Evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

Final report

2 April 2019

This report has been prepared by EY and RAND Europe for the European Commission's Directorate-General for Migration and Home Affairs (DG HOME).

European Commission

Directorate-General for Migration and Home Affairs
Directorate D: Security

Evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

Final report

Directorate-General for Migration and Home Affairs

Europe Direct is a service to help you find answers to your questions about the European Union.

Freephone number (*)**:**

00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Luxembourg: Publications Office of the European Union, 2020

PDF ISBN 978-92-76-19510-8 doi: 10.2837/864404 DR-03-20-374-EN-N

Table of contents

List of Abbreviations

AEO	Authorised Economic Operator
AI	Artificial intelligence
CEI	Critical energy infrastructure
CER	Community of European Railway and Infrastructure Companies
CI	Critical infrastructure
CII	Critical information infrastructure
CIP	Critical infrastructure protection
CIP PoC	Critical Infrastructure Protection Point-of-Contact
CIPS	EU Programme on Prevention, Preparedness and Consequence Management of Terrorism and other Security-Related Risks
CIWIN	Critical Infrastructure Warning Information Network
CSE	Central Stockholding Entity
CSIRT	Computer Security Incident Response Team
DG	Directorate-General
DG ENER	Directorate-General for Energy
DG HOME	Directorate-General for Migration and Home Affairs
DG MOVE	Directorate-General for Mobility and Transport
EBA	European Banking Authority
EC	European Commission
ECB	European Central Bank
ECI	European Critical Infrastructure
EDA	European Defence Agency
EEA	European Economic Area
EEAS	European External Action Service
EEGI	European Electricity Grid Initiative
EE-ISAC	European Energy Information Sharing and Analysis Centre
EGNOS	European Geostationary Navigation Overlay System
ENISA	European Union Agency for Network and Information Security
ENTSO-E	European Network of Transmission System Operators for Electricity
ENTSOG	European Network of Transmission System Operators for Gas
EPCIP	European Programme for Critical Infrastructure Protection
EQ	Evaluation Question
ERCC	Emergency Response Coordination Centre
ERNCIP	European Reference Network for Critical Infrastructure Protection
EU	European Union
EUROPOL	European Union Agency for Law Enforcement Co-operation
EWRS	Early Warning and Response System
GCG	Gas Coordination Group
GNSS	European Global Navigation Satellite System
GovSatcom	Governmental Satellite Communications
GSA	European GNSS Agency
JRC	Joint Research Centre
HSC	Health Security Committee
ICT	Information and communications technology
IEC	International Electrochemical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization

ISPS	International Ship and Port facility Security
IoT	Internet of Things
MS	Member States
NATO	North Atlantic Treaty Organization
NCI	National critical infrastructure
NGI	Next Generation Internet
NIS	Network and information system
OECD	Organisation for Economic Co-operation and Development
OSCE	Organisation for Security and Co-operation in Europe
OSP	Operator Security Plan
PC	Public Consultation
PPP	Public Private Partnership
PSD	Payment Services Directive
SAB	Security Accreditation Board
SCADA	System control and data acquisition
SIPS	Systematically Important Payment Systems
SLO	Security Liaison Officer
SOLAS	Safety of Life at Sea
SST	Space Surveillance and Tracking
TFEU	Treaty on the Functioning of the European Union
TNCEIP	Thematic Network on Critical Infrastructure Protection
TSO	Transmission system operator
UN	United Nations
UNISDR	UN Office for Disaster Risk Reduction

EU Member States

AT	Austria
BE	Belgium
BG	Bulgaria
CY	Cyprus
CZ	Czechia
DE	Germany
DK	Denmark
EE	Estonia
EL	Greece
ES	Spain
FI	Finland
FR	France
HR	Croatia
HU	Hungary
IE	Ireland
IT	Italy
LT	Lithuania
LU	Luxembourg
LV	Latvia
MT	Malta

NL	The Netherlands
PL	Poland
PT	Portugal
RO	Romania
SE	Sweden
SI	Slovenia
SK	Slovakia
UK	United Kingdom

Glossary

Term	Definition
Asset	A resource, whether physical or virtual, that has value to an organisation and its business operations.[1]
Crisis management	A continuous process following a crisis that typically involves four stages: response, recovery, mitigation/prevention and preparedness.[2]
Interdependency	A bidirectional relationship between two or more infrastructures, where the state of one affects the other, and vice versa.[3]
Mitigation	The lessening or limitation of the negative consequences of hazards and related disasters.[4]
Preparedness	The knowledge and capacities developed by the responsible body (e.g. governments, professional response and recovery organisations, communities, individuals) to effectively anticipate, respond to, and recover from the impacts of likely, imminent or current hazard events or conditions.[5]
Protection	Actions or measures taken to deter, mitigate and neutralise a threat, risk or vulnerability in order to ensure the functionality, continuity and integrity of critical infrastructures.[6]
Recovery	The restoration, and improvement, where appropriate, of facilities, livelihoods, and living conditions of disaster-affected communities, including efforts to reduce current and future risk factors.[7]
Resilience	The ability of a system, community or society exposed to hazards to resist, absorb, accommodate and recover from the effects of a hazard in a timely and efficient manner. This includes the preservation and restoration of its essential basic functions and structures.[8]
Response	The provision of emergency services and assistance during or immediately after a disaster in order to save lives, reduce health impacts, ensure public safety and meet the basic subsistence needs of the people affected.[9]
Risk analysis	A methodology to consider the extent of relevant risks, in order to evaluate the vulnerability and the potential impact of disruption or destruction of a critical infrastructure.[10] The level of risk is determined by the interaction of the level of threat and the vulnerabilities of a particular object or system.
Risk management	Risk management, which is distinct from risk assessment, involves weighing policy alternatives in consultation with relevant stakeholders, considering risk assessment and other legitimate factors, and selecting appropriate prevention and control options.[11]
Safety	Protection against danger or incidents.[12]
Security	Protection from a danger or threat.[13]
Service	An action providing a necessary functionality or the fulfilment of a demand.[14]
System	A combination of aspects (e.g. facilities, procedures, equipment) that serve a specific purpose.[15]
Threat assessment	Assessment of the likelihood of occurrence of a hazard or event with a harmful effect. In contrast to risk, a threat is not relating to the impact it may cause.[16]

[1] ENISA, "Asset" (ISO/IEC Guide 73), Risk management glossary. Moteff, J., & Parfomak, P. (2004). Critical Infrastructure and Key Assets: Definition and Identification - CRS Report for Congress. Congressional Research Service.
[2] Fraunhofer Institute, CIPedia Glossary.
[3] Montanari, L., & Querzoni, L. (2014). Critical Infrastructure Protection: Threats, Attacks and Countermeasures. TENACE.
[4] UNISDR. (2009). UNISDR Terminology on Disaster Risk Reduction.
[5] UNISDR. (2009). UNISDR Terminology on Disaster Risk Reduction.
[6] ECI Directive, Article 2(e).
[7] UNISDR. (2009). UNISDR Terminology on Disaster Risk Reduction.
[8] UNISDR. (2009). UNISDR Terminology on Disaster Risk Reduction.
[9] UNISDR. (2009). UNISDR Terminology on Disaster Risk Reduction.
[10] ECI Directive, Article 2(c).
[11] Lazari, A. (2014). European Critical Infrastructure Protection. Springer.
[12] Albrechtsen, E. (2002). A generic comparison of industrial safety and information security. Norwegian University of Science and Technology, Trondheim.
[13] Albrechtsen, E. (2002). A generic comparison of industrial safety and information security. Norwegian University of Science and Technology, Trondheim.
[14] Business Dictionary, 'service'. Business Dictionary.
[15] Theocharidou, M., Melkunaite, L., Eriksson, K., Winberg, D., Honfi, D., Lange, D., & Guay, F. (2016). First draft of a lexicon of definitions related to Critical infrastructure resilience, Deliverable D1.2, Improver.
[16] Derived from EC Chemical, biological, radiological and nuclear (CBRN) Glossary.

1 INTRODUCTION

1.1 Objectives and scope of the study

1.1.1 Objectives

This study aims at **evaluating the implementation of Council Directive 2008/114** on the identification and designation of European critical infrastructures (ECI) and the assessment of the need to improve their protection[17] (hereafter referred to as simply "the Directive", "the ECI Directive" or "Directive 2008/114"). The findings of the study will assist the European Commission (EC) in preparing a Staff Working Document presenting the results of the Evaluation and recommendations as to possible paths forward.

In order to achieve this overall objective, the study consisted of four main **tasks**:

- The *analysis of the scope and content* of the Directive, providing a detailed description of the Directive's objectives and intervention logic, its provisions, and the scope of application;
- The *analysis of the organisation of work aimed at implementing the Directive* describing the division of labour at EU and Member State (MS) level and accounting for the existing differences among national organisational systems;
- The *analysis of the implementation of the Directive's provisions,* focusing on how the provisions of the Directive have been implemented at the national level, and assessing existing barriers and new challenges as well as best practice as a mean to understand how to improve the implementation and the effects of the Directive;
- The *overall evaluation of the Directive,* which built on the evidence and results of previous tasks, in assessing the relevance, coherence, effectiveness, efficiency, EU added value and sustainability of the Directive.

The Evaluation drew on, among other sources, the 2012 review of the European Programme for Critical Infrastructure Protection,[18] the study into the potential impacts of options amending the Directive,[19] and the 2017 Comprehensive Assessment of EU Security Policy.[20]

1.1.2 Scope

The study analysed:

- The **security threats** faced by critical infrastructures (CI) in Europe;
- The **implementation and application of the Directive's provisions at the national level** by taking into account national measures (e.g. laws, regulations, implementing strategies, operational guidelines) that addressed the protection of CI;
- The **organisation of the work** in the implementation of the Directive at EU and MS level and the main stakeholders concerned;
- All **evaluation criteria**, related evaluation questions and sub-questions listed in the Technical Specifications[21] attached to the Request for services of the EC;
- The **relevant EU legislative and policy context** that deal either directly or indirectly with the protection of CI to frame the analysis of the coherence of the Directive and provide input for the design of future recommendations.

[17] Council of the European Union. (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 of the European Union. L 345/75. 23 December.
[18] European Commission. (2017). Commission Staff Working Document on the review of the European Programme for Critical infrastructure Protection (EPCIP). SWD (2012)190, Brussels.
[19] Ramboll. (2012). Study into the potential impacts of options amending Council Directive 2008/114/EC. Final Report.
[20] European Commission. (2017). Comprehensive Assessment of EU Security Policy Accompanying the document Communication from the Commission to the European Parliament, the European Council and the Council - Ninth progress report towards an effective and genuine Security Union. SWD(2017) 278 final, Brussels.
[21] Technical Specifications include a detailed description of the objective and scope of the study requested by the EC, the list of evaluation questions to be answered, and a set of requirements to be met in relation to the methodology and the timeline.

The following categories of **stakeholders** have been consulted:

- EC Directorates-General (DGs) and EU Agencies;
- MS competent authorities responsible for the implementation of the Directive;
- National Points of Contact on critical infrastructure protection (CIP PoC);
- CI owners/operators;
- Academia and think tanks; and,
- General public.

The study **covered the implementation of the Directive in all 28 EU MS from its entry into force** (January 2009) **up until the launch of the Evaluation** (late August 2018).

1.2 Content of the report

The report is structured in the following chapters:

- **Chapter 1** presents a summary of the objectives and scope of the Evaluation;
- **Chapter 2** presents the context and background of Directive 2008/114, including key concepts, such as its objectives, scope, main provisions and concerned stakeholders. It also includes the intervention logic used as a basis for the Evaluation;
- **Chapter 3** presents the evaluation questions, grouped according to five evaluation criteria, which have been answered to assess the Directive;
- **Chapter 4** presents the research methodology and the data limitations encountered, this in order for the reader to have a fair understanding of how data was collected and what limitations existed in carrying out the Evaluation;
- **Chapter 5** presents an overview of the implementation of the Directive at the national level;
- **Chapter 6** provides detailed answers to the evaluation questions;
- **Chapter 7** provides a set of conclusions as to the relevance, coherence, effectiveness, efficiency, EU added value and sustainability of the Directive;
- **Chapter 8** presents the recommendations concerning the current Directive;
- **Annex I** includes: a methodological note containing a catalogue of data collected and details on the consultation tools; the list of stakeholders consulted; the synopsis report of consultation activities; the bibliography and evidence supporting the analysis; and,
- **Annex II** contains the implementation tables that summarise information on the national implementation practices.

2 Background and context of Directive 2008/114

The Directive, adopted in December 2008, establishes a common procedure for identifying and designating ECI in the energy and transport sectors and a common approach for assessing the need to improve their protection.

2.1 Directive 2008/114 and its objectives

The origin of the Directive can be traced back to the European Council meeting of 17-18 June 2004[22] when, in the wake of terrorist attacks in Madrid, the European Council asked the EC to prepare an overall strategy for the protection of ECI.

