): CIIP in Ireland.

(2015g): CIIP in France. Interview with Yann Salamon. Phone conference.

European Commission (2005): Green Paper on a European programme for critical infrastructure protection. COM/2005/0576 final. Available online at http://eur-lex.europa.eu/legal-content/EN/NOT/?uri=celex:52005DC0576, checked on 06.09.15.

European Commission (2006): Communication from the Commission on a European Programme for Critical Infrastructure Protection. Available online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF.

European Commission (2013a): Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure. Available online at http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/docs/swd_2013_318_on_epcip_en.pdf

European Commission (2013b): Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union. Available online at http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1666.

European Parliament; Council of the European Union (2013): Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Available online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:en:PDF.

Federal Office for Information Security (2015a): ACS: Informationen zur Allianz für Cyber-Sicherheit. Available online at https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Ueber_uns/ueber_uns.html, checked on 07.07.15.

Federal Office for Information Security (2015b): BSI: CERT-Bund. Available online at https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/Cert-Bund/cert-bund_node.html, checked on 07.07.15.

Federal Office for Information Security (2015c): Completed interview questionnaire.

Federal Office for Information Security, Federal Office of Civil Protection and Disaster Assistance (2013): UP KRITIS. Available online at http://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/upk_node.html, updated on 07.07.15, checked on 07.07.15.

(2015h): CIIP in Netherlands. Interview with Barend Sluijter. Phone conference.

Myriam Dunn Cavelty (2012): The Art of CIIP Strategy: Tacking Stock of Content and Processes. Edited by J. Lopez et al. Critical Information Infrastructure Protection.

National Coordinator for Security and Counterterrorism (2013): National Manual on Decision-making in Crisis Situations. Available online at http://english.nctv.nl/Images/national-manual-decision-making-in-crisis-situations_tcm92-523831.pdf.

National Cyber Security Centre (2015a): ICT Management. Available online at https://www.ncsc.nl/english/Incident%2BResponse/ict-crisis-management.html, checked on 11.08.15.

National Cyber Security Centre (2015b): Cooperation. Available online at https://www.ncsc.nl/english, checked on 11.08.15.

Swedish Civil Contingencies Agency (MSB) (2015): Cooperation Group for Information Security (SAMFI). Available online at http://rib.msb.se/Filer/pdf/26177.pdf, checked on 29.06.15.

Annex A: Online Survey

ENISA: CIIP Online Survey 2015

Fields marked with * are mandatory.

General

* **Please name the country in which your agency is located:**

National Authorities

* **Has an authority with mandate on Critical Information Infrastructure Protection (CIIP) been established in your country?**
(only one answer possible)

- No authority for CIIP has been set up
- IT regulator/agency or National Regulatory Authority (NRA)
- Information security agency (authoritative) (e.g. Cyber Security Agency)
- Information security forum (coordinative) (e.g Public-Private Partnership)
- Intelligence or security service
- Ministry
- Law enforcement agency
- Emergency or CIP agency
- Others (please specify in box below)
- Unknown

* Others

1

* **What are the responsibilities of the national authority?**
(multiple answers possible)

- [ ] Advisory to operators of CII (private and public sector)
- [ ] Point of contact for incident reporting
- [ ] Monitoring the security of national CII
- [ ] Monitoring the implementation of mandatory security measures at operators of CII
- [ ] Incident response
- [ ] Supervision of national CERT
- [ ] Supervision of other institutions (please specify in bow below):
- [ ] Development of strategy or policy papers
- [ ] Issuing guidelines or proposing legislations (e.g. on security measures)
- [ ] Organise and conduct CIIP-related exercises and training
- [ ] Unknown

* Supervision of other institutions:

Incident Notification

* **Have incident notification mechanisms for operators of Critical Information Infrastructure (CII) been established in your country?**
(only one answer possible)

- ( ) No
- ( ) Yes, operators of CII can report incidents voluntarily
- ( ) Yes, operators of CII are obligated to report incidents
- ( ) Unknown

* **Did security incidents* with regard to CII occur in the last five years in your country?**
*A security incident is a breach of information security, policy or failure of controls that have a significant probability of compromising operations
(only one answer possible)

- ( ) No
- ( ) Probably (there is evidence)
- ( ) Yes, 1 – 5 incidents
- ( ) Yes, 6 – 10 incidents
- ( ) Yes, more than 10 incidents
- ( ) Unknown

* **What were the root causes of the security incidents?**
(multiple answers possible)

- [ ] External (through unauthorised actions of third parties, e.g. attacks)
- [ ] Internal (e.g. authorised employees)
- [ ] Technical failure (failures of soft- or hardware)
- [ ] External events (e.g. power failure, force majeure)
- [ ] Others (please specify in box below):
- [ ] Unknown

* Others:

* **Which sectors have been affected by security incidents in the last five years?**
(multiple answers possible)

