
# Methodologies for the identification of Critical Information Infrastructure assets and services

*Guidelines for charting electronic data communication networks*

December 2014

European Union Agency for Network and Information Security www.enisa.europa.eu

## 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

Rossella Mattioli, Dr. Cédric Levy-Bencheton

## Contact

For contacting the authors please use resilience@enisa.europa.eu.

For media enquires about this paper, please use press@enisa.europa.eu.

## Acknowledgements

This work has been carried out in collaboration with OTEPlus, in particular: Kostas Panayotakis, Maria Legal and George Papadopoulos.

We have received valuable input and feedback from the experts of the INFRASEC, ENISA Internet Infrastructure security and resilience reference group, and all participants of the validation workshop in Koln, Germany the 26th of September 2014.

We also like to thank the experts from the EU Critical Infrastructure point of contacts in each MS, National Regulatory Authorities, Cyber Security Agencies, Network operators and operators of Critical Infrastructures across EU and EFTA countries who participated at each part of this study and provided great input and feedback.

## Legal notice



## Copyright Notice



ISBN 978-92-9204-106-9, doi 10.2824/38100

## Executive summary

Communication networks are an important component of the life of millions of European citizens. These networks represent the fabric of the future information society and provide the means for the single digital market. Some parts of these communication networks are also vital for the operations of Critical Infrastructures which are fundamental for the function of modern society.

An attack or a large scale outage affecting the communication networks assets supporting Critical Infrastructure can have cascading effects and affect large part of the population or vital functions of society. But which are exactly those network assets that can be identified as Critical Information Infrastructure and how we can make sure they are secure and resilient?

This study aims to tackle the problem of identification of Critical Information Infrastructures in communication networks. The goal is to provide an overview of the current state of play in Europe and depict possible improvements in order to be ready for future threat landscapes and challenges. As it was possible to underline, currently a significant number of Member States present a low level of maturity and lack a structured approach regarding identification of Critical Information Infrastructure in communication networks and this can pose severe risks regarding the everyday increasing dependency of the vital functions of the society on these networks.

Moreover, based on the findings of the survey, the discussion with stakeholders and the analysis of the different approaches already in place, it was possible to highlight the following challenges in identifying CIIs assets and services:

- detailed list of critical services is not always present and should be tailored per Member State
- criticality criteria for the identification of critical assets is a challenging process especially regarding internal and external interdependencies
- effective collaboration between public sector and the private sector is fundamental in identifying and protecting CII assets and services and should start from asset identification.

Considering this multi-layered and complex environment and raising threat scenarios, the following recommendations emerged for Member State and operators of critical infrastructures to foster security and resilience of CIIs over communication networks in Europe:

***Member States should clearly identify Critical Information Infrastructures if not already covered in their Critical Infrastructure activities.*** *Not all MS have clearly defined the asset perimeter of Critical Information Infrastructures. For this reason, if not already covered by the Critical Infrastructure definition, Member states should clearly define which specific network assets are covered and should be secure and resilient.*

***Member States who are starting to work on the identification of CII assets should cooperate with stakeholders involved in the operations of Critical Information Infrastructures.*** *Effective collaboration between public sector (Government & mandated Agencies) and the private sector is fundamental in protecting CII assets and services. For the identification of Critical Information Infrastructures in communication networks, the involvement of two categories of stakeholders should be pursued:*

- *operators of Critical Infrastructures*
- *network operators*

*given the complementarity of their perspectives, responsibilities and expertise.*

***Member States who are starting to work on the identification of CIIs should adopt a methodology for the identification of critical network assets and services, using one or a mix of the proposed solutions in this study that better fits the need of the MS.*** *It is worth-noting that the purpose here is to present the Member States with a portfolio of methodological approaches – rather than a one size 'fits-all' methodology – so that each Member State may choose the approach or a combination of approaches that suits better to its own specific characteristics and needs.*

***Member States who base their identification of CIIs on critical services should develop a list of these services and assess internal and external interdependencies***. *While assessing the criticality of services, infrastructures and supporting network assets, MS should define criticality criteria in order to identify the critical assets and examine the system in its entirety rather than per constituent. At least four types of dependencies should be taken into consideration:*

- *Interdependencies within a critical sector (intra-sector)*
- *Interdependencies between critical sectors (cross-sector).*
- *Interdependencies among data network assets.*

*Moreover dependencies can be found at the national and international level (cross-border), further complicating the task to have a complete overview.*

***Member States should foster baseline security guidelines for communication networks used for critical services.*** *To ensure the resilience of critical networks, the Critical Infrastructure operator or asset owner should adopt security guidelines to be used also at procurement stage. For this reason a checklist with baseline security guidelines for communication networks used for critical services should be made available to align practices across the EU.*

***Member States should foster the adoption of automated procedures for CIIs tagging in order to be prepared to face future challenges.*** *To foster the security of critical networks, MS should work together with CIIs asset owners in developing a common approach to the 'Tagging' of CII assets. This could allow automated-prioritized handling of incidents affecting Critical Information infrastructures.*

# Table of Contents

Executive summary iv

1 Introduction 1

2 Overview of the Member States' approaches to CIIs identification 4

3 Stakeholders involved in the identification of CII assets and services 9

3.1 Operators of Critical Infrastructures 9

3.2 Electronic Communications Operators 10

3.3 National Cyber Security Agencies 11

3.4 National Regulatory Authorities 11

4 Overview of methodologies in the identification of CIIs assets and services 13

4.1 Non Critical Service (CS)-dependent approach: Network architecture analysis 13

4.2 Critical service (CS)-dependent approaches 14

4.3 Steps in critical services based methodologies 14

Step 1: Identification of critical sectors 14

Step 2: Identification of critical services 15
The State-driven approach 15
The operator-driven approach 16

Step 3: Identification of critical information infrastructure network assets and services supporting critical services 16

Examples of MS using the service driven approach 19
Estonia 19
Czech Republic 19

Comparison of the different approaches 20

5 Challenges in identification of CIIs assets and services 22

5.1 Identification of critical sector and services 22

5.2 Criticality criteria and dependencies assessment 24

5.3 Effective collaboration: tagging of CIIs assets and centralized views 25

**6 Recommendations 27**

**References 28**

**Annex I – Legislation in EU and MS 30**

European Union 30
Austria 30
Finland 30
France 31
Germany 31
Hungary 31
Greece 31
Italy 31
Latvia 31
Netherlands 31
Poland 31
Romania 31
United Kingdom 31

**Annex – II List of acronyms 32**

# 1 Introduction

Communication networks are an important component of the life of millions of European citizens. These networks represent the fabric of the future information society and provide the means for the single digital market. Some parts of these communication networks are also vital for the operations of Critical Infrastructures (CIs) which are fundamental for the function of modern society.

Every day, the majority of Critical Infrastructures such as water management, heating supply chains and public transport systems among others, depend on the correct function of communication networks that support their operations. These supportive systems and networks, commonly referred to as Critical Information Infrastructures (CIIs), are core pillars for the function of the economy and society and a cyber-attack or an outage affecting these assets and services could have cascading effects on large part of the population[1].

In order to properly identify and secure these critical network assets, ENISA focuses this year on how Member States (MS) identify CIIs in communication networks in Europe.

## Scope of the document

Identification of Critical information infrastructure is the first step in the process to secure and protect the availability of critical assets. Several Member States have launched different initiatives regarding this topic while others are starting now to develop their own approaches. This study analyses how Member States have developed methodologies to identify CIIs in communication networks.

The definition of CII is taken from the Council Directive 2008/114/EC on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection[2].*"ICT systems that are Critical Infrastructures for themselves or that are essential for the operation of Critical Infrastructures (telecommunications, computers/software, Internet, satellites, etc.) "*

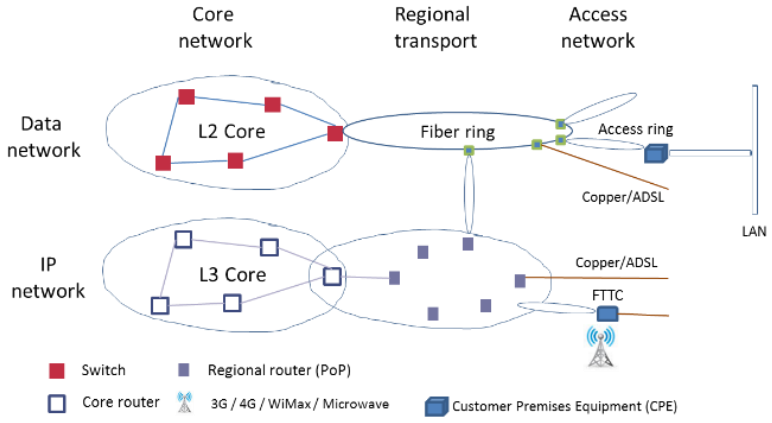


**Figure 1: Perimeter of the study - Data and IP networks**

[1] Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E., & Havlin, S. (2010). Catastrophic cascade of failures in interdependent networks. Nature, 464(7291), 1025-1028.

[2] European Commission. (2008). Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection. Official Journal L, 345(23), 12.

In this report the centre of interest is communication networks, including the Internet, public data communication networks and relevant assets in private data communication networks. The perimeter of public versus private network infrastructure is depicted in the following table. Private networks can be deployed within the private perimeter (e.g. LAN, Wi-Fi), as well as connecting private networks to each other and to the external world. The separation between public and private is not necessarily spatial (e.g. for wireless connectivity). Long distance (WAN) private networks are commonly available to companies that operate transmission/transportation infrastructures, which can in parallel be used for private communication network (e.g. fibre optic cable) deployment.