In response to this call, in October 2004 the Commission issued a **Communication on Critical Infrastructure Protection in the fight against terrorism**,[23] in which a broad definition of CI[24]

[22] European Council. (2004). Presidency Conclusions, 17-18 June 2004. 10679/2/04 REV 2, Brussels.
[23] European Commission. (2004). Communication on Critical Infrastructure Protection in the fight against terrorism. COM(2004) 702 final, Brussels.
[24] "Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of

was put forward, along with a long list of sensitive sectors and a number of suggestions for strengthening the protection of critical infrastructure in Europe and laying the foundation for the introduction of the European Programme for Critical Infrastructure Protection (EPCIP). This prompted the Commission to organise two seminars in 2005, where relevant CIP stakeholders were invited to share ideas and comments.

In November 2005, the Commission followed up on its 2004 Communication with a **Green Paper on a European Programme for Critical Infrastructure Protection,**[25] which outlined policy options for the establishment of both EPCIP and a platform for information sharing and early warning, namely the Critical Infrastructure Warning Information Network (CIWIN).[26] Feedback received on these policy options highlighted the need to reduce vulnerabilities concerning CI and the added value of establishing an EU framework for CIP in accordance with the principles of subsidiarity, proportionality and complementarity. As stated in the Green Paper, a combination of security and economic reasons explain the emergence of CIP on the EU agenda. From a security standpoint, the aim was to ensure that one MS was not made vulnerable because of the existence of lower security standards in another MS. From an economic perspective, meanwhile, the Green Paper argued that it was important to ensure the stability of the common market by introducing an integrated EU-wide approach to the protection of CI with cross-border implications.

In December 2006, the EC issued the **Communication on a European Programme for Critical Infrastructure Protection**,[27] which defined an overall policy approach and framework for CIP activities in the EU. The general objective of EPCIP is to improve CI protection capabilities across all MS through the adoption of an all-hazards approach. The key underlying rationale is that the disruption/destruction of infrastructures that provide key services can harm the security and economy of the EU and the well-being of its citizens.

Directive 114/2008 has been adopted by the EC as a building block of EPCIP. During the negotiations in the lead-up to adoption, MS came to an agreement on a "minimum common denominator" approach. This was a narrower scope than the Commission's original proposal in 2006, which covered a range of sectors.[28] The more modest approach that was agreed was primarily due to MS' reluctance to embrace a broad EU approach in an area of traditional national competence, but also certain legal basis considerations.[29] The **legal basis** for the Directive was Article 308 of the Treaty establishing the European Community. This article, referred to as the "flexibility clause", allowed the Council to act when necessary, upon the proposal of the Commission, to achieve the objectives of the EU even when a precise legal basis is missing. With the adoption of the Lisbon Treaty, this article was amended, becoming Article 352 of the Treaty on the Functioning of the European Union, which introduced the requirement for the European Parliament to provide its consent to the Council's actions.

The distinctive element of the Directive is the **introduction of the concept of ECI**. In general, CI are understood as those physical and information technology facilities, networks, services and assets that, if disrupted or destroyed, would have a serious impact on the health, safety, security, and social and/or economic well-being of citizens. The Directive acknowledges the existence in Europe of a number of CI, which, in the event of disruption, destruction, or failure, would significantly affect two or more MS, i.e. would have significant transboundary effects. In this respect, they can be seen as essentially "European" in nature. When the disruption, destruction or

citizens or the effective functioning of governments in the Member States. Critical infrastructures extend across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services".

[25] European Commission. (2005). Green Paper on a European Programme for Critical Infrastructure Protection. COM(2005) 576 final, Brussels.

[26] In the context of the preparatory phase leading to EPCIP, MS expressed their preference for making the CIWIN a voluntary system for the exchange of 'best practices' rather than a mandatory early warning mechanism. The Commission initial proposal was withdrawn in 2012 and CIWIN was transformed into an eCommunity, managed by the Commission, where the critical infrastructures stakeholders can share documents of interest.

[27] European Commission. (2006). Communication on a European Programme for Critical Infrastructure Protection. COM(2006) 786 final, Brussels.

[28] European Commission (2006). Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection. COM(2006) 787 final, Brussels.

[29] Kick-off meeting, 13 September 2018.

failure of a CI (or part thereof) in a single MS is expected to bring about serious adverse effects on other countries or even the European economy more broadly, a common level of protection for ECI is warranted. Indeed, this implies that protection measures are only as strong as their weakest link (i.e. if one fails, all fail).

In this view, the Directive contributed to the establishment of a common EU framework that strives for the coherent and uniform implementation of measures to enhance the protection of the infrastructure that would come to be designated as ECI. The Commission has a number of different policy instruments in its policy toolbox. In looking to strengthen CIP, the Commission considered a Directive to be the preferable policy tool; while non-binding voluntary measures would ensure flexibility, they would not serve to clarify the rights and obligations of the different stakeholders in an ECI context. The EC adopted a sector-by-sector approach, reflected first in EPCIP and then in the Directive[30] in order to take into account sectoral specificities (and related experience, expertise and requirements concerning CIP) and building on existing CI sector-based measures. The Directive aims at improving the level of protection of ECI against natural disasters, as well as technological and man-made threats, including terrorism. By increasing the level of protection of these infrastructures, the Directive ultimately aims at ensuring the security, health, safety and well-being of people in the EU (**general objective**).

This general objective is pursued through two **specific objectives**: namely the establishment of i) a procedure for the identification and designation of ECI; ii) a common approach to the assessment of the need to improve the protection of such ECI.

In order to meet the aforementioned general and specific objectives, the Directive includes a number of key provisions (**inputs**) to be implemented by different categories of stakeholders. These include:

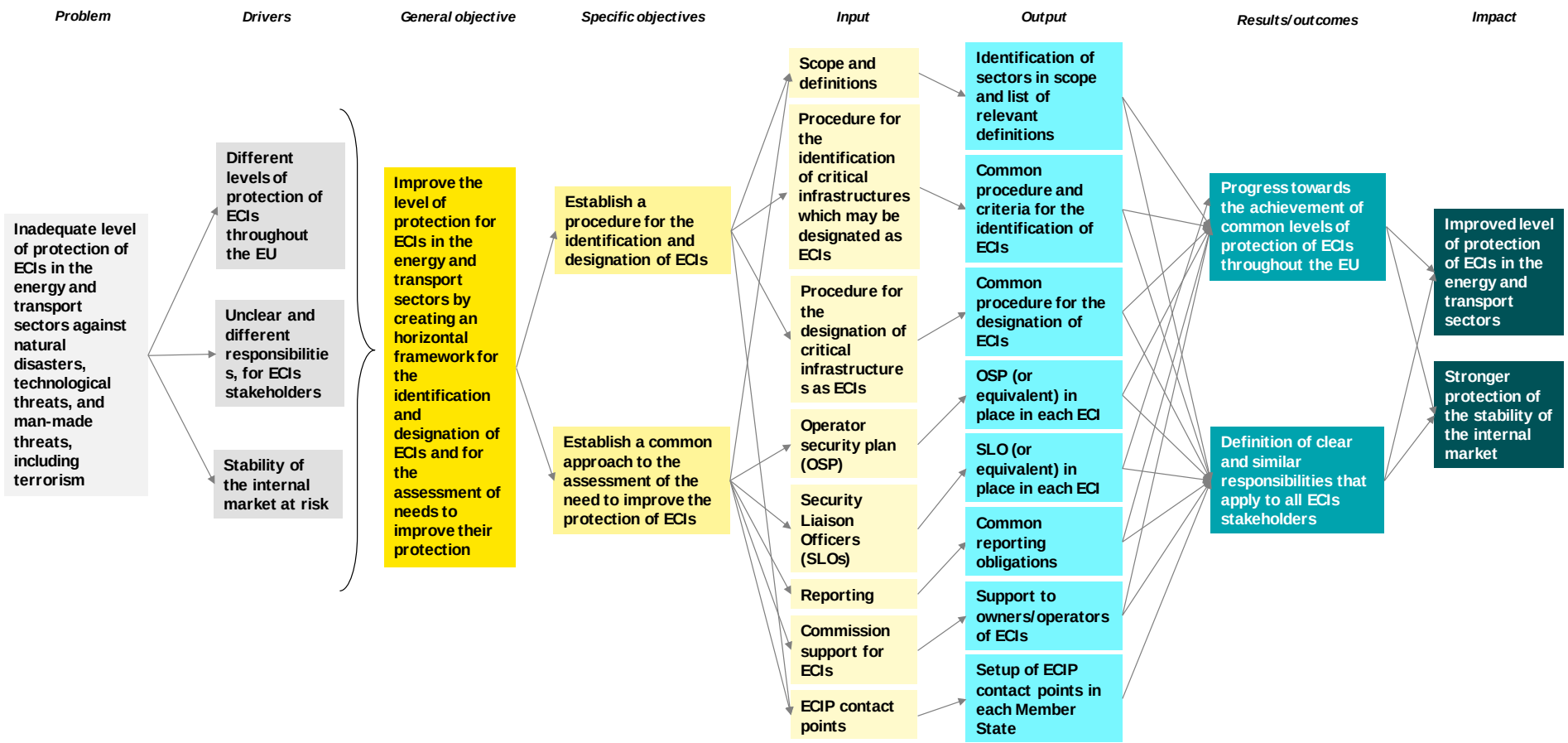
- **Identification of ECI** (Article 3): MS go through a four-step process aimed at identifying potential ECI in the energy and transport sectors, with the help of the Commission if required. The process includes notably the application by MS of a set of sectoral and cross-cutting criteria;
- **Designation of ECI** (Article 4): MS go through a co-operative designation process (e.g. discussions with other MS) involving potential ECI located on their territory;
- **The drafting of the Operator Security Plans (OSP)** (Article 5): MS ensure that an OSP documenting critical assets and security measures is in place for each designated ECI;
- **The identification of Security Liaison Officers (SLO)** (Article 6): MS ensure that a SLO is appointed to serve as the point of contact between the owner/operator of the ECI and the relevant competent authority at the MS level;
- **Reporting** (Article 7): MS conduct threat assessments in relation to ECI within one year following initial designation and then report general data to the Commission on the types of risks, threats and vulnerabilities every two years;
- **Commission support for ECI** (Article 8): The EC supports both MS and owners/operators of designated ECI by sharing best practices and methodologies for the protection of ECI; and,
- **The identification of European Critical Infrastructure Protection contact points** (Article 10): MS appoint European CIP contact points in charge of coordinating European CIP issues within and between MS and with the EC.

Annex I.5.1 describes in detail the key provisions of the Directive, the main categories of stakeholders concerned, and the workflow to identify and designate ECI.

Figure 1 outlines the intervention logic of the Directive, including the expected outputs, results and impacts.

[30] European Commission. (2006). Commission staff working document - Accompanying document to the proposal for a Council Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection - Impact Assessment. SEC(2006) 1654.

Figure 1 - Intervention logic



2.2 The relevant policy context

The protection of CI is a subject of great importance in relation to the security of EU citizens, the functioning of the internal market, and the reliable delivery of essential services to citizens in so far as they depend on some CI. For this reason, CI is the subject of several EU measures, which address the protection of CI in either a direct or indirect manner.

The protection of CI is identified as a priority in various key EU policy documents. For instance, the 2009 **Stockholm Programme**[31] identified the reduction of the vulnerability of CI to attacks as a key policy objective, but also the need to improve the degree of protection of CI. It also called for analysing and possibly reviewing the Directive in view of including additional sectors (with a priority for ICT). The **EU Internal Security Strategy**, set out in 2011, underlined how, besides protection, there was a need for a stronger focus on the resilience of CI.

In 2011, the EC created the **European Reference Network for Critical Infrastructure Protection** (ERNCIP),[32] which is intended to improve critical infrastructure protection in the EU through different projects aimed at developing technical protective security solutions. The network links together different types of CIP stakeholders. In 2012 the EC conducted a **review of EPCIP**[33] (and in particular of the Directive 2008/114). This was done in response to both Article 11 of the Directive (requiring a review to be launched in 2012) and changes underway in both the legal and policy contexts. The Lisbon Treaty, which entered into force one year after the adoption of the Directive (2009), enhanced the means of action in the area of security, giving shared competence to the Union in the area of freedom, security and justice.

Building on the findings of the 2012 review, the Commission in 2013 developed a **new, more hands-on and systemic approach to EPCIP**, focused on the implementation of certain activities. The aim of the new approach was to ensure a high degree of protection for infrastructures and increased resilience against all threats and hazards. Specifically, the new approach offered a stronger focus on **interdependencies** between CI; a step-by-step approach centred around **prevention, preparedness and response**; and the launch of a new **pilot phase focusing on four European-wide infrastructures**, namely:

- The European aviation control system, EUROCONTROL;[34]
- The satellite-based navigation system, GALILEO;[35]
- The transnational energy network (the European Electricity Grid Initiative (EEGI)[36]); and,
- The transnational gas transmission network (the European Network of Transmission System Operators for Gas (ENTSOG)[37]).