- [ ] Agriculture and food
- [ ] Water and waste water
- [ ] Healthcare and public health
- [ ] Government facilities
- [ ] Information and Telecommunications
- [ ] Transportation and logistics
- [ ] Banking and financial services
- [ ] Energy (Oil, gas, nuclear)
- [ ] Others (please specify in box below):
- [ ] Unknown

* Other sectors:

* **Which authority is responsible to investigate security incidents related to CII?**
(multiple answers possible)

- [ ] The affected company or agency itself
- [ ] National Computer Emergency Response Team (CERT)
- [ ] National authority for CIIP
- [ ] Law enforcement authorities
- [ ] Others (please specify in box below):
- [ ] Unknown

* Other authorities

* **How would you assess the risk for CII-related security incidents in your country?**
(only one answer possible)

- Very low
- Low
- Average
- High
- Very High

National Exercises

* **How often are national exercises for CIIP conducted?**
(only one answer possible)

- Every three years
- Every two years
- Once a year
- More than once a year
- Unknown

* **Are CIIP-exercises cross-sectorial or sector-specific?**
(multiple answers possible)

- Sector-specific (please name exercise(s) and sector(s) in box below):
- Cross sectorial (please name exercises and sectors in box below):
- Unknown

* Exercise and sectors

Cooperation between Public and Private sector

* **What kind of cooperation mechanisms have been established between the public and private sector?**
(multiple answers possible)

- [ ] No cooperation
- [ ] Only informal cooperation
- [ ] Voluntary information sharing platform
- [ ] Working groups
- [ ] Public-Private Partnership
- [ ] Unknown

Obligations and Requirements

* **What are incentives for operators of CII to implement security measures?**
(multiple answers possible)

- [ ] Financial subsidies or tax incentives
- [ ] Technical guidelines or best practices
- [ ] Secondary legislation
- [ ] Primary legislation
- [ ] Others (please specify):
- [ ] Unknown

* Other incentives:

* **What kind of mandatory requirements or legal obligations for operators of CII exist in your country?**
(multiple answers possible)

- [ ] Security incident notifications
- [ ] Internal audits
- [ ] External audits
- [ ] Organisational security measures (e.g. risk assessment, ISMS, BCM, etc.)
- [ ] Technical security measures (e.g. Layered security, Cryptography)
- [ ] Others (please specify in box below):
- [ ] Unknown

* Other requirements

5

* **What kind of policy instruments for CIIP have been developed in your country?**
(multiple answers possible)

- [ ] Strategy or policy papers
- [ ] Guidelines and best practices
- [ ] Legislation (e.g. laws or regulations)
- [ ] Others (please specify in box below):
- [ ] Unknown

* Other policy instruments

Thank you for participating in this survey!

Annex B: Interview Guide

Interview guide

G1	• **Please name the country in which your agency is located:**

G2	• **Has your country published a national strategy or comparable policy paper for Critical Information Infrastructure Protection (CIIP)?** • **Are there any other policy papers, guidelines, laws or regulations, which set a framework for CIIP?**

G3	• **What are the major threats and risks for Critical Information Infrastructure (CII) in your country?** • **Have these threats and risks been outlined in an official document?**

G4	• **What are the major strategic goals and objectives with regard to CIIP?** • **Have these goals and objectives been outlined in an official document?**

G6	• **Has a national risk assessment plan for CII-related security incidents been developed?**

G7	• **Are exercises for CIIP conducted in your country?** • **Does your country participate in international exercises?**

G8	• **Could you describe the roles and responsibilities of governmental agencies and operators of CII during a national CII-related security incident? (e.g. Issuing legislation, Supervision, Receiving reports. Incident response, Advisory, etc.)**

G9	• Is there an institution or agency which has been designated to act as information platform during CII-related emergencies? • If yes, has this institution been tasked with additional duties or responsibilities?

G10	• Has a designated authority with the national responsibility for CIIP been established in your country? • What competencies and powers does this authority have?

G11	• Are there other governmental agencies, which are considered to be relevant for CIIP in your country? • What are their roles and responsibilities? • Could you describe the role of operators of CII in CIIP?

G12	• What are forms of cooperation between the governmental agencies and the private sector? (e.g. PPPs, Information sharing platforms, Forums, etc.) • If there is an information sharing platform: What kind of information is exchanged?

G13	• Are there specific cooperation mechanism between governmental agencies with regard to CIIP (formal or informal)?

G14	• Have awareness raising campaigns or training programmes been conducted?

G15	• Has a national CERT with responsibilities in CIIP been established in your country? • What are the responsibilities and tasks of the CERT in national CIIP? • Is the national CERT supervised by a governmental agency?

G16	• Are there specific obligations for operators of CII? For example incident notification, implementation of security measures (technical or organizational, e.g. Risk assessments, Business continuity plans, Testing, etc), security audits, or compliance tests?

G17	• Are any incentives given for operators of CII to invest in security? For example tax benefits or other financial subsidies?

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

Catalogue Number: **TP-04-15-821-EN-N**

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

ISBN: 978-92-9204-136-6
doi: 10.2824/534303