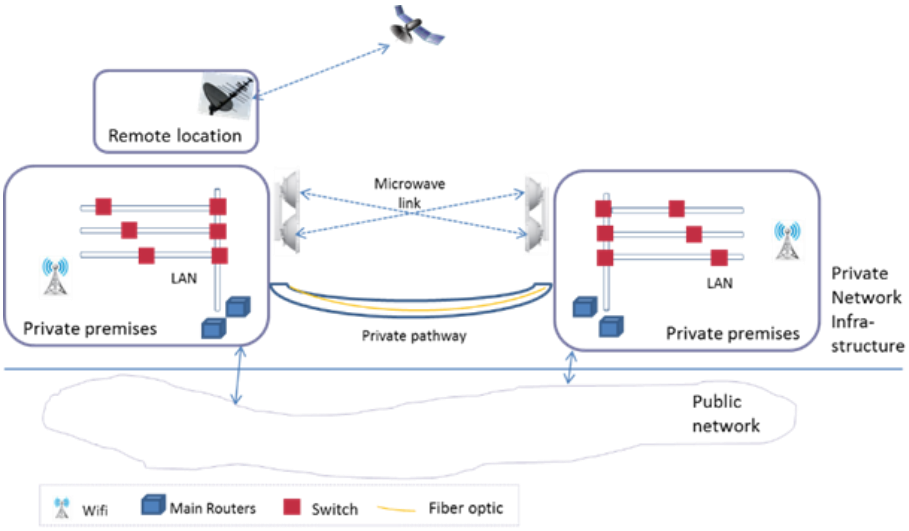


**Figure 2: Perimeter of the study - Private and Public IP and data communication networks**

## Target audience

This document is aimed at Member States that are interested in identifying CIIs assets and services in the area of communication networks. The target community consists of decision makers in mandated agencies/functions or National Regulatory Authorities for communication networks (NRAs) in charge of the definition of methodologies to identify Critical Information Infrastructures.

Due the multi-layered interdependencies involved in Critical Information infrastructure protection, this study covers also the perspective of critical infrastructure assets owners and operators that should be involved in any related initiative in the security and resilience of these assets.

## Goal

The goal of this study is to provide an overview of existing approaches in identification of CIIs across Europe and understand the dynamics of this complex multi-layered environment which involves not only operators of critical infrastructures but also network operators and mandated agencies. In doing so, also gaps and future challenges will be underlined and recommendations will be proposed to foster security and resilience of these critical communication networks. Specifically, this study investigates how to

1. define Critical sectors and Critical services supported by electronic communication networks
2. identify CIIs assets and services which support these critical services
3. strengthen & protect the identified CII in concert with the asset owners.

From the point of view of CI/CII assets owners and operators, the objective is to support them in the identification of their CIIs assets and ensure the protection of their critical assets in concert with the mandated agency of the MS. The aim is to identify the network assets that needs to be secure, and in case of outages, ensure resilient interconnections. In absence or with minimal availability, services essential to Critical Infrastructures can severely hamper the functioning of society.

## Methodology

The methodology for this study is organized in three steps:

1. Information gathering:
    - Desktop research of 760 documents regarding MS legislation and initiatives in the area of infrastructure security and resilience including identification of public and private stakeholders being responsible for managing these initiatives, frameworks for categorization of assets in electronic communication networks, with special focus on CIIs and relevant research
    - 35 online surveys answered by NRAs, Cyber Security Agencies, Contingency Agencies, CERTs, network operators and operators of Critical Infrastructures
    - 11 focused interviews performed with NRA, Cyber security Agencies, network operators and operators of Critical Infrastructures.
2. Analysis: based on the result of the desktop research, an analysis was performed to identify current maturity levels in identification of critical sectors, assets and services, good practises and possible challenges.
3. Validation session: to validate the findings and propose a portfolio of solutions that would fit all needs:
    - Validation session workshop http://europa.eu/!qU87Rd with cyber security agencies, network operators, operators of Critical Infrastructure and academia.
    - Extensive online feedback via NRAs, Cyber Security Agencies, Network operators and operators of Critical Infrastructures who participated at each part of the study, EU Critical Infrastructure point of contacts in each MS and ENISA Internet Infrastructure Security and Resilience Reference Group.

## Structure of this document

This document is structured as follows:

- Introduction - Introduction and general overview
- Chapter 2 - Outline of the MS status regarding the identification of critical sectors, assets and services and definition of critical information infrastructures
- Chapter 3 - Summary of the perspective of the different stakeholders involved
- Chapter 4 - Overview of methodologies of identification of critical information infrastructures
- Chapter 5 - Possible improvement to fill existing gaps and be prepared for future challenges
- Chapter 6 - Recommendations

# 2 Overview of the Member States' approaches to CIIs identification

During the information collection period, an effort was made to depict the current status in the 28 EU Members States regarding the definition of CIIs and the methodologies to identify specific network assets and services. Thanks to desktop research analysis, the 35 online survey responses and 11 interviews with the relevant stakeholders, it was possible to collect information to have an overview of the current definition in 23 Member States and related research. The goal was to depict in which country a clear definition of CII is present and which is the level of CII identification methodologies and related activities.

Starting from the European definition[3], the goal was to recognise how MS identify CIIs at national level and develop their own definition and methodologies to translate it in actual network assets and services that need to be secured and resilient. For this, all relevant and available legislation in each MS, with focus on communication networks, was analysed. For reference please refer to **Annex I – Legislation in EU and MS**.

The following key findings and conclusions can be drawn from the analysis of the information that has been collected regarding legal, regulatory and strategic initiatives undertaken in 23 Member States concerning the identification of critical sectors, assets and services.

The main starting point for identifying CII assets and services are the CI depending on them, given that critical infrastructures (e.g. transportation, finance, electric power and water) are increasingly dependent on the evolving information infrastructure for a variety of information management, communications and control functions[4]. In turn, CIs are defined on the basis of critical sectors / services.

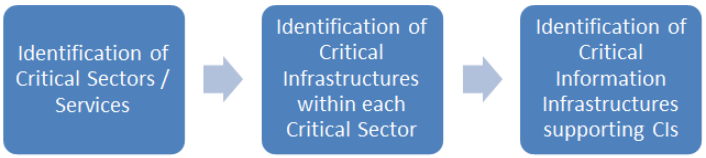


**Figure 3: Critical sectors and infrastructures identification flow**

In the Green Paper on a European Programme for Critical Infrastructure Protection[5], the European Commission provides an indicative list of 11 critical sectors:

i. Energy
ii. Information, Communication Technologies (ICT)
iii. Water
iv. Food
v. Health
vi. Financial

[3] Council Directive 2008/114/EC on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection :"ICT systems that are Critical Infrastructures for themselves or that are essential for the operation of Critical Infrastructures (telecommunications, computers/software, Internet, satellites, etc.) "

[4] Centre for European Policy Studies (2010), "Protecting Critical Infrastructure in the EU", CEPS Task Force Report, 2010

[5] Commission of the European Communities (2005), "Green Paper on a European Programme for Critical Infrastructure Protection", COM (2005) 576 final

vii. Public & Legal Order and Safety
viii. Civil Administration
ix. Transport
x. Chemical and Nuclear Industry
xi. Space and Research

This list is not used as such across all MS; rather, countries have put in place their own list of critical sectors since not all sectors are relevant for all countries. Furthermore, based on the special characteristics and peculiarities of each country, the list may need to be enriched with new sectors. For example, the nuclear industry is only relevant for countries that have nuclear plants, whereas a few countries have identified as critical the emergency and / or rescue services, which are not included in the list proposed by the European Commission.

It is also important to underline how some countries may use different terms as it is the case of France where the term "point d'importance vitale" is used or Estonia which defines vital services instead of critical sectors.

The table below gives an overview of the mapping of the critical sectors identified by each country[6].

| Sectors | Energy | ICT | Water | Food | Health | Financial | Public & Legal Order | Civil Admin. | Transport | Chemical & Nuclear Industry | Space & Research | Other | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AU | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | | |
| BE | ✓ | ✓ | | | | ✓ | | | ✓ | | | | |
| CZ | ✓ | ✓ | ✓ | ✓ | | ✓ | | ✓ | ✓ | | | Emergency services | |
| DK | ✓ | ✓ | | ✓ | ✓ | | | | ✓ | | | | |
| EE | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | Rescue services | |
| FI | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | | | | |
| FR | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | Industry | |
| DE | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | | | Media & Culture | |
| EL | ✓ | | | | | | | | ✓ | | | | |
| HU | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | | | Industry | |
| IT | ✓ | | | | | | | | ✓ | | | | |
| MT | ✓ | ✓ | | | ✓ | ✓ | | ✓ | ✓ | | | | |
| NL | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | | |
| PL | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | | Rescue systems | |
| SK | ✓ | ✓ | ✓ | | ✓ | | | | ✓ | | | Industry | Postal |

[6] Information is presented for 17 EU Member States and Switzerland since for the remaining EU MS either no information was found during the desktop research or the related information is available only in the local language.

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **ES** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | |
| **UK** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | | Emergency services |
| **CH** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | | Industry |

**Table 1: Critical sectors per country**

After the analysis of how CI are defined in the Member States that were studied, the following step was to understand CII efforts and existing approaches to identify critical communication assets and services.

Firstly, it was understood that the significance of CII Protection has been acknowledged by the majority of the Member States. This has been dealt with either in the framework of their CI Protection programmes and initiatives or as part of the development of their cybersecurity strategies. This means that usually there are no dedicated strategies for the protection of CII but rather refinements and adjustments are made to existing strategies and concepts on CI protection in order to accommodate issues related to the protection of information infrastructure.

Secondly, based on the information gathered, it was possible to note that that there are different maturity levels with regards to CII activities across the MS. On the basis of the collected information, four different maturity levels could be defined as presented in the following table:

| | |
|---|---|
| Level 1 | Absence of activities related to the protection of critical information infrastructures. Under this category fall MS that have just transposed the EC Directive 114/2008 and have identified only transport and energy as critical sectors. |
| Level 2 | Identification of the ICT sector as one of the critical sectors that should be addressed. Under this category may fall MS that have acknowledged the Information and Communication Technologies sector as one of the critical sectors for the maintenance of the vital societal functions. |
| Level 3 | Development of a general methodological framework for the identification of CI assets. Member States that have in place a detailed methodological approach for the identification of CI assets and services, with specific steps and responsibilities assigned to involved stakeholders, may be classified into this category. Since the focus is on CII, It is a prerequisite that MS have acknowledged ICT as one of the critical sectors. |
| Level 4 | Development of a definition for CII and establishment of specific criteria for the identification of CII assets. Under this category fall the Member States that are mostly advanced in the area of CIIP and have taken specific measures for the identification and protection of CII assets. |

**Table 2: Maturity levels in identification of CIIs**

These maturity levels range from the absence of activities related to the identification of CII to the establishment of specific measures for the identification and protection of CII assets. Based on the information gathered, it was possible to place the analysed MS on the following continuum that represents their indicative state of the art.