The **2015-2020 Internal Security Strategy**[38] underlined the need to ensure resilience, operational preparedness and political coordination to react, deal with and mitigate crises and

[31] Conclusions of the European Council of 10/11 December 2009 on 'The Stockholm Programme — an open and secure Europe serving and protecting citizens (2010-2014)'. 17024/09, Brussels.
[32] EC website, ERNCIP Project Platform, https://erncip-project.jrc.ec.europa.eu/about-erncip.
[33] European Commission. (2012). Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure (EPCIP). SWD(2012) 190 final, Brussels.
[34] Eurocontrol is based on the EC's close work with the European Organisation for the Safety of Air Navigation and aims at achieving the objectives of the Single European Sky Initiative. It focuses on air traffic management (which is one of the sub-sectors covered by Directive). Eurocontrol objectives include encouraging governmental and industrial coordination with regard to aviation cyber-security strategies, policies, and plans, as well as sharing of information to help identify critical vulnerabilities. This initiative also aims at creating policies and allocating resources to ensure that, for critical aviation systems: security is ensured by design of system architectures; systems are resilient; data transfer methods are secure; integrity and confidentiality of data are ensured; system monitoring, incident detection and reporting methods are implemented; forensic analysis of cyber incidents is carried out.
[35] The European Union's Global Satellite Navigation System (GNSS), also referred to as Galileo, provides accurate positioning and timing information. The programme is under civilian control, interoperable with existing satellite navigation systems, and includes transport, logistics, telecommunications and energy.
[36] The EEGI is one of the European Industrial Initiatives (EIIs) under the Strategic Energy Technology Plan. It proposes a nine-year European research, development and demonstration programme to accelerate innovation and develop electricity networks of the future in Europe.
[37] The ENTSOG aims to facilitate and enhance co-operation between national gas transmission system operators across Europe to ensure the development of a pan-European transmission system in line with European Union energy goals.
[38] Council of the European Union (2015), Draft Council Conclusions on the Renewed European Union Internal Security

natural and man-made disasters. The EU's commitment to enhanced efforts for the protection and resilience of CI against both terrorist and cyber threats was also highlighted in the *2016 Global Strategy for the European Union's Foreign and Security Policy*.[39]

More recently, the 2017 **Comprehensive *Assessment* of the EU Security Policy**[40] recognised how the protection of CI is a key objective of the 'Protect' strand of the *2005 EU Counter-Terrorism Strategy*.[41] While the Assessment found the conceptual CIP framework still to be valid, it saw the need for wider consideration of the implications that new security challenges and increased interdependency between infrastructures might have going forward. Furthermore, the Assessment called for a review of the Directive considering the need to repeal/replace it in light of recent developments.

At the EU level, the ECI Directive is part of a complex and highly fragmented policy context, which includes a number of pieces of **sector-specific legislation** that address the security of critical infrastructure in the sectors covered by the Directive (energy and transport) and in other sectors currently outside the scope but that gained importance with the recent entry into force of Directive (EU) 2016/1148 concerning measures for high common levels of security of network and information systems (otherwise known simply as the NIS Directive). The sectors covered by the NIS Directive and not by the ECI Directive include: banking; financial market infrastructures; health; drinking water supply and distribution; and digital infrastructure. The totality of legislation and policy initiatives addressing the security of CI in different sectors makes up and defines the EU's overall CIP framework, and, as such, the study analysed it in view of drafting relevant recommendations for the future development of specifically the ECI Directive (see Annex I.4 for a list of the legislation that was analysed).

At the international level there is no unified policy for CI protection. CI protection is however high on the international agenda, as shown by recent initiatives. For instance, the **UN Security Council** in 2017 approved a Resolution[42] calling upon Member States to put in place comprehensive measures for the protection of CI against terrorist attacks.

The work of the **Organisation for Economic Co-operation and Development (OECD)** is also relevant to CIP. In 2014, it adopted a *Recommendation on the Governance of Critical Risks*, which focused on critical risks in general.[43] On digital infrastructures specifically, the OECD adopted in 2015 the *Recommendation on Digital Security Risk Management for economic and social prosperity,* which aimed at the adoption by all OECD countries of a digital security risk management approach, and of preparedness and continuity plans. Furthermore, the OECD is currently working to revise the 2008 *Recommendation on the Protection of Critical Information Infrastructures* (CII) which was originally developed to foster the introduction of frameworks to protect CIIs from all possible hazards. In addition, the OECD has organised several workshops related to CIP[44] and has developed the OECD Toolkit for Risk Governance, which collects good practices from OECD countries on the governance of risks - including to CI.

The **North Atlantic Treaty Organisation (NATO)** is also involved in security and resilience of CI, especially in the energy sector.[45] Finally, the **International Organisation for Standardisation** (ISO) developed widely used standards that cover risk analysis and risk

Strategy 2015-2020, Brussels.

[39] European Union. (2016). Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign and Security Policy. Publications Office of the European Union, Luxembourg.

[40] European Commission. (2017). Comprehensive Assessment of EU Security Policy Accompanying the document Communication from the Commission to the European Parliament, the European Council and the Council - Ninth progress report towards an effective and genuine Security Union. SWD (2017) 278 final, Brussels.

[41] Council of the European Union. (2005). The European Union Counter-Terrorism Strategy. 14469/4/5 REV 4, Brussels.

[42] Resolution 2341 (2017).

[43] Critical risks are defined as "threats and hazards that pose the most strategically significant risk, as a result of i) their probability or likelihood and of ii) the national significance of their disruptive consequences, including sudden onset events (e.g. earthquakes, industrial accidents, terrorist attacks), gradual onset events (e.g. pandemics), and steady-state risks (notably those related to illicit trade or organised crime)".

[44] A joint OECD/JRC workshop was held in September 2018 on System thinking for critical infrastructure resilience and security; within a series of workshops about Strategic Crisis Management, in collaboration with the Swiss Federal Chancellery, a workshop titled Managing Critical Infrastructure Crises took place on June 2017; In February 2018, there have been the Workshop on Digital Security and Resilience in Critical Infrastructure and Essential Services: Digital Security in Energy, Transport, Finance, Government, and SMEs.

[45] European Parliament. (2007). Note on NATO's role in Critical Infrastructure Protection, presented during the parliamentary hearing on 31 January 2007 before the LIBE committee.

management practices and that are relevant for CI operators (such as ISO/IEC 27000-series). See Annex I.8.4 for additional details on the various relevant international initiatives.

2.3 Baseline

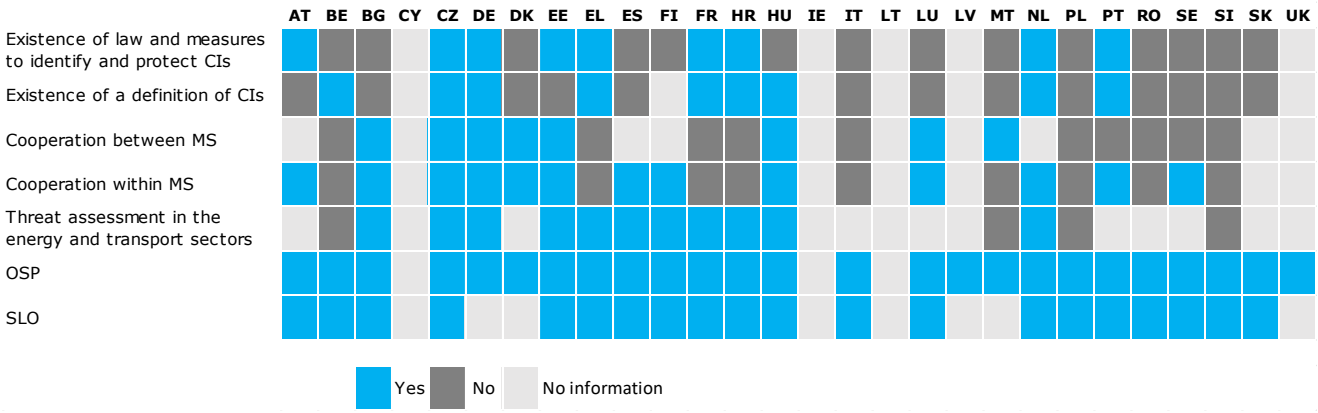
When first proposed in 2006, the problem that the Directive aimed to address was the **inadequate level of protection of CI with a European dimension**, specifically in the energy and transport sector. This was due to:

- **Different levels of protection of CI throughout the EU**, which represented an issue due to the fact that protection measures are only as strong as their weakest link. This was viewed as an especially pressing issue given the fact that the damage or loss of a piece of infrastructure in one MS could have negative effects on several others and on the European economy. This interconnectedness was perceived as increasingly likely in 2006, in view of new technologies and market liberalisation (e.g. in electricity and gas supply), thus implying that infrastructure is typically part of a larger network;
- **Unclear and different responsibilities of CI stakeholders**, as most critical infrastructure is privately owned and operated leading to significant decentralisation. Moreover, sector operators possess particular experience, expertise and requirements concerning the protection of their critical infrastructure; and,
- **Risk of instability of the internal market**, which is linked to the fact that many CI operators with facilities/operations in different MS were subject to different obligations and legal frameworks concerning CIP that had economic implications relating to the cost of doing business in different MS (e.g. redundant security requirements in different jurisdictions).

To the Evaluation team's knowledge, there were no comprehensive analyses on the CIP frameworks adopted by MS before the entry into force of the Directive,[46] and this made it difficult to fully understand the content and type of existing measures, and thus to have a baseline for the Evaluation.

With a view to provide for an overview (albeit partial) of pre-existing measures and to allow for meaningful comparisons with the current situation, the Evaluation team investigated whether the key elements introduced by the ECI Directive were already present before 2008, and estimated the level of completeness of the pre-existing national CIP frameworks. By triangulating information provided by the European CIP points-of-contact at MS level (hereafter referred to as CIP PoCs) (through the online survey and feedback gathered in the case studies) with the information gathered in the implementation tables, it is possible to see (in dark grey) in Figure 2 (below) the elements of the ECI Directive that were missing from national frameworks prior its entry into force.

Figure 2 - National CIP measures before 2008



Source: Authors' elaboration based on field and desk research

In almost half of the MS (13) there was **no definition as to what exactly constitutes a critical infrastructure**. Similarly, in 14 MS (though with some differences as explained below) there were

[46] There are a few non-comprehensive analyses of CIP frameworks pre-2008, such as the International CIIP Handbook (Abele-Wigert, I., & Dunn, M. (2006). International CIIP Handbook, vol. 1), more focused on CIIs, but including some details of the CIP framework for eight EU MS.

no specific laws and measures in place intended to identify and protect CI (which speaks to **the lack of a clear regulatory framework**). Meanwhile, there was no co-operation between MS to exchange information on CIP practices or implement CIP measures in 10 MS.

On the other hand, fewer gaps were reported in terms of the performance of threat assessments in the energy and transport sectors (4 MS reported gaps) and in terms of co-operation within individual MS (9 MS reported this as a gap).

Concerning the development of OSPs, most MS (25) had before the introduction of the Directive equivalent requirements in place. This was due to national or international obligations, or was done as part of corporate risk management and/or resilience planning.[47] Moreover, a large number of MS (20) also had in place measures calling for a position analogous to the SLO required by the Directive. Obviously, such measures were named differently before 2008, but the content of the OSP and the functions of the SLO may be considered equivalent. The variety of the nature of these equivalent arrangements/functions speaks to the fact that most MS had in place either civil emergency and national security-related sectoral requirements (e.g. energy sector) or stringent requirements relating to protection and security measures in line with relevant international, EU, and/or national requirements (e.g. transport sector).[48]

While the existence (or the absence) before 2008 of key elements introduced by the ECI Directive provides a benchmark in order to assess the changes subsequently brought about in the different MS on account of the Directive, it should not be considered as a proxy for the level of maturity of national CIP frameworks given that, as mentioned earlier, information on national-level CIP frameworks prior to 2008 is limited. For instance, several elements introduced by the ECI Directive were missing from the CIP frameworks of the Nordic countries, though this is not to say that their pre-existing arrangements were any less effective than in MS where the specific elements prescribed by the Directive were already in place. Indeed, as shown later in the study (Section 6.2.2), the Nordic countries generally speaking adopted a substantially different approach to ensuring the security of CI than that put forward by the EC, for instance in focusing at an early stage on resilience.[49]

3 EVALUATION QUESTIONS

The overall objective of this Evaluation study is to assess the relevance, coherence, effectiveness, efficiency, EU added value and sustainability of Directive 2008/114 as applied in the EU28 MS. In the context of this Evaluation, and in accordance with the Better Regulation Guidelines, the Evaluation team sought to answer the following questions:

- **Relevance**, or to what extent the Directive addresses current and future needs and challenges;
- **Coherence**, or whether and to what extent the Directive is coherent and complementary with other interventions at MS, EU and international level;
- **Effectiveness**, or whether and to what extent the Directive has achieved its general and specific objectives;
- **Efficiency**, or whether and to what extent the costs of the Directive were proportionate given the delivered benefits;

[47] The pre-2008 existing measures for SLO and OSP or equivalent are enlisted in Annex 2 of JRC. (2008). Non-Binding Guidelines - For Application of the Council Directive on the Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve Their Protection. Publications Office of the European Union, Luxembourg. Interview: one representative from EC DGs and Agencies and one representative from CI owners/operators.

[48] Booz & Company GmbH. (2012). Study to support the preparation of the review of the Council Directive 2008/114/EC on the "identification and designation of European critical infrastructures (ECI) and the assessment of the need to improve their protection".