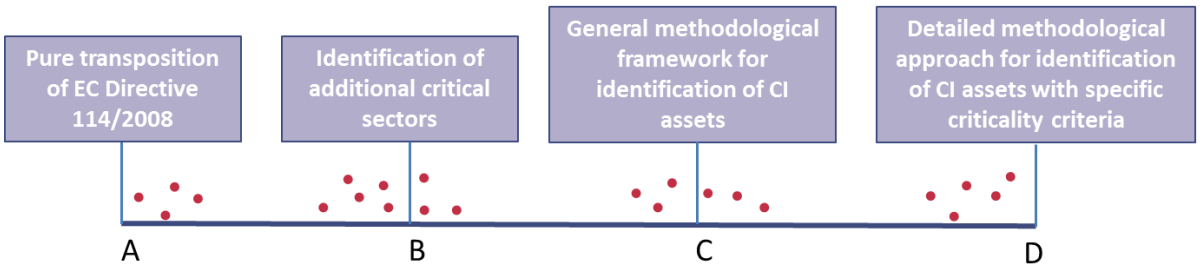


**Figure 4: CI identification maturity continuum and MS positioning**

As presented in this section, 17 Member States of the 23 covered in this study have addressed the issue of **identification of critical sectors**. In these MS there is a **list of critical sectors and in certain cases also subsectors and related critical services. The lists** have been prepared taking into account national priorities, related EC Directives and specific country characteristics. A structured methodology is present only in 5 MS while the other MS are either at the early stage of CII identification or are defining the legislative decrees for the definition of the methodology in this moment.

When focusing on identification of CIIs in the area of communication networks, from the online survey and the follow-up interviews it was possible to identify that:

- a **significant number of Member States present a low level of maturity** and lack a structured approach
- challenges are posed by the **identification of critical services** and the complexity of the definition of **criticality criteria in order to identify the critical assets**.
- there is the need for **effective collaboration between public sector (Government & mandated Agencies) and the private sector, which often controls numerous critical infrastructures**

The major considerations can be summarized as follows:

- **The differences observed in the CIIP maturity level across the various MS seem to be aligned with the variance observed in the overall MS maturity concerning ICT** as illustrated by the Network Readiness Index (see table below). The World Economic Forum's Networked Readiness Index (NRI)[7] measures the propensity for countries to exploit the opportunities offered by information and communications technology (ICT) taking into consideration ten factors. An analysis of the NRI results shows that while many European countries are leading in the rankings, many others lag behind.

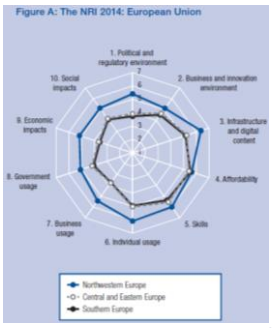


**Figure 5: The Network readiness index (2014) in EU[8]**

[7] The World Economic Forum's Networked Readiness Index (NRI) http://www.weforum.org/issues/global-information-technology/the-great-transformation/network-readiness-index

[8] World Economic Forum (2014), The Global Information Technology Report 2014, p.19

- A comparison of the implementation level with the NRI of the individual MS suggests that MS with lower NRI rankings exhibit also a lower regulatory maturity level regarding CIIP. This can be justified by the **lower degree of ICT adoption for the support of critical services. This pushes down in the scale of priorities the need to focus on the identification and protection of critical information infrastructures**.

# 3 Stakeholders involved in the identification of CII assets and services

As underlined in the previous chapter, an issue that emerged from the online survey and the follow-up interviews is the fundamental need for **effective collaboration between public sector (Government & mandated Agencies) and the private sector, which often controls numerous critical infrastructures.** This is due to the complexity of interdependencies, the role of the asset owners and efforts to make these assets secure and resilient.

When it comes to CIIs, given the criticality of certain services offered to the public, the population and the geographic scope supported, a business risk may become national risk, and in such a case, the service providers are defined by the mandated agency as operators of CIs.

The operators of CIs need to identify and classify the communication network infrastructures supporting critical applications, according to their criticality. They are responsible for determining the core processes, the respective applications and, as a last step, the network assets and services (connectivity solutions) which are used to operate the respective applications. An asset can be critical related to (a) the business value, (b) the scope of the population served or (c) the technical dependence of critical applications and this classification depends on the sector and the role of the CI.

For these reasons, parallel to the mapping of different approaches on identification in the different MS, an effort was made to investigate the views of the stakeholders that could be involved in the identification of critical assets and service used in communication networks, namely:

- Operators of Critical Infrastructure,
- Electronic Communication Providers,
- National Telecommunications Regulatory Authorities
- Cybersecurity Agencies.

In the following paragraphs, the main points that were highlighted in the framework of the online survey and the follow-up interviews are summarized per stakeholder category.

## 3.1 Operators of Critical Infrastructures [9]

Operators of CIs are the asset owners and commonly face major risks which may have a detrimental effect on society and the depending vital societal functions. These risks may be directly linked to the critical service provided or emerging from activities that are not related to the core business of the operator of CIs. During the discussion with this type of stakeholder it was underlined that:

- Operators of CIs are in charge of operating and securing their infrastructures, whereas in several Member States they are legally obliged to carry out a risk assessment analysis and submit business continuity plans to the responsible Government authorities.
- In certain industry sectors they are also obliged to comply with certain regulations which may have impact on the operation, infrastructures and data networks used, an example would be the Finance sector.
- In order to comply with regulations, operators of CIs classify their infrastructures and processes as well as the respective supporting applications/information.
- In certain cases, operators of CIs have a highly diversified portfolio of services and respective infrastructures. Such operators need to apply a diversified approach according to service criticality.

[9] The terms 'Critical Service Provider' and 'Critical Infrastructure Operator' reflect highly complementary roles

## 3.2 Electronic Communications Operators

Several network operators participated in the study, providing useful insights regarding their role in securing and protecting CIIs and the level of maturity of the market, in general. Network operators are not responsible for classifying infrastructures as CIIs. Usually the designated operator of CI is required to identify their relevant CII assets and services and prepare a plan to better protect them. This also means that contracts and relevant Service Level Agreements (SLAs) are renewed, based on the operator of CIs demands.

Network operators expect to see an increasing demand for secure and resilient connectivity solutions, based on evolving technology, and need to prepare for this. Thus the network operators, active in a competitive market and complex evolving technological landscape, have to continuously improve, in order to be able to provide increasingly resilient and secure CII, connectivity solutions and interconnection services, based on more demanding SLAs.

Specifically:

- Network operators are not responsible for classifying infrastructures as CIIs. Currently there is no such legal obligation in any Member States, and such a responsibility is not foreseen to date. This may be a MS responsibility, in certain cases legislated but, as it was possible to note above, this varies in maturity and efforts. Therefore the designated operator of CI is commonly required to identify their relevant CII assets and services and prepare a plan to better protect them. This may involve enhancing security and resilience features of the connectivity solutions which support their CI(s). This also means that contracts and relevant SLA are renewed, based on the requirements of the operator of CIs and specific procurement requirements are defined for those assets and services which are defined as critical and which will be covered in the chapter ad-hoc.
- The process to strengthen and/or enhance security and resilience of CII is usually business-driven in order to fulfil the CI operator's requirements. In certain cases, CI operators are driven by the need to comply with regulations, with implications on network security and resilience. In other words, the network operators receive service requests from the CI operator or asset owner to render their connectivity services more secure and resilient, to guarantee the operations of the CIIs enabling their critical services.
- In order to ensure the resilience of critical external networks, the CI operator or asset owner set related requirements at the procurement stage and uses multiple and physically separated network paths. In addition, they put in place SLAs. Regarding the security of external networks, CI operators or asset owners follow different strategies. All CI operators or asset owners set requirements at the procurement phase for business data protection on the external network. Sometimes the network operator is constrained by external factors when deploying resilient connectivity, such as administrative permissions, delays introduced by other service providers of the same operator of CIs. Thus SLAs should take into account such situations, to protect the NOs.
- Network operators expect to see an increasing demand for secure and resilient connectivity solutions, based on evolving technology, and need to prepare for this. Thus the network operators, active in a competitive market and a complex evolving technological landscape, have to continuously improve, in order to be able to provide increasingly resilient and secure CII (connectivity solutions and interconnection services), based on more demanding SLAs. Therefore, they have to be able to offer connectivity solutions with higher redundancy & increased capacity exploiting all access technologies available (wired & wireless). Moreover, they have to be able to offer complex SLAs related to connection availability/performance/security.

- Regarding the network operators' Business/Operations Support Systems (BSS/OSS) functionality to support internal processes related to CIIs, the overall impression is that currently there is no particular deployment of functionality to support a differentiated provisioning & assurance process for CII related solutions. The sophisticated OSS approach involves the deployment of an SLA management platform which may auto- interact with the network assets 'linked' to the 'customer facing service', in order to support a complex and demanding SLA.
- The evolution of CII related SLAs, requested by the CI operators, to assure the provision of increasingly resilient and secure CII, will apply pressure for the deployment of more sophisticated BSS/OSS; this in return shall allow for automated-systematic handling of complex SLAs, while containing the operation cost.
- Automation of provisioning and assurance processes is the key to effective and efficient CII operation. The achievement of a high degree of automation is a challenging task for each NO in a complex & evolving network infrastructure landscape.

## 3.3 National Cyber Security Agencies

National Cybersecurity agencies may have a leading role in all activities related to the identification and protection of CIIs, one example is ANSSI in France. Depending on their mandate, they can be involved in the:

- Development of legislation (laws and implementing decrees) related to identification and protection of CIIs
- Supervision of the implementation of the relevant legislation by the involved parties
- Review and audit of the CII-related parts of the security plans developed by the CI operators.
- Continuous consultation with critical asset owners in the framework of established public-private partnerships
- Cooperation with asset owners on asset loss.

Cybersecurity agencies that participated in the survey underlined that:

- **Collaboration among organizations is an important factor** (if not a prerequisite) for the successful implementation of CIIP-related initiatives and programmes. This collaboration involves both the collaboration between industry and state as well as cross-sector cooperation. In some cases, Public-Private Partnerships have been established in order to foster the cooperation on the basis of mutual trust (e.g. the UP KRITIS initiative in Germany[10]).
- Business-risk management is not sufficient when vital societal functions are at stake; rather, **society-based risk management is required given that the implications of the potential failure of a critical service exceeds the boundaries of a specific provider and affects the entire society[11]**.

## 3.4 National Regulatory Authorities

As for cybersecurity agencies, National Regulatory Authorities for communication networks may have the mandate for CIIs depending on the national legislation. From the information gathered during the online survey and interviews, it was possible to understand their role and challenges such as:

[10] German Internet platform on Critical Infrastructure Protection http://www.kritis.bund.de/SubSites/Kritis/EN/Home/home_node.html

[11] Swedish Civil Contingencies Agency, A first step towards a national risk assessment https://www.msb.se/en/Products/Publications/Publications-from-the-MSB/

- The **pronouncing of a specific infrastructure as critical may depend on the size of the affected population, the cross-sector dependency and the geographical impact**. Moreover, **personal safety and impact on privacy** were also mentioned as important parameters in one case.
- Responding National Regulatory Authorities (NRAs) publish **guidelines for issues ranging from CII vulnerabilities and CII procurement to Internet infrastructure resilience**. The majority of them have a formal or informal participation in security related info exchange platforms.
- **Audits of operators of CIs and network operators regarding CIIs security/resilience are performed annually** by most of the responding NRAs and are partially based on specific standard requirements. In case of non-conformities, usually there is a recommendation and / or order to rectify the error and if not rectified a fine may be imposed. These are performed on an ad-hoc basis and ISO-27001 is taken as a basis for specific points of the audit.
- **Public-private partnerships for resilience** are already in place or planned in several countries, whereas the responding agencies take part in cross-border collaboration activities for the enhancement of CII resilience in their own country.

As part of the survey the NRAs were also asked which actions would be interesting to meet the needs of securing CII in the future. While not exhaustive, these should be seen as directions for areas of research. Some ideas that emerged among others are:

- Deploy information systems, which would support **automated-prioritized handling of incidents affecting CII so** that incidents that involve CIIs' networks assets are notified automatically and the handling is prioritized.
- Maintain a **database** which includes the following information entities:
    - CIs and the relevant critical service(s) they provide
    - CIs and relevant data (location) and potential dependencies
    - CIIs and the communication operator which operate those CII
    - Role/person responsible for the CII

Based on this database, agencies mandated on CIIs should consider implementing/deploying an Information Security Management System (ISMS), related to **CIIs incident handling**. This ISMS should support classified/diversified CIIs incident handling.

- The above CIIs database could be linked to an incident alert system, in order to **auto-identify CII and handle CII alerts in a diversified mode.**
- Given an incident outbreak:
    - a **preliminary damage assessment** procedure followed could **be prioritised/diversified for CII**
    - the rules are stricter for CIIs in the "chain of custody" documented for the evidence collected
- **Statistics** on security incidents could be kept with distinct reference to CII.
- Conduct **root cause analysis** in case of an incident, in a diversified mode for CIIs (e.g. all cases involving CIIs are handled, **higher priority given**, more effort made, analysed in more depth).

# 4 Overview of methodologies in the identification of CIIs assets and services

In this section, an overview of different methodological approaches is given. Those approaches were identified either during the desktop research or are already being implemented by some MS in the framework of their overall strategy for the identification and protection of CI.

The goal is to evaluate the critical network assets on which MS depend, and ensure that they are sufficiently resilient. Operators of CI/CIIs commonly operate applications which are used to manage/control the critical services offered and/or the CI which support the provisioning of those critical services. For these reasons it must be possible to identify these specific assets.

As it emerged during the study, two broad categories of approaches can be identified:

- **A non Critical service** dependent approach that does not involve an analysis of the supported critical services; instead it only looks at the network infrastructure. **For the time being, no MS is using this approach but it is a wide known practice in the private sector to map networks**.
- **Critical Service (CS) dependent approaches** that start with the identification of critical services and then, based on the services, tries to identify which assets are belonging to these services and therefore can be considered as CII assets and services. **This methodology is based on the impact that the disruption of a service can have on the vital functions of the society** and mainly two different approaches are used by different Member States: the state-driven and the operator-driven.

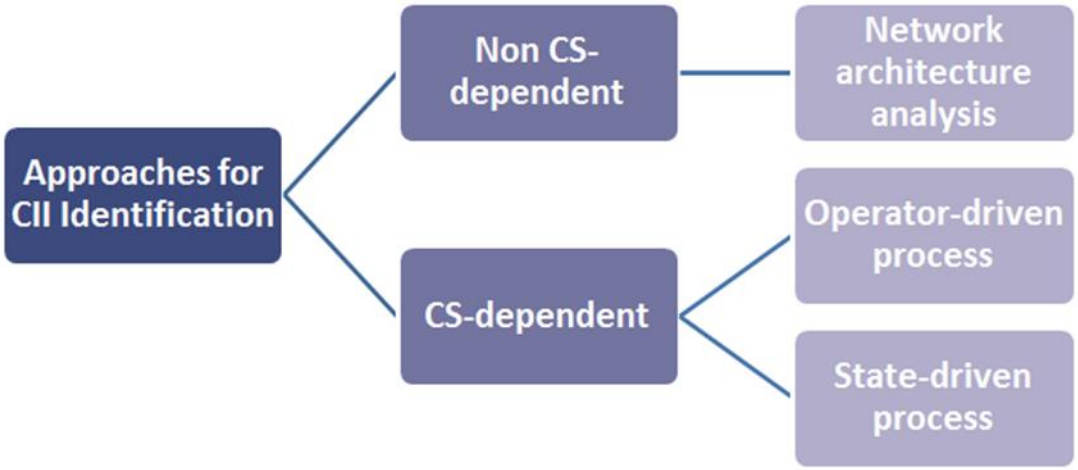


**Figure 6: Methodological approaches for Critical Information Infrastructure identification**

## 4.1 Non Critical Service (CS)-dependent approach: Network architecture analysis

The "***Network Architecture Analysis"*** approach involves the analysis of the national network as a whole, so that the Member State develops a national overview of the data network Infrastructure. More specifically, it involves:

- The **analysis of the IP and data network, the traffic load patterns, and failure patterns**.
- The **identification of components**, which are critical to the operation of the overall network or a major part of the network (e.g. core network, links that serve a significant percentage load or a significant share of international traffic).

This approach constitutes the **traditional commonly applied approach in mapping, analysing and protecting the network components**. It is based on the fact that the core network and certain additional components serve the majority of the traffic; therefore they should be designed in a resilient manner. It is expected that all network operators review, analyse and take actions to assure & gradually enhance the resilience of the critical network components. Therefore**, public private collaboration should be developed to have a holistic view of the network architecture**.

The main drawback of this approach is that **it ignores critical services**, served by the connectivity solutions since it looks directly at the network infrastructure as a whole. Furthermore, it **does not identify access network components which architecture-wise may seem insignificant, but may be critical to a critical service's connectivity**. Moreover, due to the overall infrastructure point of view, **it involves a high degree of complexity, which increases significantly when dealing with the lower network hierarchy levels (transport and access network) and the relevant components / assets**.

## 4.2 Critical service (CS)-dependent approaches

Critical service-dependent approaches follow a three-step procedure as depicted in the following table. In this case, some **MS first identify the critical sectors and then for each one of the critical sectors they proceed with the identification of critical services, critical applications and finally critical information infrastructure assets**. In the following paragraphs, we detail each individual step and then we present two MS that use this approach.

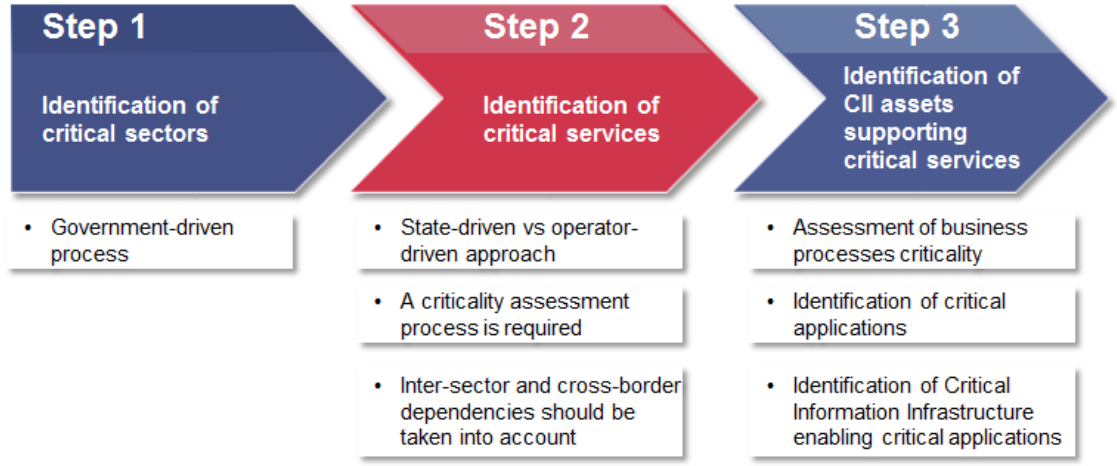


**Figure 7: Steps of Critical Information Infrastructure identification in a CS-dependent approach**

## 4.3 Steps in critical services based methodologies

In this section we detail each individual step in the identification of CIIs and regarding the identification of critical services, we also provided an overview of the two different approaches used by different member states, the state-driven approach and the operator-driven approach.

### Step 1: Identification of critical sectors

As presented in Section 2, Member States have addressed the issue of identification of critical sectors to a greater or lesser extent and all have a longer or shorter **list of critical sectors**, which has been prepared taking into account national priorities, related EC Directives and specific country characteristics.

## Step 2: Identification of critical services

Once the critical sectors are defined, the next step is to define the critical services such as for example water management, heating supply chains and public transport systems. At this point, we may differentiate between two approaches based on **who assumes the leading role for the identification of the critical services**:

a) the ***state-driven approach*** where the leading role is assumed by the government agencies that have the mandate to identify and protect CI - in most of the cases the responsible ministries.
b) the ***operator-driven approach*** where the leading role is assumed by the Critical Infrastructure Operators.