[49] Pursiainen, C. (2018). Critical infrastructure resilience: A Nordic model in the making? International Journal of Disaster Risk Reduction, 27, 632–641. Even from an early stage, the Nordic countries' approaches have been more holistic than the EC approach, and focused on a more fundamental level of vital societal functions, which in turn are provided by CI, rather than on sector-based infrastructures. This is clearly a more inter-sectoral approach compared to the original EPCIP, and closer to the concept of resilience. Moreover, they all rely on an all-hazards approach, refraining from putting emphasis on the terrorist threat scenario only. They are not only engaged in co-operation within the EU, but have also adopted an institutionalised approach towards cross-border co-operation within the Nordic and Baltic Sea countries. To conclude, they favour the Public Private Partnerships instead of a strong regulation.

- **EU Added value**, or to what extent the effects from the EU action are additional to the value that would have resulted from action at the national level only; and,
- **Sustainability**, or how much the effects already achieved on account of the Directive are likely to be long-lasting, if the Directive were repealed.

Table 1 provides a list of the specific evaluation questions and sub-questions relating to each of the aforementioned criteria.

Table 1 - Evaluation questions

Relevance
1 To what extent is the Directive relevant in view of current and future needs/challenges?
1.1 To what extent are the definitions set out in the Directive still deemed to be suitable and fit for purpose?
1.1.a To what extent is the notion of critical infrastructure/European Critical Infrastructure as defined in the Directive appropriate in light of contextual changes and the needs of stakeholders?
1.1.b To what extent does the definition of critical infrastructure provided in the Directive fit with the sectors that is applied to?
1.2 To what extent do the scope, set of objectives, but also the formal means of implementation set out in the Directive correspond to the current and possible future threats facing critical infrastructure?
1.3 Is the Directive suitable to the needs/interests of the relevant industries and other stakeholders?
1.4 To what extent does the Directive contribute to stated EU priorities?
1.5 Are there provisions contained in the Directive that might be considered obsolete?
1.6 How well-adapted is the Directive to the various technological/scientific, economic, social, political and environmental advances that have occurred since it was passed?
Coherence
2 To what extent the Directive is coherent and complementary to other relevant policy interventions at MS, EU, and international level?
2.1 To what extent the Directive is coherent and complementary to other policy interventions with similar objectives at MS level?
2.2 To what extent the Directive is coherent and complementary to other policy interventions with similar objectives at EU and international levels?
2.3 To what extent are there synergies, inconsistencies, gaps or overlaps between existing EU legislative framework and the respective legislative frameworks that exist at the MS level?
Effectiveness
3 To what extent has the Directive been effective in delivering intended results?
3.1 To what extent has the Directive achieved the stated objectives?
3.2 To what extent can any observable achievements regarding the enhanced security of CI be attributed directly to the Directive, or rather to other developments (i.e. the introduction of other instruments, actions at the Member State level, on the part of operators, etc.), linked to, or independent, form the Directive?
3.3 To what extent, if at all, has the Directive impacted on the protection of CI at the MS level that was not designated as ECI during the reference period?
3.4 Are there any factors that limit the effectiveness of the Directive? Is so, what are these, where do they stem from, and which stakeholders do they involve?
Efficiency
4 To what extent the Directive has achieved intended results in the most efficient manner?
4.1 Have the results that can be attributed to the Directive been achieved at a reasonable cost? Is the regulatory burden on MS, industry and other relevant stakeholders created by the implementation of the Directive (i.e. specific requirements/procedures) commensurate with observable results?
4.2 What factors have influenced the efficiency of the Directive? To what extent?
EU added value
5 To what extent has the Directive achieved EU added value as opposed to what could have been achieved at either the national or the international level?
Sustainability
6 Are the effects already achieved on account of the Directive likely to be long-lasting, if the Directive were repealed?

4 RESEARCH METHODOLOGY

The study commenced on 28 August 2018 and lasted seven months.[50] It was implemented as planned, using the tools and techniques envisaged in the analytical framework developed in the preparatory phase of the study (detailed in Annex I.1), including desk and field research.

4.1 Desk research

Desk research focused on: i) documents at the **EU level** establishing the overarching policy and legislative framework for the protection of CI, as well as relevant legislation in the sectors covered by the Directive (energy and transport) and other sectors currently outside the Directive's scope but mentioned as important in the Directive itself and in the new EPCIP approach, or that fall within the scope of the NIS Directive (e.g. banking and financial infrastructure, health, space, information and communications technology (ICT), drinking water supply and distribution); ii) documents at the **international level**, including international standards and initiatives relating to the protection of CI; and iii) documents at the **national level,** including national legislative measures, strategies, administrative procedures and guidelines that were in one way or another relevant in transposing and implementing the provisions of the Directive. Drawing on the evidence from the 2012 review of the Directive,[51] the Evaluation team conducted an in-depth analysis of national implementation measures with the aim of filling existing gaps in the empirical record and updating the previous overview with any changes that took place after 2012.

Relevant information at the national level is systematised in the **implementation tables** included in Annex II, which have been designed in accordance with the main aspects of the provisions of Directive 2008/114 and of national CIP frameworks. The sources that have been consulted as part of the Evaluation are referenced in relation to each category of information recorded in the tables. The implementation tables have also been subject to a round of validation, that in many cases resulted in the inclusion of additional information[52] provided by the CIP PoCs from a total of 24 Member States.[53] Concerning those MS that did not provide information in completing the implementation tables (CY, IE, LT and UK), the pertinent information for these is the result of desk research alone. Annex I.4 provides an overview of the documents consulted at the EU and international level as part of the desk research.

4.2 Field research

A total of **147 stakeholders**[54] have been consulted as part of the Evaluation. This has been achieved using a combination of instruments addressing either the EU or the MS level:

- At the EU level: 27 **interviews** with representatives from EC DGs and Agencies, and European associations of CI owners/operators;
- At the MS level: All but four MS (CY, IE, LT and UK)[55] have been consulted through a variety of means, including: an **online survey** targeting PoCs and other national competent authorities and CI owners/operators in order to collect comprehensive and specific information on the implementation of the Directive; two **workshops** (one with PoCs/competent authorities and one with CI owners/operators) organised with the support of the EC in Brussels on 13-14 November 2018, where the Evaluation team gathered feedback on the interim findings of the study; and four **case studies** that aimed at collecting first-hand information on the implementation of the Directive in four MS (DK, ES, FR, SK). Each case study consisted of six interviews per MS involving the PoC, other national competent

[50] In order to account for the responses of the Public Consultation, the project timeline was extended. For this reason, the submission of the Final report for review by the Contractor was postponed (from 15 January 2019 to 22 February 2019).
[51] Booz & Company GmbH. (2012). Study to support the preparation of the review of the Council Directive 2008/114/EC on the "identification and designation of European critical infrastructures (ECI) and the assessment of the need to improve their protection".
[52] When coming from the PoCs, information is reported in the implementation tables with a different colour code (blue) and with indication of the PoC among the sources.
[53] AT, BE, BG, CZ, DE, DK, EE, ES, FI, FR, EL, HR, HU, IT, LU, LV, MT, NL, PL, PT, RO, SE, SI, SK.
[54] This number accounts only for stakeholders involved directly by the Evaluation team and do not account for the answers to the PC.
[55] It is worth noting that CY and IE did not take part to the consultations conducted for the previous study from 2012 (Booz & Company GmbH), while it was possible to retrieve information on LT and UK from that study.

authorities and CI owners/operators. An additional **consultation with the PoCs** was carried out in February-March 2019 in order to validate the findings of the study;

- Moreover, 10 experts in the CIP field working in academia and/or think tanks have been consulted through **interviews**.

Moreover, at the EU level, a **public consultation** (PC) was launched by the EC targeting a wide array of stakeholders, including members of the public. The consultation consisted of a survey containing a number of questions related to the current and future threats facing CI, the Directive, and its implementation by the MS.

In order to mitigate the effects of some of the limitations encountered in the study (see Section 4.3), in addition to what was originally planned, additional field research has been undertaken in the form of **a round of validation of the implementation tables**. The CIP PoCs were asked to validate the content of the tables, fill in any gaps in the information contained, and, where necessary, resolve any instances of conflicting information available through different sources.

Annex I.1.3 includes additional detail regarding each consultation tool, while Annex I.3 includes a synopsis report summarising all consultation activities. Feedback gathered through the field research is included in the report on an anonymous basis as appropriate.

4.3 Limitations of the methodology and robustness of findings

4.3.1 Problems encountered and solutions found

The study encountered some difficulties, namely:

- **Fragmentation of information and unclear identification of national measures related to the implementation of Directive 2008/114**. The different MS pursued different approaches in implementing the Directive. For instance, in some MS, like RO and HR, national legislatures adopted new legislation or amended existing legislation in order to bring the existing normative framework in line with the requirements of the Directive. Meanwhile, other MS (e.g. AT, FI, NL, UK) opted to leave existing legislation unchanged. In such instances, the Directive was implemented through administrative measures. While some MS introduced new legislation covering most of the provisions of the Directive, others only adopted measures covering specific aspects, an arrangement that served to create some confusion between pre-existing national laws and the Directive. Moreover, MS notified to the EC the transposition of the Directive but did not always clearly indicate the specific measure at national level that accomplished this. This made it difficult to identify all relevant information within the time and budget constraints of the project.

Solution found: The Evaluation team worked to update the findings of the 2012 evaluation of the Directive[56] with recent developments in order to fill any gaps in the record. Moreover, sources identified by the Evaluation team through desk research have been triangulated and integrated with sources and inputs gathered from the national PoCs engaged through the online survey and ad hoc queries.

- **Some information relating to the implementation of Directive 2008/114 was not available through desk research**. For instance, criteria and related thresholds used by MS to assess the risks associated with the disruption or destruction of a CI, information on channels used for bilateral and multilateral discussions, or the content of the OSPs maintained by CI operators, and the related controls performed by national competent authorities are not typically available in consulted national documentation. This meant that the analysis of these provisions relied chiefly on stakeholder feedback, leaving limited scope for triangulation of evidence.

Solution found: The results of the desk research conducted by the Evaluation team and summarised in the implementation tables were shared with all PoCs. A total of 24 MS[57] responded, allowing the Evaluation team to integrate in the implementation tables details on national practices with publicly available information. Moreover, case studies were used in order to achieve a higher level of detail and to investigate aspects that are not described in national law. While much of this information is confidential, the interviews

[56] Booz & Company GmbH. (2012). Study to support the preparation of the review of the Council Directive 2008/114/EC on the "identification and designation of European critical infrastructures (ECI) and the assessment of the need to improve their protection".
[57] AT, BE, BG, CZ, DE, DK, EE, ES, FI, FR, EL, HR, HU, IT, LU, LV, MT, NL, PL, PT, RO, SI, SK, SE.

that were carried out as part of the case studies enabled the Evaluation team to gain a better understanding of national implementation practices.

- **The current level of CIP is the result of the co-existence of several instruments.** At the *EU level*, these include the ECI Directive, EPCIP and other sectoral and cross-sectoral security measures. At the *national level*, these include measures aimed at implementing EU instruments as well as other national initiatives to protect CI. The co-existence between EU and national-level instruments made it difficult to isolate the contribution of the Directive specifically. The Directive covers highly regulated sectors in which a significant amount of EU legislation has been implemented over the years. It seems that there is comparatively little documentation concerning the results achieved by other measures in relation to the protection of CI (e.g. evaluations, fitness checks of sectoral legislation); the little information that is available is fragmented in nature. Moreover, the implementation of the Directive's provisions relies on different approaches to the definition of the national policy for the protection of CI. In light of the narrow scope of the study, which is limited to the implementation of the ECI Directive, information on national CIP frameworks was not collected on a systematic basis.

Solution found: The Evaluation team widened the scope of the analysis of the coherence of the Directive in order to improve its understanding of the relationship between the Directive and other existing measures. At the EU level, the analysis focused on a number of pieces of sectoral EU legislation covering security-related aspects with the aim of identifying areas of overlap, duplication or potential synergy (Section 6.2.1). At the national level, the analysis relied only on stakeholder feedback gathered as part of the online survey and the case studies. Findings stemming from the analysis at the EU level were used to guide consultations at the national level and to understand if identified areas of overlap represented a concern for national stakeholders. This allowed for the Evaluation team to make a qualitative assessment as to the causal linkages between the implementation of the Directive and the current level of protection of CI vis-à-vis the MS that were the objects of the case studies.

- **ECI are not known, as this information is confidential**. The fact that this information is confidential made it impossible to distinguish between operators of infrastructures that are considered critical (and therefore subject to national-specific security requirements) at the MS level and European CI. This made the analysis of the results and costs associated with Directive implementation complex. The Evaluation team surveyed operators without knowing whether their responses would be based on experience running designated ECI, or "merely" informed opinions on the matter more generally. This difficulty also reduced the room for triangulation between different sources of information, with some considerations only based on stakeholders' opinions.

Solution found: The Evaluation team phrased questions according to hypothetical scenarios and asked stakeholders to express their views on potential changes that might occur in the context of their daily work in the event that the infrastructure that they are responsible for were to be identified as ECI. Moreover, evidence from MS with a large number of designated ECI have been compared with evidence from MS with a small number of (or no) designated ECI, this in order to understand to what extent the Directive was implemented differently in these two categories of MS. Case study interviews and the aforementioned workshops were also used as opportunities to double-check the existence and nature of the costs documented through other forms of consultation.