### The State-driven approach

In the case of the State-driven approach (in this report also called 'critical service-driven'), the whole process is guided by the governmental agencies that have the mandate to identify and protect CIs. Having decided on the critical sectors, they apply a method to systematically identify critical services. Next, they identify the operators of CI involved in these services. The identification of specific assets may be performed in collaboration, aiming at assuring effectiveness, aligned with societal needs.

This approach and its steps are presented in the following table. Basically the CII/CIIP mandated organizations define the list of actual critical services and notify the operators of these services. The operator of CIIs is therefore in charge to define the specific network assets and appropriate measures to ensure security and availability of the connectivity. The mandated agencies then review the plan and periodically update the list of critical services due to continually changing threat landscape.

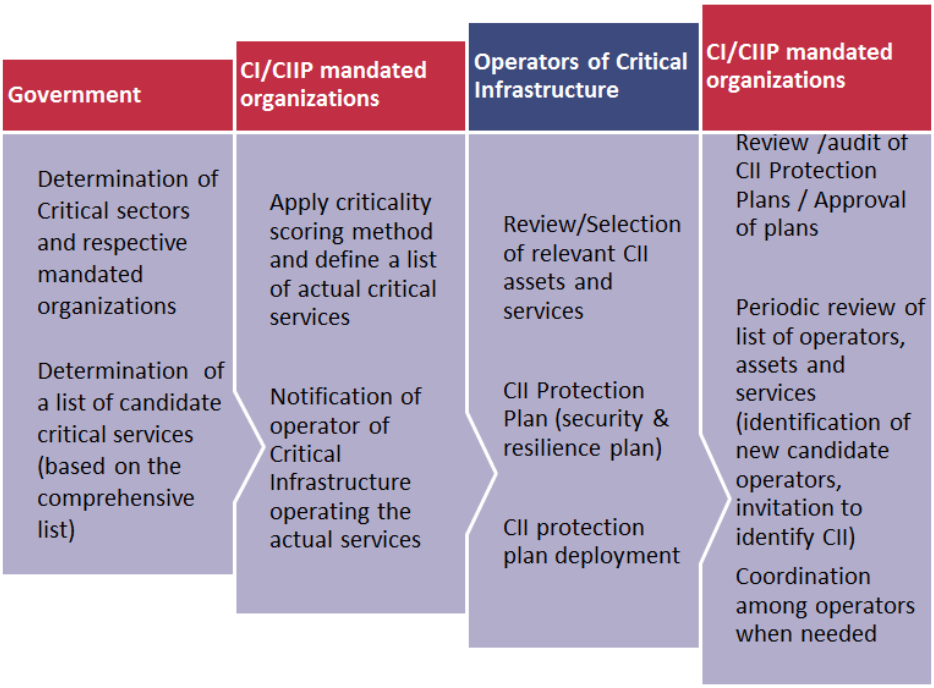


**Figure 8: State-driven approach – Steps followed and parties involved**

### The operator-driven approach

In the case of the operator-driven approach, the leading role is assigned to the operators of CIs. The Member State identifies a list of operators (called also 'vital operators'), who are responsible to identify the individual critical services and assets that comply with a number of risk analyses and risk management directives. Then, the responsible ministries review the selected services and assets along with the drafted CI protection plans.

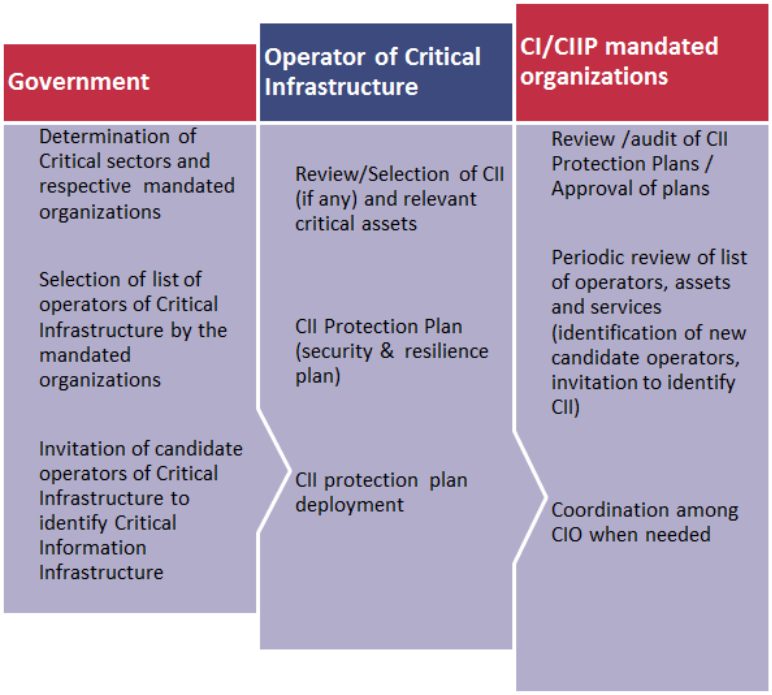


**Figure 9: Operator-driven approach – Parties involved and steps followed**

The ministries identify the "vital operators" or the "vital service providers" within their own area of responsibility and these operators are then legally bound to perform a risk assessment analysis, identify a list of individual critical assets and develop CIIP structured plans. In this approach the identification of the critical services is the responsibility of the operators. A typical example can be found in France (instruction 6600/2014). This is a pragmatic approach given the current state of the art of CII identification since operators have a better knowledge of their infrastructures. It also represents a shift of the effort needed to the operator to which is delegated the accountability.

## Step 3: Identification of critical information infrastructure network assets and services supporting critical services

Following the identification of critical services, the final step is to identify and classify the CII network assets and services supporting those critical services. This step represents the final phase of the translation of high level legislation into actual critical network assets and services that need to be secured, resilient and monitored.

These assets and services are part of a business supply chain. And as it was underlined at the beginning, due to their criticality, the associated business risk become national risks where the perimeter is now the business operations in provisioning that specific service.

The criticality of each business process supporting the operation of a critical service can be assessed based on the impact it has on the predetermined service operation frame. Such impact factors may be:

- Service Consumer (Citizen /Customer) experience with reference to service consumption (e.g. electric power cuts due to power transmission process malfunction)
- Process malfunction leading to service malfunction or outage (e.g. fault handling process malfunction and degradation lead to significant delay in fault resolution prolonging a service outage)

Similar analysis approaches based on the 'supply-chain and value-chain perspective', have been proposed [12] in order to assess dependencies and cyber-asset criticality.

An overview of core processes and relevant indicative applications for a utility service (e.g. power, water, and telecom), is presented in the following table. The picture tries to depict all the processes involved when providing a critical service and the components that should be taken into consideration in assessing and protecting critical assets and services. Moreover, the provision of critical services consists of several business processes, which in their turn are supported by business applications that need to be served by a communication network. Therefore, communication networks are of paramount importance for all stages involved in the provision of critical services, i.e. service fulfilment, service operation and service assurance.

The operation of many critical applications supporting critical service processes may be fully dependent on communication networks. This is commonly the case when data (e.g. measurement/status data, transaction data) are captured at various geographic locations and transferred via the data network to a central point for processing by the critical applications, which is the case in all ICTs applications.

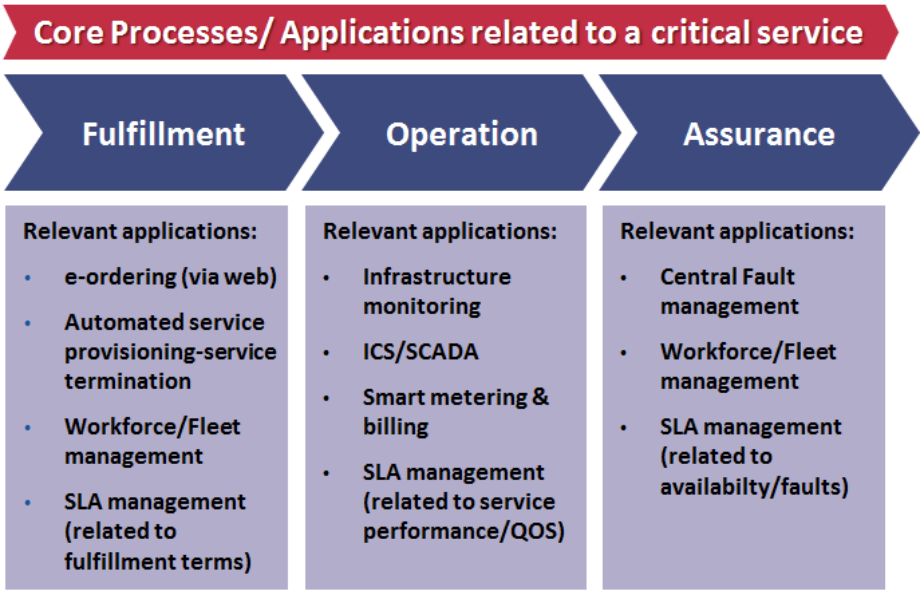


**Figure 10: Indicative core processes and applications supporting a critical service**

Since communication networks are sector agnostic and the asset groups are usually the same,[13] independently of the critical service supported, an indicative list of potential CII assets, identified using the presented methodology and located at the access network, could look like this:

- Fiber ring supporting a critical link (e.g. a datacentre physical connection)

[12] Multinational Experiment 7 Outcome 3 – Cyber Domain Objective 3.1, Threats and Vulnerability Methodology , 2.2.1 Analysis of supply chain and value chain

[13] ENISA Technical Guideline on Threats and Assets https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets

- Fiber cable from local exchange to local cabinet as for Fibre-to-the-Cabinet (FTTC) solutions
- Customer Premises Equipment(CPE), e.g. Fiber termination equipment, router, DSL modem/router, switch supporting a carrier ethernet connection at an operator of critical infrastructure
- Microwave equipment supporting a point-to-point access link
- Worldwide Interoperability for Microwave Access (WiMAX) equipment

It must be underlined that this is only an example and the actual list depends on the critical service supported, the different characteristics of the MS and of the operator. The goal here is to give an example of the actual network assets that should be identified using this methodology.

Regional/area network components supporting the CII could also be critical assets. These may be:

- Digital Subscriber Line Access Multiplexer (DSLAM) at the local exchange
- Broadband Remote Access Server (BRAS) connected to the DSLAM
- Router used to connect to the Internet
- GigaEthernet for backhauling (e.g. DSLAM to BRAS)

Core and transit network components are critical to CII, since they support a bigger part of the network. These may be:

- Backbone and (Border Gateway Protocol) BGP routers handling a significant percentage of the internet traffic
- Gigabit Ethernet switches used for the Carrier Ethernet (CE) service
- Backbone links handling a significant percentage of the traffic

The higher a network component is in the network hierarchy, the higher the probability that it serves one or more critical services. Moreover vulnerabilities which are affecting CII are not specific but they are commonly affecting all types of communication networks. Below follows an abstraction of the typical attack surfaces regarding physical and logical infrastructure that should be considered and it is valid for CII and also for all types of data and IP networks:

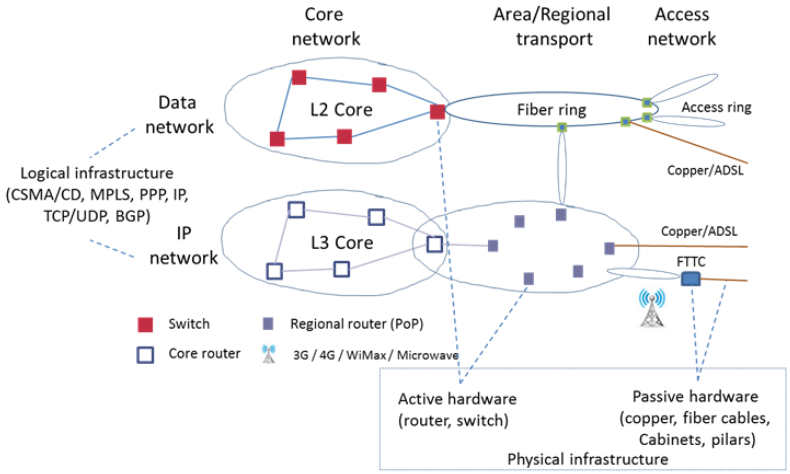


**Figure 11: Typical network attack surfaces**

## Examples of MS using the service driven approach

### Estonia

Estonia is one of the very few European countries that has developed a definition for the term of "Critical Information Infrastructure" and has assigned to a specific body the responsibility for the protection of Critical Information Infrastructures, RIA - the Estonian Information System Authority[14].

**Estonian definition of Critical Information Infrastructure**

Information and communications systems whose maintenance, reliability and safety are essential for the proper functioning of a country. The critical information infrastructure is a part of the critical infrastructure.[15]

The basis for Critical Infrastructure Protection in Estonia is the Emergency Act that was issued in 2009[16], which defines **an extended list of vital services, i.e. services that are essential for the maintenance of society, and the health, safety, security, economic or social well-being of people. Currently, this list consists of 43 services.**

Furthermore, Estonia has developed a **methodological approach for the identification of Critical Information Infrastructure assets**, which comprises the following steps:

a) **For each one of the vital services identified, a Ministry is appointed as 'service organizer'** and this Ministry is responsible to propose the **criteria and the criteria thresholds** in order to identify the vital service providers. For example, for the IT sector one of the used criteria is the number of customers served by a specific company.
b) Then, **the vital service providers carry out a risk assessment analysis** and draft a business continuity plan, which they submit to the responsible Ministry ('service organizer').
c) One of the outputs of the risk assessment analysis is the **list of critical IT resources,** which RIA is responsible to check and provide feedback on how this list could be improved.
d) Based on the outputs of the risk analysis assessments of all vital service providers, a **national list of critical information infrastructure is compiled**. Furthermore, a **national interdependencies analysis** is carried out based on the input provided by the vital service providers.

### Czech Republic

In the Czech Republic CIIs are identified through a specific process in accordance with Act no. 240/2000, on Crisis Management. A **CII is defined as an element of CI in the cyber security sector**. Every CI element (and every CII element) needs to fulfil **two sets of criteria**, which are **cross-cutting criteria and sectorial criteria**.

**Cross-cutting criteria define the gravity of malfunction or disruption of the system,** i.e. if it causes death to more than 250 people, or the economy of the state is damaged of more than 0,5% GDP, or it has serious impact on providing necessary services to more than 125,000 people, etc. **Sectorial criteria determine five areas within the cyber security sector where CII might be identified.** One of the most important sectorial criteria is that the **information or communication system significantly or completely affects the operations of other already identified element of CI, e.g. a communication system upon which the operation and security of a power plant is dependent.** CII can also be identified in the area of information systems administrated by public authority containing personal information about 300,000, and others.

**A CII is identified and determined by legal act.** If the CII is administered by a governmental department, the governmental resolution is issued. If the CII is administered by other (mostly private) bodies, the NSA CZE issues a specific general measure decision.

## Comparison of the different approaches

After the presentation of the different approaches and some MS examples, below the different advantages and disadvantages of each approach are listed. It is important to underline that the purpose of this study is to present the MS with a portfolio of methodological approaches – rather than a single 'fits-all' methodology – so that the MS can tailor the approach that suits better its own specific characteristics and needs.

| | Advantages | Disadvantages |
|---|---|---|
| **Network Architecture Analysis** | The **traditional commonly applied** approach in mapping, analysing and protecting the network components. This is usually employed **in the private sector**.<br><br>It is based on the fact that the core network and certain additional components serve the majority of the traffic, therefore they should be designed resilient**. It is expected that all network operators review, analyse and take actions to assure & gradually enhance resilience of the critical network components**.<br><br>Given that the ICT sector is commonly considered critical, its core infrastructures are CII. | **Ignores critical services**, served by the connectivity solutions (CII).<br><br>Requires an analysis of the overall national network (which means having an overview of the whole network infrastructure formed by the various network operators).<br><br>Cost-benefit criteria, used in network design & deployment decisions, may be analysed in financial terms only.<br><br>**It does not identify access network components** which architecture-wise may seem insignificant, but may be critical to a critical service's connectivity.<br><br>Complexity in mapping internet infrastructures, has been stressed in previous reports [17].<br><br>**Complexity is extremely high** when dealing with the lower network hierarchy levels (transport & access network) and the relevant components/assets. |

[14] https://www.ria.ee/en/
[15] https://www.ria.ee/CIIP/
[16] EMERGENCY ACT, passed 15 June 2009
[17] ENISA, Guidelines for enhancing the Resilience of eCommunication Networks

| | | |
|---|---|---|
| **State-driven approach / Critical services driven approach** | **More systematic**. If designed properly, it could be better aligned to the actual societal needs.<br><br>**Better assessment of the critical services**, the relevant value chain and involved parties. May involve a process spanning multiple CI/CIIs operators. Since relationships have a 'many to 'many' nature (e.g. critical service to operates), the service value chain complexity should be analysed early-on.<br><br>Done prior to the selection of the operator of CI/CIIs.<br><br>Better MS control of the process. | Detailed list of critical services is not always present in each MS approach<br><br>Define criticality criteria for the identification of critical assets is a challenging process especially regarding interdependencies aspects<br><br>The **complexity can be significant** (including cross-sector dependencies, cross-border CI issues). Requires a higher level of sophistication, in the initial analysis of services.<br><br>State-driven investment in the development/application of the method is needed. Any such approach has not been identified. |
| **Operator Driven approach** | **Pragmatic approach** given the current state of the art of CII identification since operators have a better knowledge of their infrastructures.<br><br>It also represents a shift of the effort needed to the operator to which is delegated the accountability. | Need for a strict rule set which has not been identified. Lack of rules (e.g. a uniform criticality level applied) may lead to **a non-homogeneous deployment of protection measures** (which would not assure alignment to societal needs).<br><br>The concept of **critical service** maybe under-examined (going directly from operator to critical assets).<br><br>Cross-sector or cross-operators critical service dependencies may be inadequately assessed.<br><br>**Need for strict audit on the identified CI assets**.<br><br>Relevant cost for the operator of CI/CIIs (to apply strict CIP) may provide incentive to minimize the CI, CII and assets identified.<br><br>Effective collaboration between public sector (Government & mandated Agencies) and the private sector is fundamental in protecting CII assets and services. |

**Table 3: Comparison of methodological approaches in identification of CIIs**

# 5 Challenges in identification of CIIs assets and services

Based on the findings of the survey presented in chapter 2, the feedback from stakeholders and the analysis of the different approaches, it was possible to underline the following challenges:

- detailed list of critical services is not always present and it is difficult to develop from scratch.
- defining criticality criteria for the identification of critical assets is a challenging process
- effective collaboration between public sector (Government & mandated Agencies) and the private sector is fundamental in identifying and protecting CII assets and services.

For these reasons, some improvements for addressing the above issues are presented here. In the improvements we will focus on **critical services dependent approaches**. As presented, the network architecture approach does not scale to a size of a MS due to its complexity and also doesn't take into consideration access network components which architecture-wise may seem insignificant, but may be critical to a critical service's connectivity.

## 5.1 Identification of critical sector and services

During the stocktaking process, it became clear that a significant number of Member States present a low level of maturity and lack a structured approach. Therefore, it was considered useful to have a reference list of critical sectors / services that they could consult in order to define their own list depending on their specific geographical characteristics, culture and history.