- **The baseline situation before 2008 is not fully known.** While there is some information on national CIP measures prior to the Directive coming into force, there is to the Evaluation team's knowledge no extensive analysis that would allow for a systematic comparison between the pre-2008 situation and the current situation, which would inform the assessment of the changes brought about by the Directive.

Solution found: The Evaluation team reconstructed to some extent the pre-Directive situation starting from the answers of the PoCs to some specific questions included in the online survey. These were then triangulated with information collected through the desk research and the case studies. This exercise allowed for an overview of the existence of the elements included by the Directive in specific national CIP frameworks prior to the adoption of the Directive.

4.3.2 Overall quality of data

Despite the difficulties that were encountered, the **quality of the information gathered is generally satisfactory** thanks to a combination of additional actions taken on the part of the Evaluation team and the role played by stakeholders in validating the information that was

collected. The information is satisfactory both in terms of quality and of breadth of representation from different categories of stakeholders, not least at the MS level. This being said, limitations have been highlighted in the recommendations for future action as appropriate (see Chapter 8).

5 PRESENT IMPLEMENTATION STATE OF PLAY

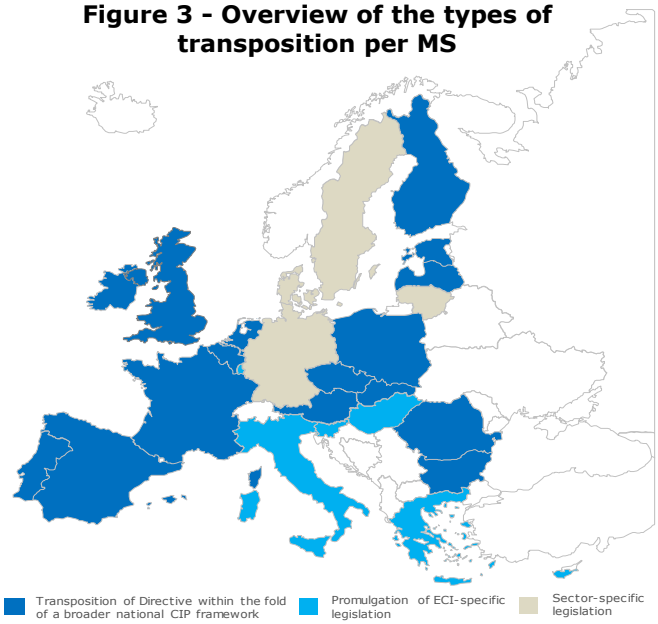
This Section provides a **comparative analysis of the implementation/application of the Directive at the national level**. It lays out the necessary groundwork and context in order to respond to the evaluation questions, and aims to provide a comprehensive overview as to how the different provisions of the Directive have been practically implemented by the MS.

The findings are mainly drawn from the data included in the implementation tables (see Annex II), are numbered to facilitate cross-referencing, and are highlighted with the symbol '☞'. When other evidence is used, this is referenced in the corresponding footnote. After providing an initial overview of the implementation and transposition strategies adopted by the different MS in the Section below, the discussion will then turn to an analysis of the main provisions of the Directive.

5.1 Implementing and transposing measures

The MS adopted a variety of approaches in transposing the Directive in their national legislation. The following general approaches were observed:

Figure 3 - Overview of the types of transposition per MS



Source: Author's elaboration of data in Implementation tables

- Transposition of the Directive as part of broader national CIP frameworks;[58]
- Promulgation of ECI-specific measures (i.e. legislation focusing exclusively/almost entirely on ECI);[59]
- Sector-specific legislation (i.e. legislation pertaining specifically to the energy sector or the transport sector, with separate transposition measures in each sector).[60]

The majority of MS (18) opted to transpose the Directive within the fold of national CIP legislation (either through amendments to existing national legislation or by writing such legislation "from the ground up", as was the case in BG, HR, RO and ES). The remaining MS are distributed more or less equally in terms of the other two approaches (the promulgation of ECI-specific measures and sector-specific legislation) (4 and 6 MS, respectively). The results of this exercise are depicted in Figure 3.

Generally speaking, most ECI-related legislation had been drafted by the MS by 2012, and only a handful of MS have amended their legislation since then. Moreover, even when amendments were made, these have only **provided clarifications on specific topics**. The only exception is Croatia, which passed a comprehensive National Law on Critical Infrastructures in 2013. However, it is important to bear in mind that Croatia acceded to the EU on 1 July 2013, meaning that its transposition legislation was predictably performed at a later date when compared

[58] 12 MS amended or introduced national legislation (BE, BG, CZ, EE, ES, HR, LV, MT, PL, PT, RO, SK), five MS introduced administrative amendments (AT, IE, FI, NL, UK), and FR deemed that there was no need for any transposition measures (existing national legislation deemed to be sufficient).
[59] CY, EL, HU, IT, LU, SI.
[60] DE, DK, LT, SE. In SE modifications of the national legislation were very limited and mainly focused on the allocation of responsibilities for the identification of potential ECI and the designation of the PoC. Even though sectoral legislation was not substantially modified as a consequence of the Directive, the identification process has been performed by the competent sectoral institutions and according to the criteria described in the Directive.

to the other MS. National transposition is therefore quite consolidated, with few developments of note in recent years (described in Annex I.6.1).

5.2 Definitions and scope

5.2.1 Definitions

National transposition has primarily focused on the definitions of CI and ECI, respectively. Concerning the **definition of CI**, **a plurality of MS (12)**[61] **opted to introduce the same (or a quite similar) definition as that proposed in the Directive**, and 4[62] did not include a CI definition in the transposition legislation (on account of the fact that the MS introduced amendments to administrative provisions rather than new legislation). In the case of 1 MS (IE), information was unavailable.

However, as represented in Table 2, the fact that the definition was transcribed in a broadly similar way **means a certain degree of heterogeneity across MS can be observed vis-à-vis specific aspects of the definition** (☞ *Finding 1*). The biggest difference concerns the **nature of CI**. For 10 MS these are both assets and systems, putting the various definitions in line with that provided in the Directive.[63] However, in 2 cases[64] the definition solely focuses on the systemic character of CI. Finally, in 7 other cases,[65] an asset-focused definition is used. The difference is not purely semantic, as defining CI as assets indicates a focus on the protection of specific components, while viewing CI as systems suggests a broader view focused on ensuring the continuity of the service provided by the infrastructure.

Table 2 - Elements included in the definition of CI by MS[66]

Elements of the definition of CI		Number of MS
Object	Asset	17
	System or part thereof	12
	Process	2
	Network	2
	Critical infrastructure object	1
	Vital service or function	3
	Point of vital importance	1
	Organisational and physical structure and facility	1
	Institution	1
	Enterprise	1
Essential to…	Vital societal functions	14
	Health	16
	Safety and security	18
	Economic or social well-being of people	12
	State economy/economic stability	6
	Continuous functioning of the government	2
	Functioning of a vital/essential service	2
	Other elements mentioned by single MS: property; environment; basic needs of the population; war potential; survival capacity of the nation; supply shortages; interests of the state or society; interests of the state or society; avoidance of social disruption	1

Source: Authors' elaboration

Some variance can also be observed concerning **the elements against which an infrastructure is considered to be essential**. MS tend to focus on "vital societal functions", "health", "safety",

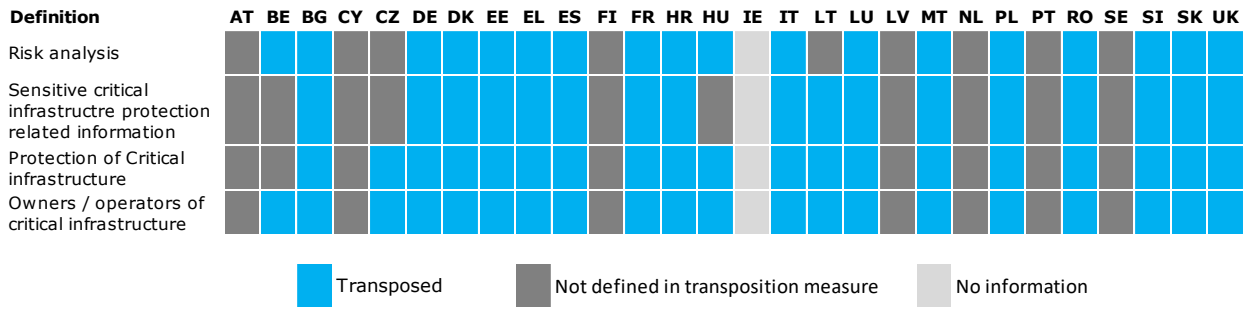
[61] AT, BE, BG, DK, EL, IT, LV, LU, MT, PT, RO, SI.
[62] CY, FI, NL, SE.
[63] AT, BE, CZ, DK, EL, HR, LU, LV, MT, PT.
[64] BG, PL.
[65] ES, HU, IT, LT, RO, SI, SK, though it is important to note that ES, IT, RO and SK place emphasis on assets being part of infrastructures.
[66] Blue cells relate to the elements of the definition included in the Directive.

"security", and "economic or social well-being" as indicated in the Directive,[67] though a sizeable number of MS (6) also introduce the notion of economic stability. Meanwhile, 3 MS used definitions focused on the continuous functioning of the government/survival capacity of the nation.

Less variance was observed in terms of the definition of ECI. 17 MS[68] adopted the same definition of ECI as that introduced in the Directive,[69] while 6 did not formally introduce the definition in the transposition measures.[70] Of the remaining MS, 3 opted to introduce an "abridged" definition of ECI, which omits reference to cross-cutting criteria (though this is not to suggest that the methodology for identifying ECI as stated in the Directive is not applied in these MS).[71]

Concerning the **other definitions** present in the Directive (e.g. "protection" of critical infrastructures, "sensitive information", "risk analysis", "owners/operators of ECI"), those MS that did not directly transpose these definitions were those that pursued administrative provisions (AT, FI, NL, SE). In those cases where a dedicated ECI legislation was introduced, the definitions were often transported on a near-verbatim basis (as in the case of IT, LU, EL and SI).

Figure 4 - Transposition of Directive 2008/114 definitions (excluding CI/ECI)[72]



Source: Authors' elaboration

Finally, **11 MS**[73] **introduced additional definitions** in their national transposition legislation (☞ *Finding 2*). Some key examples include definitions like: *Cross-cutting and sectoral criteria* (CZ, ES, HR, HU, LU, SK); *Competent authorities/stakeholders* (HR, RO, SI); *Critical zones* (defined by EU as areas in which an elevated number of CI/ECI are present); *Emergency* in the context of CIP and how to manage it when it arises (EE, ES, HU, PL, RO). Other definitions that have been provided in legislation include *essential service* (RO), *cybersecurity* (EE, ES, HU) and *negative effect/spill-over* produced by the disruption of a CI/ECI (IT).

5.2.2 Scope

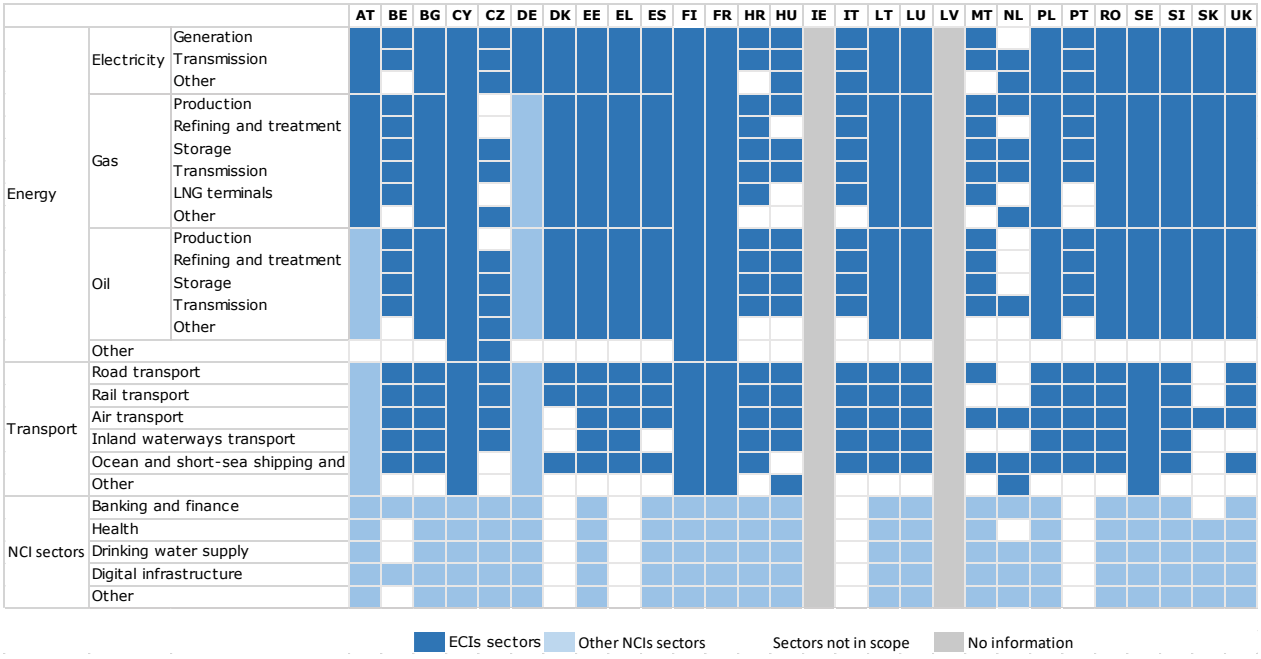
Most of the MS included in the scope provisions pertaining to the energy and transport sectors and the related sub-sectors listed by the Directive, with some additional specificity provided by some MS depending on the sector (see Figure 5).

For the energy sector, a significant majority of the MS (24) specified the sub-sectors, indicating in most cases that all three sub-sectors are in scope (with the exception of AT and DE). 3 MS (CY, FI and FR) indicated in their transposition legislation that the energy sector is in scope, while not indicating specific sub-sectors (which leaves open the possibility of applying the rules of the Directive to other sub-sectors).

[67] 12 MS (AT, BE, BG, DK, EL, IT, LU, LV, MT, PT, RO, SI) mention that CI are essential to vital societal functions, health, safety & security, economic or social well-being of people. Note that some MS introduced definitions that omit either the word "safety" or the word "security". These are AT, DK, EL, PT (which omit "security" from the definition), as well as IT and LV (which omit "safety"). However, these latter cases can be likely ascribed to linguistic characteristics, as there are not always separate words for "safety" and "security". This is also reflected in the corresponding translations of the Directive.
[68] BE, BG, CZ, DK, FR, EL, HR, HU, IT, LU, LV, LT, MT, PT, RO, SL, UK (only for Gibraltar).
[69] Namely CI located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure. Article 2(b) of the Directive.
[70] AT, CY, EE, FI, NL, SE.
[71] ES, DE, SK.
[72] Note: definitions for UK also apply to Gibraltar.
[73] BG, CZ, EE, ES, HR, HU, IT, LU, PL, RO, SK.

The situation in the transportation sector is more diverse and complex (☞*Finding 3*). The air transport sub-sector is the one most often cited in the transposition legislation (19), while inland waterways (14), sea transport (16) and rail transport (17) are cited less often. The type of transportation infrastructure in scope generally follows the geographical and transport needs of MS. For instance, MT did not indicate the rail infrastructure sub-sector, given the fact that it is a relatively small island with no currently operating railway infrastructure, while CZ, being landlocked, did not identify the sea shipping sub-sector as one of relevance to the MS for the designation of ECI.

Figure 5 - Sectors and sub-sectors where MS can identify ECI and NCI[74]



Source: Authors' elaboration

Differences in the identification of sub-sectors also appear to be linked to sectoral transposition approaches. For instance, DE adopted a sectoral approach to transposition (as shown in Section 5.1); due to the result of the identification process DE focused on the energy sector, and particularly the electricity sub-sector.

Moreover, **CIP measures in 22 MS have a wider sectoral scope compared to that of the Directive** (☞*Finding 4*). For instance, those MS that went beyond the scope of the Directive referenced banking and finance, healthcare, the supply of drinking water and digital infrastructure as key NCI sectors.

5.3 Identification of ECI

There is evidence of **different starting points and approaches towards the identification of potential ECI** (☞*Finding 5*). While some MS (such as FR) already had a list of CI prior to the Directive coming into force, others (ES, RO) saw the adoption of the Directive as an opportunity to list the existing infrastructures located on their territory. Moreover, when transposing the Directive, MS adopted various practices. These included: a sectoral identification process in other MS (FR); a bottom-up approach where CI operators were obligated to submit to the competent authority an "identification report" (HU); or other identification means using other inputs (AT, PT).[75]

[74] A particular case is NL, where the focus is on critical processes, identified by the sectoral ministries within each sector, and whose continuity is guaranteed by one or more operators. Even though currently critical processes have been identified in the sub-sectors marked in blue in the Table, nothing excludes that a sectoral ministry could identify as critical one process within a sub-sector marked as white as it in an on-going process.
[75] Workshop: PoCs.

In considering the first step of the identification process (the application of sectoral criteria), **all MS for which data was available**[76] **apply sectoral criteria as indicated in the Directive, with little further elaboration and detail on the matter** (☞*Finding 6*). MS do not publish the sectoral criteria.

The second step (the application of the definition of CI), **has been, generally speaking, transposed *verbatim* in national transposition legislation, with little to no variance** (☞*Finding 7*). In 11 MS,[77] the criteria are included in dedicated legislation or documents, usually government decrees. Some MS (5)[78] also made use of the EC's non-binding guidelines and approximate thresholds.

The thresholds for the cross-cutting criteria are typically defined on a case-by-case basis[79] as indicated in the Directive **and are confidential** (☞*Finding 8*). In 2 cases (FI, SI), no reference is made to how thresholds are defined in the transposition legislation. In this context, it can be mentioned that 1 CIP PoC that was interviewed suggested that the cross-cutting criteria and approximate thresholds which form part of the EC's non-binding guidelines for the implementation of Directive 2008/114 might be applied directly.

Even though cross-cutting criteria are often confidential, there is evidence that **they are interpreted and implemented in a very heterogeneous way across MS** (☞*Finding 9*). This is confirmed by stakeholders consulted during the four case studies that were carried out as part of the Evaluation. Moreover, the analysis of the little information that is publicly available on cross-cutting criteria shows heterogeneity and seems to suggest that the thresholds themselves can be quite different and, thus, somewhat difficult to compare (see Box below).

Box 1 – Examples of cross-cutting criteria

In the case of **Czechia**, cross-cutting criteria for the identification of critical infrastructure are defined in the Governmental Order No. 432/2010 and are as follows:

- More than 250 casualties or more than 2,500 people who require hospitalisation for longer than 24 hours;
- Economic impact with a threshold value of economic loss greater than 0.5% of GDP; or
- Impact on society with a threshold value of a large limitation of necessary service provision or another serious disruption into the daily lives of more than 125,000 people.

In **Spain**, the cross-cutting criteria take into account the impact on the population (casualties and injured), economic effects, environmental effects, and service disruption (recovery time in terms of number of days, geographical extension, size of affected population, cascading effects on other assets, etc.).
To assess the impact, a criticality scale is used, with a range from 0 to 5. Scores of 4 and 5 are considered critical while lower scores (1-3) are essential. Assets are mapped against the consequences of a potential service failure. In turn, the criticality levels (from 0 to 5) are mapped against the cross-cutting criteria (casualties, economic impact, etc.). This analysis is done jointly with sector-specific criteria, which are unique to each of the 12 critical sectors mentioned in the Spanish legislation.

Estonia uses a somewhat different approach. Here, a rating scale is used on a case-by-case basis instead of providing exact thresholds for the identification of vital services. This rating scale considers:

- Number of service users or number of people (from fewer than 1,000 to over 100,000) that benefit from the service over the course of a given year;
- Necessity of use by private individuals or companies over the course of a given year (from being used only when other services are not available to being used every day);
- Service replaceability (from immediate replacement to irreplaceable);
- Connection to other vital services and services of general interest (from influencing none to influencing five or more other services);
- Is the service itself an alternative to other socially important services (vital services and services of general interest) (from not being an alternative to being an alternative to three or more other services);
- Timeframe of feeling the consequences of disruptions (from weeks to hours); and
- Influence on the life and health of the person in need of the service (from being a nuisance to being a lethal threat).

[76] AT, BE, BG, CZ, DK, EE, ET, FR, DE, EL, HR, HU, IT, LT, LU, LV, MT, NL, PL, PT, RO, SE, SK, SI, UK.
[77] AT, BE, BG, CZ, DE, DK, ES, HU, IT, SE, SK.
[78] EE, DE, IT, LU, SI.
[79] BE, BG, FR, EL, LT, MT, NL, PL, PT.

Austria also uses a tiered approach, based on the "APCIP Masterplan 2014".[80] The following primary criteria are considered as part of the Austrian approach:

- Time factor – impact within minutes/hours;
- Type of impact – impact on security police; impact on lives/health of people;
- Extent of impact – impact on a vast number of people; and
- Redundancy – no/few comparable companies available to provide the service.

Besides the cross-cutting criteria, **the "availability of alternatives" was also interpreted differently by MS** (☞*Finding 10*). The issue lied in exactly what constitutes an alternative. For instance, stakeholders interviewed during the case studies reported that, especially in the case of transport sector, this notion was interpreted in a broad sense. For this reason, any means of transport was seen to be an available alternative. [81] In other words, this requirement has been applied more as a workaround—allowing MSs to look "elsewhere" instead of performing the entire identification procedure.[82]

The third step (the application of the transboundary element) **was transposed quite similarly across MS, which typically re-stated the main relevant points of the Directive without providing any additional detail** (☞*Finding* 11).[83] Details as to how the dialogue with authorities and operators in other countries to discuss transboundary impacts such exchanges might take place are not provided in national laws.

The final step in the ECI designation process (the application of cross-cutting criteria) is intertwined with the previous steps, and in particular with the second step (the application of the definition of CI). An analysis of how cross-cutting criteria (and relevant thresholds) were applied was described earlier in this Section.

While it appears that the identification process was initiated by all MS where information was available,[84] **only a limited number of MS (13) ultimately identified at least one potential ECI**.[85] In most cases, **those infrastructures that were initially identified did not pass through every stage of the four-step process**, meaning that they were not assessed as being potential ECI[86] (☞*Finding* 12).

5.4 Designation of ECI

Aside from the designating authority, which is often clearly identified in national transposition legislation, **the process of designation tends to be less formalised** (☞*Finding* 13). The designation process between different MS is, typically speaking, described in a way that is coherent with the Directive, which does not specify how such bilateral/multilateral discussions on the designation should take place, nor the specific content. This is due to the fact that this information pertains to traditionally sensitive issues, such as security and diplomacy (the designation process inevitably involves dialogue with other MS). CIP PoCs have been reluctant to share specific details

[80] Austrian Programme for Critical Infrastructure Protection.
[81] Case study: 2 MS; Survey: three PoCs; Workshop: PoCs. In 2 case studies stakeholders mentioned that transport CI were not identified as ECI because alternative means of transport to the other MS existed. The concept of "no alternatives" is considers ambiguous, as it is hard to define what represents an essential service. The operator mentioned that a literal application of the law in the rail sector seems to imply that rail is never in scope, as there are always alternatives, such as road transport. However, even local commuter train interruptions would have significant adverse effects, even though local rail are not strictly speaking CI.
[82] Lazari, A. (2014). European Critical Infrastructure Protection. Springer.
[83] Cases in which more detail is given include SI, where it is specified that this is achieved through informal bilateral dialogue with other MS; the NL, which applies the transboundary element by requiring an annual report by the sectoral ministries to identify potential ECI; ES, which also focuses on operators that operate CI in more than one MS to select potential ECI; FR, which assess international interdependencies through CI operator reports and by means of the national security directive in force.
[84] Survey: 91% (N=20) of PoCs answered that the MS they represented did start the identification process. The PoC of one country, answered Do not know, but ECI have been designated in its country. Only 2 PoCs mentioned that the identification process was not started, though information provided in the Implementation tables clarifies that the responses in these cases are to be intended merely that the identification process was not fruitful in identifying potential ECI. No information available for CY, IE, LT, LV and UK.
[85] Information retrieved from survey responses triangulated with data on designation provided by DG HOME.
[86] Survey: 81% (N=17) of PoCs declaring that their MS started the identification process reported that this was concluded with the identification of a potential ECI in no or less than half of cases.

on this, but reported that this process can take place through different channels and with different degrees of formality. A more detailed list of the channels used by some MS[87] to conduct negotiations is provided in Table 3.

Table 3 - Communication channels for bilateral/multilateral discussions

Communication channels between MS	Number of MS
Formal meetings and visits	5
Exchange of emails or informal letters	4
Formal letter	3
Working groups[88]	1
Telephone	1

The final step in the procedure (informing ECI operators of designation) **tends to be described in greater detail in national transposition legislation, though observed practices are predictably quite varied**. Aside from the formal designation letters mentioned in the paragraph above, the national transposition measures typically give an indication as to the maximum amount of time permitted between designation and notification of operators (e.g. five days in LT, 10 days in RO), the form that this notification should take, and, at least in the case of ES, how any such notification should be communicated.

Naturally, the designation process depends on the outcome of the identification process. Given the limited number of potential ECI which survived the different steps in the identification process, fewer MS (11)[89] entered into bi/multi-lateral discussions on designation with other MS than entered into discussions on cross-cutting criteria during the identification step.

No specific issues were signalled by MS authorities in relation to the designation stage. The results of designation discussions seem to have a slightly higher "rate of success" than the identification process. After all, around half of the MS (6) that launched the designation process ended up with the designation of *all*, *most, or half* of the total number of potential ECI identified during the identification phase.[90]

As of September 2018, there are **93 designated ECI**.[91] Based on the information that has been made available, it can be seen that:

- All but five ECI (88) are in the energy sector, with the remaining 5 in the transport sector (☞*Finding 14*);
- There is a strong geographical component to the distribution of ECI. Only 10 MS have designated ECI, and around 60% of these have been designated in just 2 MS. The majority of ECI as of September 2018 are located in MS in Central and Eastern Europe (☞*Finding 15*); and
- Large MS have designated a relatively small number of ECI.