In that direction, having reviewed several national definitions, an indicative list of critical sectors and associated sub-sectors and services, is provided in the following table. While compiling the list, an effort was made to consider the **complete value chain of each critical sector**. It is suggested that this list be used as a reference list by MS (as a starting point), in order to evaluate the sectors and the services to be classified as critical.

| Critical Sector | Critical subsector | Critical services |
|---|---|---|
| **1. Energy** | Electricity | • Generation (all forms)<br>• Transmission / Distribution<br>• Electricity Market |
| | Petroleum | • Extraction<br>• Refinement<br>• Transport<br>• Storage |
| | Natural Gas | • Extraction<br>• Transport / Distribution<br>• Storage |
| **2. Information, Communication Technologies (ICT)** | Information Technologies | • Web services<br>• Datacentre/ cloud services<br>• Software as a Service |
| | Communications | • Voice/ Data communication<br>• Internet connectivity |
| **3. Water** | Drinking water | • Water storage<br>• Water distribution<br>• Water quality assurance |
| | Wastewater | Wastewater collection & treatment |

| | | |
|---|---|---|
| **4. Food** | | • Agriculture / Food production<br>• Food supply<br>• Food distribution<br>• Food quality/safety |
| **5. Health** | | • Emergency healthcare<br>• Hospital care (inpatient & outpatient)<br>• Supply of pharmaceuticals, vaccines, blood, medical supplies<br>• Infection/epidemic control |
| **6. Financial services** | | • Banking<br>• Payment transactions<br>• Stock Exchange |
| **7. Public Order and Safety** | | • Maintenance of public order and safety<br>• Judiciary and penal systems |
| **8. Transport** | Aviation | • Air navigation services<br>• Airports operation |
| | Road transport | • Bus / Tram services<br>• Maintenance of the road network |
| | Train transport | • Management of public railway<br>• Railway transport services |
| | Maritime transport | • Monitoring and management of shipping traffic<br>• Ice-breaking operations |
| | Postal/ Shipping | |
| **9. Industry** | Critical industries | • Employment[18] |
| | Chemical / Nuclear Industry | • Storage and disposal of hazardous materials<br>• Safety of high risk industrial units |
| **10. Civil Administration** | | • Government functions |
| **11. Space** | | • Protection of space-based systems |
| **12. Civil protection** | | • Emergency and rescue services |
| **13. Environment** | | • Air pollution monitoring and early warning |

[18] Employment / GDP /supply of goods sustaining activity

| | | |
|---|---|---|
| | | • Meteorological monitoring and early warning<br>• Ground Water (lake/river) monitoring and early warning<br>• Marine pollution monitoring and control |
| **14. Defense** | | National defense |

**Table 4: List of critical sectors and related critical services**

## 5.2 Criticality criteria and dependencies assessment

Independently of which of the two approaches a Member State adopts and which organisation shall take the leading role, a structured process should be followed in order to identify the critical services. This was underlined by stakeholders as particularly difficult and for this reason an initial outline is here presented.

Usually, this process consists of the following activities:

a) **Application of sector specific criteria**, in order to come up with a short-list of potential critical services

b) **Assessment of criticality level of short-listed services.** Criticality is the: (I) level of contribution of an infrastructure to society in maintaining a minimum level of national and international law and order, public safety, economy, public health and environment, or (ii) impact level to citizens or to the government from the loss or disruption of the infrastructure.[19]

Impact is usually evaluated with respect to three primary characteristics:

i. **scope or spatial distribution** – the geographic area that could be affected by the loss or unavailability of a critical infrastructure;

ii. **severity or intensity or magnitude** – the consequences of the disruption or destruction of a particular critical infrastructure;

iii. **Effects of time or temporal distribution** – the point that the loss of an element could have a serious impact (immediate, one to two days, one week).

Several Countries have issued criticality criteria in order to identify the critical assets. A table of indicative impact criteria is presented below, which could be used as a reference list by Member States that have not defined yet their own criticality criteria.

| Criterion title | Explanation |
|---|---|
| **Population affected** | The percentage of the population of the MS affected from the disruption of the service |
| **Concentration** | The density of the population on the geographic area affecting the service |
| **Economic Impact** | The cost of service disruption in terms of GDP percentage. |
| **Public confidence** | The effect that the proper operation of this service has on the public confidence towards the government |

[19] E. Luiijf, H. Burger and M. Klaver, Critical infrastructure protection in the Netherlands: A quick-scan, Proceedings of the EICAR Conference, 2003.

| | |
|---|---|
| **International Relations** | The effect that that a service interruption will have on the relationships between the MS and 3rd countries. |
| **Public order** | The effect that a service interruption may cause to the public order |
| **Public operations hindered** | The daily operations of the public, such as going to work via public transportation, are stopped or thwarted |
| **3rd party MS services are affected** | Inter-dependencies with critical services of other MS should be accounted for. |

**Table 5: List of critical sectors and related critical services**

c) **Assessment of dependencies**. An important dimension to be taken into consideration during the identification of critical services is the dependencies among the different sectors and subsectors as well as cross-border dependencies. Dependencies may cause a service and /or infrastructure to be identified as critical, not because of the first order of disruptions, but due to the cascading effects that their disruption may have on other services / infrastructures. Furthermore, disruption of a service in one MS may cause serious effects in other countries.

While assessing the criticality of services, infrastructures and supporting network assets, it is crucial to examine the system in its entirety rather than per constituent, given that there are at least four types of dependencies that should be taken into consideration:

- **Interdependencies within a critical sector (intra-sector):** In the telecommunications sector strong intra-sector dependencies exist. A significant example is the fact that a single Network Operator owns the fixed network 'last mile' and offers wholesale services to the other Network operators (the so-called Local-loop-unbundling (LLU)). Therefore the business processes of all NOs depend on the process of the NO which owns the 'last mile'.
- **Interdependencies between critical sectors (cross-sector):** Interdependencies or dependencies between critical sectors have been documented in previous studies. In terms of criticality analysis, the fact that interdependencies between infrastructures exist should be taken into consideration, as suggested in literature, both at the logical and at the physical level.
- **Interdependencies among communication network assets:** Data networks are built by linking components/nodes. Component interdependency is an inherent property of a data network: each network node depends on other nodes to exchange and forward data packets in order to provide communication services. Apart from the 'physical connectivity interdependency' clearly reflected in the network architecture, many 'logical connectivity interdependency' types exist in the modern data networking landscape.

Moreover dependencies can be found at the **national and international level (cross-border), further complicating the task to assess risk.**

## 5.3 Effective collaboration: tagging of CIIs assets and centralized views

For the identification of Critical Information Infrastructures in communication networks, **the involvement of two categories of stakeholders should be pursued**, **i.e. operators of CIs and Network operators**, given the complementarity of their perspectives, responsibilities and expertise.

**Operators of CIs** set the requirements for connectivity solutions that they need to procure from the network operators. In other words, operators of CIs place the order (which may be characterized by a high degree of complexity) and network operators fulfil the order. The operators of CIs need to identify and classify the access & private network infrastructures supporting critical applications, according to their criticality. They are responsible to determine the core processes, the respective applications and, as a last step, the network assets and services (connectivity solutions) which are used to operate the respective applications.

**Network operators**, on the other hand**,** are responsible to determine the network assets & services, enabling the connectivity solutions needed by the operators of CIs.

**Cybersecurity agencies/ NRAs with mandate on CIIs** may have a leading role in all activities related to the identification and protection of CIIs and as presented in the stock taking aim in the future to have:

- Information systems which would support **automated-prioritized handling of incidents affecting Critical Information Infrastructure.**
- Maintain a **CI/CIIs assets and services database** which should include **relevant critical services details, location, dependencies, role/person responsible and point of contacts**.

To foster the security of CII and develop effective cooperation, MS should work together with CIIs asset owners in **developing a common approach to the 'Tagging' of CII assets** and have a **holistic overview of their status**:

- Operators of CII should identify the **detailed network assets and tag them using a common taxonomy** that can be used to federate the different views.
- Mandated agencies could develop the **ability to have a centralized view of the CII network assets and related information in order to react timely in case of incident**.

This could allow **automated-prioritized handling of incidents** affecting CIIs and lead to a prompt and coordinated response in case of incident or outage.

# 6 Recommendations

**Recommendation 1: Member States should clearly identify Critical Information Infrastructures if not already covered in their Critical Infrastructure activities**. As underlined during the stock taking, not all Member States have clearly defined the asset perimeter of Critical Information Infrastructures. For this reason, if not already covered by the Critical Infrastructure definition, Member States should clearly define which specific network assets are covered and should be secure and resilient.

**Recommendation 2: Member States who are starting to work on the identification of CII assets should work together with the stakeholders involved in the operations of Critical Information Infrastructures.** Effective collaboration between public sector (Government & mandated Agencies) and the private sector is fundamental in protecting CII assets and services. For the identification of CIIs in communication networks, the involvement of two categories of stakeholders should be pursued:

- operators of Critical Infrastructures
- Network operators

given the complementarity of their perspectives, responsibilities and expertise.

**Recommendation 3: Member States who are starting to work on the identification of CII should adopt a methodology for identification of critical network assets and services, using one or a mix of the proposed solutions in this study that better fits the need of the MS.** It is worth-noting that the purpose here is to present the Member States with a portfolio of methodological approaches – rather than a single 'fits-all' methodology –that each Member State may choose the approach or a combination of approaches that suits better to its own specific characteristics and needs.

**Recommendation 4: Member States who base their identification of CIIs on critical services should develop a list of these services and assess internal and external interdependencies.** While assessing the criticality of services, infrastructures and supporting network assets, Member States should define criticality criteria in order to identify the critical assets and examine the system in its entirety rather than per constituent. At least four types of dependencies should be taken into consideration:

- Interdependencies within a critical sector (intra-sector)
- Interdependencies between critical sectors (cross-sector).
- Interdependencies among communication network assets.

Moreover dependencies can be found at the national and international level (cross-border), further complicating the task to have a complete overview.

**Recommendation 5: Member States should foster baseline security guidelines for communication networks used for critical services.** To ensure the resilience of critical networks, the Critical Infrastructure operator or asset owner should adopt security guidelines to be used also at procurement stage. For this reason a checklist with baseline security guidelines for communication networks used for critical services should be made available to align practices across the EU.

**Recommendation 6: Member States should foster the adoption of automated procedures for CIIs tagging in order to be prepared to face future challenges.** To foster the security of critical networks, Member States should work together with CIIs asset owners in developing a common approach to the 'Tagging' of CII assets. This could allow automated-prioritized handling of incidents affecting Critical Information infrastructures.

## References

Bilbao-Osorio, B., Dutta, S., & Lanvin, B. (2014). The Global Information Technology Report 2014. World Economic Forum.

Bush, R., & Austein, R. (2013). The Resource Public Key Infrastructure (RPKI) to Router Protocol. RFC 6810.

Bush, R., Austein, R., Patel, K, Gredler, H., Waehlisch, M. (2014). Resource Public Key Infrastructure (RPKI) Router Implementation Report. RFC 7128.

Bush, R., Austein, R. (2011). The RPKI/Router Protocol. Internet-Draft.

Butler, K., Farley, T.R., McDaniel, P., Rexford, J. (2010). A Survey of BGP Security Issues and Solutions, BGP Peer Session Security Solutions . Proceedings of the IEEE, vol. 98, issue 1, pp 100-122.