A factor that might potentially have triggered a high rate of ECI designations is the particular geographical situation or geopolitical status of certain MS. It could be argued that, since Directive 2008/114 has a focus on transboundary externalities and on the concept of "affected MS", MS with long and/or a higher number of borders may have been engaged in more bilateral discussions aimed at designating ECI than countries with shorter borders or fewer immediate neighbours. Geographical considerations may also explain a higher number of designations in MS with a strategic position within the Union in terms of energy transmission. However, this is mere speculation; there is no definitive evidence from the Evaluation to substantiate these claims.

Moreover, the **number of designated ECI seems to be somehow correlated with the type of transposition measure adopted.** For instance, the MS that opted to formally embed the ECI identification and designation process within a wider CIP framework by means of legislative measures are more likely to have designated ECI on their territory. It appears that norms relating to the identification and designation of ECI must **"find a place" within a broader context of**

[87] AT, BE, BG, DE, EE, FR, IT, RO.
[88] Estonia formed in 2010 a working group involving Finnish, Lithuanian and Latvian experts.
[89] Information retrieved from survey responses triangulated with data on designation provided by DG HOME.
[90] Survey: 35% (N=6) of PoCs.
[91] Information provided by DG HOME.

national CIP in order for an ECI identification and designation process to go forward. If they are relegated to sectoral legislation or isolated within ad-hoc transposition norms, the probability of identifying and designating ECI appears to decrease significantly.

5.5 Operator Security Plan

In the Directive, the content of the Operator Security Plan (OSP) is described at a general level. In some cases (BE, BG, EL, IT, RO), the transposition legislation stipulates that the content of each OSP must include the same level of detail as that provided by the Directive. Meanwhile, in other MS (FI, NL, SE), a similar amount of detail is not required. The lack of detail in such cases can also be attributed to the fact that, as the OSP or equivalent was already present in most MS, no specific transposition legislation was required.

Operator Security Plans are confidential documents and it has thus not been possible to compare, in terms of content, one ECI to another. However, evidence from the field research confirmed the current differences among MS.[92] Given the limited details included in the Directive, **each MS adopted this provision using their own interpretations of what needed to be done**; this has led to the **adoption of different criteria for use in assessing risks** for each MS (☞*Finding* 16).

The Directive seems to have done little to harmonise the OSP requirement. In many cases, MS already had equivalent requirements (see the baseline at Section 2.3) and it can be said that the Directive "helped formalise and bring under legal framework what was already in place at an operational level".[93]

Concerning the review of the OSP, which the Directive recommends performing regularly, only 9 MS have introduced in their respective transposition legislation indications as to when these should be carried out.[94] The remaining MS for which data was available (11) have not indicated how often OSPs should be reviewed, but only that this should be done on a regular basis.[95]

In terms of verification that operators have indeed put in place their OSP, **two approaches** seem to be play (☞*Finding* 17):

- An **enforcement approach**, whereby MS regularly carry out regular formal reviews of OSPs and on-the-spot checks;[96]
- A **collaborative approach**, in which no formal regulatory/compliance checks are imposed. Instead, the system is based on mutual collaboration between the government and operators.[97] Indeed, the presence of structured CIP forums (the Centre for the Protection of National Infrastructures in the UK being a prime example) and/or Public-Private Partnership (PPP) approaches in some MS implies that the level of communication and co-operation between the public and private sector was already significant prior to the Directive. In such contexts formalised "enforcement" measures are not viewed as being particularly necessary.[98]

5.6 Security Liaison Officer

Often MS' transposition measures do not include specific requirements that the Security Liaison Office (SLO) should satisfy (e.g. role, key responsibilities, clearance). Such

[92] Case study: 3 MS (PoC, Other Ministries, CI owners/operators). Workshop: CI owners/operators.
[93] Booz & Company GmbH. (2012). Study to support the preparation of the review of the Council Directive 2008/114/EC on the "identification and designation of European critical infrastructures (ECI) and the assessment of the need to improve their protection".
[94] Yearly in the case of HR, LT and PT; twice a year in EE, PL and RO; every two years in ES; every four years in CZ; every five years in IT.
[95] AT, BE, CY, DE, FR, EL, HU, LU, LV, SK, UK (for Gibraltar).
[96] BE, CZ, EE, ES, FR, HR, HU. These checks are typically graduated with the perceived threat level and importance of the CI/ECI.
[97] This is the case of AT, NL, SE, UK.
[98] Booz & Company GmbH. (2012). Study to support the preparation of the review of the Council Directive 2008/114/EC on the "identification and designation of European critical infrastructures (ECI) and the assessment of the need to improve their protection".

requirements are instead typically provided for in resolutions and/or administrative decisions (☞*Finding* 18).

Given that the Directive does not clearly define the SLO function, the individuals that are assigned the role vary in terms of competency, responsibility and background. One EU-funded report on this subject[99] has shown the existence of **heterogeneous criteria and job descriptions** (☞*Finding* 19). Currently, the situation in terms of SLO profiles varies among the MS, with some setting stringent criteria, while others simply restate in their transposition measures the text of the Directive (see Box 2).

Box 2 – Examples of SLO descriptions

The applicable law in **Czechia** states that the SLO must be a person meeting all requirements of professional competence, has obtained university or college education (in security studies, civil protection or crisis management), or has at least three years of experience in one of these fields. In **Hungary** it is stated that the SLO must be capable of performing his/her duties potentially on a 24/7 basis. In **Romania**, the law states that the SLO is the head of a specialised compartment (comprised of at least a three-member team) under the direct authority of the leader of the competent public authorities, respectively that of the national/ECI owner/operator. In **Italy**, the ECI owner/operator has simply to communicate the name of the designated SLO to the responsible public authorities without specifying what specific role the SLO has.[100] In **Malta**, the CIP Directorate provided on its website a description of the desired academic background, skills, and attributes of a SLO.[101] More specifically, the person should be a subject matter specialist, with a degree in risk, continuity and/or disaster management. Besides management skills, this person should have the right interpersonal skills to communicate at all levels of its organisation.

Moreover, in the vast majority of MS there is **no explicit indication concerning the communication channels used by SLOs in order to communicate with competent MS authorities**.[102] This might be for the fact that such information is confidential in some MS, but it could also be due to a lack of procedures, especially in MS with no designated ECI.

5.7 Reporting

The content of the threat assessment, conducted by MS in relation to subsectors where ECI have been identified, is confidential. Nevertheless, it was possible to determine that **the content of the threat assessment is typically focused on sector-specific issues and risks.** For instance, AT's threat assessment for the energy sector focused on blackouts, interdependences and cyber threats. Furthermore, these can include proposals for the implementation of organisational and technical measures necessary to prevent, react and, where appropriate, alleviate the possible consequences of different threat scenarios (as is the case in ES's sectoral strategic plans).

As for the biannual report on risks, threats and vulnerabilities required by the Directive, a large majority of MS adopted the Directive without making any further specifications. With some minor exceptions, most MS have simply identified the competent body responsible for sending the necessary documentation to the EC within the foreseen timeframe.

In the vast majority of cases, the CIP PoC or the coordinating Ministry is the designated authority that submits the required reports to the EC. These reports are compiled on the basis of information gathered from owners/operators of ECI and/or other competent bodies.

All MS that designated an ECI submitted these reports to the Commission.[103] However, **the use of this information by the Commission has been limited** (☞*Finding* 20). The EC has not systematically provided feedback on these reports, nor has it worked to synthesise the situational pictures at the MS level in order to create a pan-EU assessment of CI vulnerability.

[99] Setola, R. (2014). Security Liaison Officer Project - Final Report. COSERITY Lab (project co-funded by the EC).
[100] Setola, R. (2014). Security Liaison Officer Project - Final Report. COSERITY Lab (project co-funded by the EC).
[101] Malta CIP Directorate Website, SLO Profile, https://maltacip.gov.mt/en/About/Pages/SLO-Profile.aspx.
[102] Indeed, only in LT it was found that the law requires, after the appointment of an SLO, that the Prime Minister's Office should provide a specific telephone number and an email address to the SLO, in order to have direct communication and report possible events, incidents, risks and threats.
[103] Data provided by DG HOME triangulated with responses to the survey question "To your knowledge, how frequently does the Member State that you represent submit data to the European Commission on the types of risks, threats and vulnerabilities facing sectors in which ECI have been designated?".

5.8 European CIP contact point and organisational set-up

In Article 10 of the Directive, it is stipulated that each MS should designate a European CIP Contact Point charged with coordinating all issues concerning the protection of ECI at national and international level. This includes managing relations and interactions with other MS and the EC. The Directive leaves room for each MS to allow other competent authorities, in addition to the one officially identified as European CIP Contact Point, to be involved in issues relating to CIP.

The European CIP Contact Points are more commonly referred to as CIP PoC and during their meetings discuss CIP issues in general. In this context, it is worth noting that the CIP Contact Point function was also called for when EPCIP was introduced. Here it was stated that "each MS should appoint a CIP Contact Point who would coordinate CIP issues within the MS and with other MS". In practice, these have become one and the same function at the MS level; it seems that the European CIP Contact Points (in the Directive) and the CIP Contact Points (EPCIP) have de facto been merged into the CIP PoCs with responsibilities concerning both CIP- and ECI-related issues.[104]

The Contact Point provision of the Directive has been **approached differently** in the MS, with the designation of offices within ministries of interior being most common (☞*Finding* 21).

However, as shown in Table 4, there is variety in the choice of the institutional body tasked with interacting with the EC and/or with other MS. Indeed, depending on the MS, the CIP PoCs can deal with interior affairs, justice, defence matters, and may represent dedicated CIP agencies, sectoral regulators/oversight authorities or bodies involved in civil protection.

Table 4 - Overview of institutional bodies designated as PoCs

Institutional body designated as PoC	MS
Ministry of Interior	AT, BE, BG, CY, CZ, DE, EE, HU, MT, PT, SK
Prime Minister Office	AT, FR, IT, LT, LU, PL, UK
CIP Agency	ES, RO
Other	DK, EL, FI, HR, LV, NL, SE, SI

Source: Authors' elaboration

Given the range of entities nominating CIP PoCs, there is also **wide variety in the level of specialisation of the CIP PoCs** (☞*Finding* 22). While some MS (e.g. BE, FR, EL, MT, RO, ES, PL) have agencies or directorates within the competent ministries focused solely or chiefly on CIP acting as PoCs, others have bodies that deal with a wide spectrum of matters, including CIP.

On a more general level, **the organisational setup concerning the implementation of the ECI Directive** (identification and designation of ECI, communication, reporting and threat assessment) **varies significantly from one MS to another in terms of both type and number of actors involved** (☞*Finding* 23) (see Figure 6).

[104] Hereinafter ECIP contact points will be referred to only as CIP PoC.

Figure 6 - Number of MS that involve the different types of actors in the Directive's main implementation steps[105]

	Prime Minister	Ministry of Interior	Sectoral Ministries	Ministry of Economy	CIP Agency	Government	Other
Identification	7	11	21	6	3	0	7
Designation	7	15	15	5	4	8	11
Communication with EC and CI operators	7	10	11	3	3	2	8
Reporting and threat assessment	6	10	16	3	4	2	11

Source: Authors' elaboration

The **identification process** is initiated by different types of stakeholders depending on the MS, with a significant **prevalence of sectoral ministries and regulators** (23 MS[106]) (☞*Finding 24*), usually in co-operation with a central authority (typically ministries of interior).[107] The type of authority responsible for ECI identification depends on the type of transposition strategy adopted by the MS. For instance, in cases where transposition served to amend sectoral legislation in the transport and energy sectors, the identifying authority tends to be the sectoral ministry or regulator. On the other hand, the use of inter-ministerial working groups in the CI identification process (which are coordinated by offices of the prime minister) is more prevalent in cases where transposition involved the development of ECI-specific legislation.[108]

The authorities in charge of the designation process thus tend to be quite varied across the MS. However, what is clear is that when compared with the identification process, MS tend to "escalate" the **designation process** to the upper-most political level. For instance, in eight MS the designation procedure for ECI foresees a collective government decision.[109] Elsewhere, the designation is performed by the sectoral ministry and/or the ministry of interior; in nine MS, these two authorities co-operate in the designation process.[110]

There is also great heterogeneity in terms of responsibility for conducting **threat assessments and reporting to the EC**, though in most cases (16 MS) there is a strong involvement of sectoral ministries, given their subject matter competency. Nonetheless, different approaches are also used.[111]

The variety of actors involved in the main steps in implementing the ECI Directive demonstrates the extent to which **national European CIP governance is fragmented** (☞*Finding 25*). The list of involved parties at the MS level is long, and includes ministries or sectoral regulators involved

[105] Note that one MS may involve more institutions at the same time.
[106] This number represent the number of sectoral authorities and the Ministries of Economy in DE and EE, which are in charge of the sectors in scope
[107] BE, BG, CY, CZ, DE, DK, EE, ES, FI, FR, HR, HU, IT, LT, LU, LV, NL, PL, RO, SE, SI, SK, UK. Of these, in four cases (CY, CZ, HU, SK) the identification process is performed in co-operation solely between the sectoral ministries and the Ministry of Interior, in six (BE, ES, FI, IT, LV, SI) there is involvement of the sectoral Ministry, the Ministry of Interior along with other actors. In three cases (BG, DK, SE) the identification is carried out solely by the sectoral ministries, while in eight cases there is co-operation between the sectoral ministries and other actors, excluding the Ministry of Interior.
[108] As in the case of IT and LV.
[109] CZ, HR, IT, LT, NL, PL, SE, SL.
[110] BE, BG, DE, ES, HU, IT, LV, SI, SK.
[111] For instance: existing national risk assessments can be leveraged (NL), which can be tailored to the specific needs of operators (FR); risk analyses can be carried out or coordinated by the Ministry of Interior/law enforcement/civil protection (CZ, HR, PT); they can be performed by a tailored agency or working group tasked with infrastructure protection (BE, ES, IT, LU); they can be based on a sectoral approach (AT, HU, FI), with strong bottom-up involvement of municipalities and CI operators (SE).

in the energy and transportation sectors, ministries of the interior (which tend to have a focus on policing/internal affairs/civil protection), dedicated agencies (which will have a subject matter expertise concerning CIP), offices of the prime minister, and even ministries of economy/economic development. In practice, this means that the European CIP process typically involves an average of three actors per MS (see Table 5, showing the number of types of national authorities, following the classification provided in Figure 6 above). This implies that stakeholders involved in the process are likely to "speak different languages" within individual MS and between MS.