Caesar, M. & Rexford, J. (2005). BGP routing policies in ISP networks. IEEE Network, vol. 16, issue 6, p.p. 5-11.

Chatzis,N., Smaragdakis, G., Feldmann, A. On the importance of Internet eXchange Points for today's Internet ecosystem.

Cisco Security Intelligence Operations. Protecting Border Gateway Protocol for the Enterprise.

Clemente, D. (2013) Cyber Security and Global Interdependence: What Is Critical?, Chatham House

Fekete, A. (2011). Common Criteria for the Assessment of Critical Infrastructures. International Journal of Disaster Risk Science, vol. 2, Issue 1, pp 15-24.

Fraser, B. (1997). Site Security Handbook. RFC 2196.

Gill, P., Schapira, M., & Goldberg, S. (2011). Let the market drive deployment: a strategy for transitioning to BGP security. ACM SIGCOMM Computer Communication Review, vol. 41, issue 4, pp 14-25.

Hammerli, B., & Renda, A. (2010). Protecting Critical Infrastructure in the EU, CEPS Task Force report, Centre for European Policy Studies, Brussels.

Internet Society. (2013). Resilience of the Commons: Routing Security.

Internet Society. (2012). Report on Routing Resiliency Measurements Workshop. Atlanta, GA, USA.

ISO 27001 (2013). Information technology - Security techniques - Information security management systems – Requirements. Avalable at http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.

ISO 27002 (2013). Information technology - Security techniques - Code of practice for information security controls. Available at http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.

ISO 22301 (2012). Societal security - Business continuity management systems - Requirements.
ISO 20000-1. (2011). Information technology - Service management Part 1: Service management system requirements.

Lepinski, M., & Kent, S. (2012). An Infrastructure to Support Secure Internet Routing. RFC 6480.

Luiijf, H., & Klaver, M. (2005). International Interdependency of C(I)IP in Europe. Proceedings of CIP Europe.

McPherson, D., Amante, S., & Osterweil, E. (2012). IRR & Routing Policy Considerations. Internet-Draft.

Multinational Experiment 7, Outcome 3 – Cyber Domain, Threats and Vulnerability Methodology

Murphy, S. (2006). BGP Security Vulnerabilities Analysis. RFP 4272.

Postel, J. (1983). Character Generator Protocol. RFC 864.

Rinaldi, S., Peerenboom, J., & Kelly, T. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems, vol. 21, issue 6, pp 11-25.

Savola, P. (2008). Experiences from Using Unicast RPF. Internet-Draft.

Stefanescu, A., Overeinder, B., Pierre, G. (2011). Effects of RPKI Deployment on BGP Security.

Theoharidou, M., Kotzanikolaou, P., Gritzalis, D. (2009). Risk-based criticality analysis. IFIP Advances in Information and Communication Technology, vol. 311, pp 35-49.

Tierney, K. & Bruneau, M. (2007). Conceptualizing and Measuring Resilience: A Key to Disaster Loss Reduction. TR News 250, pp 14-17.
Touch, J., Mankin, A., & Bonica, R. (2010). The TCP Authentication Option. RFC 5925.

Villamizar, C., Chandra, R., & Govindan, R. (1998). BGP Route Flap Damping: Prevent sustained routing oscillations, without sacrificing route convergence time. RFC 2439.

# Annex I – Legislation in EU and MS

### European Union

Green Paper on a European Programme for Critical Infrastructure Protection COM (2005) 576.

Directive 2008/114/EC of 8 December 2008 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection.

Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services

Communication COM(2011) 163 final from the Commission to the European Parliament, the council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security' European Parliament resolution of 12 June 2012 on Critical Information Infrastructure Protection – Achievements and Next steps: towards Global Cyber-security

Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications"

European Parliament resolution of 12 June 2012 on Critical Information Infrastructure Protection – Achievements and Next steps: towards Global Cyber-security

Communication COM (2009) 149 final on Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience

### Austria

Telecommunications Act 2003 https://www.rtr.at/en/tk/TKG2003

### Finland

Act on the Protection of Privacy in Electronic Communications (516/2004)
http://www.finlex.fi/en/laki/kaannokset/2004/en20040516.pdf

Regulation (FICORA 41 D/2009 M)
http://www.ficora.fi/attachments/englantiav/5k3A9Fyzw/FICORA41D2009M.pdf

Communications Market Act
http://www.finlex.fi/en/laki/kaannokset/2003/en20030393.pdf

Regulation (FICORA 9 D/2003 M)
http://www.ficora.fi/attachments/englantiav/5mCqE9KKW/FICORA09D2009M.pdf

Regulation (FICORA 57 A/2013 M, specifically chapter 2)
http://www.ficora.fi/attachments/englantiav/64u7tHKEx/Viestintavirasto57A2012MEN.pdf

Act on the Protection of Privacy in Electronic Communications
http://www.finlex.fi/en/laki/kaannokset/2004/en20040516.pdf

**France**
Instruction generale interministerielle relative a la securite des activites d'importance vitale - n°6600/sgdsn/pse/psn du 7 janvier 2014

**Germany**
German Federal Data Protection Act in the version promulgated on 14 January 2003 (Federal Law Gazette I p. 66), as most recently amended by Article 1 of the Act of 14 August 2009
http://www.gesetze-im-Internet.de/englisch_bdsg/englisch_bdsg.html

Referentenentwurf des Bundesministeriums des Innern: Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme, Stand 18.08.2014,
http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_IT-Sicherheitsgesetz.pdf?__blob=publicationFile

**Hungary**
Act on identification, assignment and protection of Critical Infrastructure and buildings - Act. CLXVI. of 2012. and its annex 1., 2. and 3. (2012. évi CLXVI. törvény mellékleteire (1,2,3)
http://www.complex.hu/kzldat/t1200166.htm/t1200166.htm

**Greece**
Law 4070/2012

**Italy**

"Codice delle comunicazioni elettroniche"pubblicato nella Gazzetta Ufficiale n. 214 del 15 settembre 2003
http://www.parlamento.it/parlam/leggi/deleghe/03259dl.htm

**Latvia**
Regulations Regarding the Information to be Included in the Action Plan of a Merchant of Electronic Communications, the Control of the Implementation of Such Plan and the Procedures, by which End Users shall be Temporarily Disconnected from the Electronic Communications Network

**Netherlands**
Dutch Telecommunications Act, Translation of 'Telecommunicatiewet - Juni 2012
http://www.government.nl/documents-and-publications/notes/2012/06/07/dutch-telecommunications-act.html

**Poland**
Polish Telecommunication law, 2004
http://isap.sejm.gov.pl/DetailsServlet?id=WDU20041711800

**Romania**
LAW No. 154/2012 regarding the regime of the electronic communications networks infrastructure, Government emergency ordinance No. 111/2011 on electronic communications

**United Kingdom**
UK "Regulation of investigatory powers Act" , 2000
http://www.legislation.gov.uk/ukpga/2000/23/contents

## Annex – II List of acronyms

| | |
|---|---|
| ADSL | Asymmetric Digital Subscriber Line |
| AES | Advanced Encryption Standard |
| AS | Autonomous System |
| ATM | Automated Teller Machine |
| BCP | Business Continuity Plan |
| BGP | Border Gateway Protocol |
| BRAS | Broadband Remote Access Server |
| BSS | Business Support Systems |
| CDMA | Code Division Multiple Access |
| CDN | Content Delivery Network |
| CERT | Computer Emergency Response Team |
| CI | Critical Infrastructure |
| CII | Critical Information Infrastructure |
| CIP | Critical Infrastructure Protection |
| CIIP | Critical Information Infrastructure Protection |
| CPE | Customer-Premises Equipment |
| CSMA | Carrier Sense Multiple Access |
| DiffServ | Differentiated Services |
| DoS | Denial-Of-Service |
| DDoS | Distributed Denial-Of-Service |
| DNS | Domain Name System |
| DNSSEC | DNS Security Extensions |
| DSL | Digital Subscriber Line |
| DSLAM | Digital Subscriber Line Access Multiplexer |
| FTTC | Fibre to the Cabinet |
| GDP | Gross Domestic Product |
| GIS | Geographic Information Systems |
| GPON | Gigabit Passive Optical Network |
| ICS | Industrial Control Systems |
| IP | Internet Protocol |
| ISMS | Information Security Management System |
| ISP | Internet Service Provider |
| IXP | Internet Exchange Point |

| | |
|---|---|
| LAN | Local Area Network |
| LNI | Logical Network Inventory |
| LTE | Long Term Evolution |
| M2M | Machine-to-Machine |
| ME | Metro Ethernet |
| MNS | Managed Network Services |
| MPLS | Multiprotocol Label Switching |
| MPPE | Microsoft Point to Point Encryption |
| MSS | Managed Security Services |
| NO | Network Operator |
| NOC | Network Operations Center |
| OSI | Open System Interconnection |
| OSS | Operation Support Systems |
| OTN | Optical Transport Network |
| PBX | Public Branch Exchange |
| PDV | Packet Delay Variation |
| PKI | Public Key Infrastructure |
| PNI | Physical Network Inventory |
| PPP | Point-to-Point Protocol |
| PSTN | Public Switched Telephone Network |
| PoPs | Points of Presence |
| QoS | Quality of Service |
| SCADA | Supervisory Control and Data Acquisition |
| SIEM | Security Information and Event Management |
| SLA | Service Level Agreement |
| SLAM | Simultaneous Localization and mapping |
| SPOF | Single Point of Failure |
| VAS | Value-Added Service |
| VDSL | Very-high-bit-rate Digital Subscriber Line |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| WiMAX | Worldwide Interoperability for Microwave Access |

## Related ENISA papers

[1] Understanding the importance of the Internet Infrastructure in Europe: Guidelines for enhancing the Resilience of eCommunication Networks (2013)

[2] National Roaming for Resilience, National roaming for mitigating mobile network outages (2013)

[3] Report on Resilient Internet Interconnections (2012)

[4] Secure routing: State-of-the-art deployment and impact on network resilience (2010)

[5] Business and IT Continuity: Overview and Implementation Principles (2008)

TP-06-14-120-EN-N

**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

ISBN number: 978-92-9204-106-9
doi: 10.2824/38100

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