Table 5 - Number of types of actors involved in the European CIP[112]

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Number of types of actors involved	2	3	2	3	3	4	2	3	1	4	3	3	3	3	*NA*	6	3	2	5	2	4	4	1	3	2	6	2	3

Source: Authors' elaboration

5.9 Overview of key findings of the implementation analysis

The key findings generated from the analysis of the implementation of the Directive are summarised in the Table below and are cross-referenced in the analysis aimed at answering the evaluation questions included in Chapter 6.

Finding number	Description
1	Heterogeneity of the definition of CI across MS
2	Additional definitions introduced in various MS legislation
3	Differences across MS regarding the sectoral scope in the transportation sector
4	Wider scope in the majority of national CIP frameworks compared to the Directive
5	Different starting points for the identification of potential ECI
6	Verbatim transposition of the sectoral criteria for the identification process
7	Verbatim transposition of the CI definition step
8	Confidentiality of the thresholds for the application of the cross-cutting criteria
9	Heterogenous interpretation of the cross-cutting criteria
10	Differences on the interpretation of the "availability of alternatives"
11	Verbatim transposition of the transboundary element step
12	Limited number of MS identifying potential ECI
13	Lack of formalisation of the designation process
14	Large majority of designated ECI in the energy sector
15	Concentration of the ECI in a small number of MS
16	Differences across MS in the criteria used for assessing risks
17	Enforcement or collaborative approach to the review of the OSPs
18	Limited access to the information regarding the SLOs
19	Heterogeneity of criteria and job descriptions for SLOs
20	Limited use of the information reported by MS to the EC
21	Differences in the approach to the designation of the CIP PoCs
22	Heterogenous specialisation of the various CIP PoCs
23	Different number and types of actors involved in the implementation of the Directive
24	Prevalence of sectoral ministries in the identification process
25	Fragmentation of the national European CIP governance

6 ANSWERS TO THE EVALUATION QUESTIONS

6.1 Relevance

This Section assesses the relevance of Directive 2008/114. The first part (Section 6.1.1) focuses on the relevance of specific aspects of the Directive, i.e. the objectives, the definitions, the scope and the formal means of implementation. The second part (Section 6.1.2) focuses on the relevance of the Directive to stakeholders' needs, recent advances and EU priorities.

[112] The number of types of stakeholders involved can go from 0 to 7 (i.e. Prime Minister, Ministry of Interior, Sectoral Ministries, Ministry of Economy, CIP Agency, Government, Other).

6.1.1 Relevance of specific aspects of the Directive

6.1.1.1 Relevance of the objectives

EQ 1.2 To what extent do the scope, set of objectives, but also the formal means of implementation set out in the Directive correspond to the current and possible future threats facing critical infrastructure?

The objectives of the Directive remain relevant in light of current threats to CI from terrorism, cyber-attacks from organised criminals and state actors, hybrid threats and insider infiltration. In an increasingly interconnected Europe, where CI in one country often depend on CI in other countries, and where the absence of internal borders makes the mobility of threats easier, the whole system of CI and related functions is only as strong as its weakest link.[113] This justifies the existence of a common approach to protect ECI.

While the objectives generally remain relevant,[114] there is room to clarify what 'a common approach' means.

On the one hand, the vast majority of MS have in place today elements of the common approach championed by the Directive. These include: laws and other measures in order to identify and protect CI; definitions of CI; co-operation with other MS and with relevant stakeholders at the national level; threat assessments in the energy and transport sector; and requirements for both OSPs and SLOs. In approximately half of the MS, these elements have been put in place or improved following the adoption of the Directive, and can be considered to some extent positive results of the Directive (see Section 6.3.1). As described in Section 5, all MS have transposed the Directive in their national legislation – albeit using different approaches. In this respect, the MS have all taken steps to protect ECI, contributing to the common approach advocated by the Directive.

On the other hand, when looking at these elements more closely, significant variations across MS remain, particularly concerning the definition of CI (*Finding 1*), in the attitude towards risk and criteria used to determine whether an infrastructure is critical (*Finding* 16, *Finding 9*), and in the roles and competences of stakeholders involved in CIP (*Finding 25*, *Finding 21*). The feedback from stakeholders consulted as part of the Evaluation supports these findings. For instance, only half of PoCs and representatives from other ministries considered that the Directive resulted in a common and agreed-upon procedure for the identification and designation of ECI,[115] or a common approach to the assessment of the need to improve the protection of ECI.[116] Similarly, operators highlighted the current variety of approaches across MS, pointing to the limited harmonising effects of the Directive.[117] The PC only provided further confirmation of the variety of approaches being pursued by the MS,[118] while highlighting the outstanding need for a common level of protection of CI. Seen from this perspective, the objectives of the Directive are still relevant.

Therefore, the assessment of the relevance of the objectives of the Directive cannot be conclusive and requires a clarification of the meaning of 'common approach' which currently appears to be subject to different interpretations:

- PoCs tend to interpret the common approach as a **common strategy** defined at high level, and the Directive as a strategic document. They stress that the Directive aims to achieve a common outcome across MS (i.e. a high level of protection) rather than at achieving the

[113] CORDIS. (2018). A pan European framework for strengthening Critical Infrastructure resilience to climate change. Interview: 4 EC DGs and Agencies; MT PoC.
[114] PC: 88% (N=56) of the respondents consider the provisions of the Directive to be relevant to some, fairly large and large extent to ensure a common level of protection of CI across the EU in the energy sector. This share goes to 75% (N=42) of respondents in the transport sector.
[115] Survey: 50% (N=11) of PoCs and 47% (N=7) of representatives from Other authorities considered that the Directive resulted in a common procedure for the identification and designation of ECI to a high or to a very high extent.
[116] Survey: 45% (N=10) of PoCs and 44% (N=7) of representatives from Other authorities considered that the Directive resulted in a common approach to the task of assessing the need to improve the protection of ECI to a high or to a very high extent. Restricting the same to MS with ECI only, the percentages are even lower: 60% (N=6) of PoCs and 44% (N=7) of representatives from Other authorities.
[117] Workshop: CI owners/operators. Given the impossibility to identify ECI and ECI operators, this finding should be considered in relation to the CIP framework in general.
[118] PC: 45% (N=28) of respondents agree and strongly agree that the Directive has contributed to achieving common levels of protection for CI in the EU, 34% (N=21) of respondents disagree and strongly disagree.

implementation of common procedures.[119] This is because procedures build on administrative contexts and CIP frameworks that differ across MS, but also because the need for operational coordination is stronger between neighbouring countries whose respective CI are more relevant in terms of the effects of a potential disruption/disruption.[120] If this is the chosen interpretation, the fact that almost all MS have in place the elements of the CIP framework should be seen as a sign that a common approach has indeed been achieved and that the current objective is one of maintaining (and improving on) it;

- Operators tend to interpret the common approach in a more **operational sense** insofar as it relates to common definitions, methodologies and common minimum standards on risk analysis and risk management requirements in the OSP, as well as of governance systems.[121] This marks a significant change when compared to the security practices that operators were applying before the Directive. It also ensures a more level playing field in applying security measures, eliminates possible competitive advantages of operators working in less regulated MS, and facilitates operations in different MS. If this is the chosen interpretation, CIP approaches still differ across MS, making the objectives of the Directive still relevant and encouraging a greater level of detail in some definitions and provisions contained in the Directive (such as the OSP, the SLO, risk analysis, and cross-sector dependencies) and further guidance on how to implement them.

The clarification of the desired level of harmonisation appears therefore to be a needed step for any future decision in the European CIP policy area and requires an in-depth analysis of national CIP frameworks and an assessment of the current level of protection of CI and ECI that goes beyond publicly available information.

6.1.1.2 Relevance of the definitions

EQ 1.1 To what extent are the definitions set out in the Directive still deemed to be suitable and fit for purpose? EQ 1.1.a. To what extent is the notion of critical infrastructure/European critical infrastructure as defined in the Directive appropriate in light of contextual changes and the needs of stakeholders[122]*?*

The Directive helps to create the basis for a common framework for CIP by providing definitions. **However, these definitions are generic and do not cover all key elements**.[123] On the one hand, the vagueness of the definitions makes them easily adaptable by stakeholders to their national contexts and to wider developments or new emerging threats in future. On the other hand, their vagueness also limits the ability of MS and CI owners/operators to deliver a common approach in the practical implementation of the Directive (*Finding 1*, *Finding 5*). Annex I.7.1.1 includes a detailed assessment of the relevance of each definition, the main findings of which are presented here:

- The **definition of 'CI'** is considered appropriate and helpful in the identification of national CI. However, the definition itself includes some terms that would benefit from further articulation, namely '*assets*' and '*systems*'. Doing so would serve to minimise the risk for differences in how MS interpret these terms, especially in the context of translation into different national languages. Moreover, '*vital functions'* could be more clearly defined (see also Section 5.2.1),[124] and further guidance on what is deemed to be '*critical*' would be helpful to MS;

[119] Workshop: PoCs. Interview: 1 EU CI owners/operators.
[120] Case study: 2 MS.
[121] Workshop: CI owners/operators. Representatives from the railway sector make an exception, as they view the Directive as a strategic document. While they do not see the need to make the Directive more operational in general, the expressed the need for minimum coordination at the EU level on a common methodology for assessing the risks. Views expressed by the Community of European Railway and Infrastructure Companies (CER)'s answers to Open Public Consultation on Improving passenger railway security (February 2018).
[122] The analysis of the relevance of the Directive to contextual changes and stakeholders' needs is presented in Section 6.1.2.2 and 6.1.2.1. To avoid duplication, this Section focuses on the relevance of the definitions in general.
[123] Survey: 61% (N=14) of PoCs consider that the definitions included in the Directive either do not cover all key elements needed to identify and protect CI, or only do this to a low extent. The share of Other ministries and CI operators sharing this view is lower, respectively 27% (N=4) and 23% (N=10).
[124] The terms 'vital functions' are not further explained in the JRC non-binding guidelines.

- The **definition of 'ECI'** is somewhat relevant. While it is helpful in identifying ECI, the term suffers from some limitations. Specifically, the definition of ECI specifies that the cross-cutting criteria should consider effects resulting from 'cross-sector dependencies on other types of infrastructures'. These cross-sectoral interdependencies include the dependence of a CI on another CI in a different sector, or on the services delivered in the context of other sectors (e.g. ICT or financial services, or the reliance of hospitals, banks and other workplaces on electricity supply). This means that a single attack could result in a 'domino effect' where an attack on one CI impacts other sectors and MS. However, interdependencies – and the cascading effects across different sectors – are not further addressed or operationalised in the context of the three cross-cutting criteria (casualties, economic effects, and public effects) that MS should use in order to assess the impact of an attack targeting CI.[125] Although there is a sizeable literature on methodologies for use in assessing interdependencies among CI, there is no single approach that is widely accepted and used by security actors.[126] This explains the view of many stakeholders that the current definition lacks a perspective on networks and interdependencies. Moreover, the ECI definition focuses on 'CI located in MS', meaning that it does not capture CI that have an inherently pan-EU dimension, but are located in multiple MS, such as the Galileo ground infrastructure, are space-based, or that offer a service on an EU-wide level, (e.g. the European electricity transmission grid, the gas transmission network, Eurocontrol, and Galileo, all of which were the focus of four pilot projects launched by the Commission as part of its new approach to EPCIP in 2013);[127]
- **The definitions of 'protection' and 'risk analysis'** are no longer suitable as they lack clarity and omit important details. Specifically, the '*protection'* definition does not explain how protection could be implemented on the field, nor does it incorporate the idea of critical infrastructure resilience (discussed in more detail in Box 3), which has become a central concept in the context of CIP in recent years. Furthermore, the relevance of 'protection' is further challenged by the absence from the scope of the Directive a crisis management plan to respond to incidents. Finally, the '*risk analysis*' definition lacks detail as to how such exercises should be carried out.

Box 3 – The relationship between protection and resilience

Resilience and **protection** have emerged as two concepts that are central to CIP. However, there are diverging views regarding the definitions of these terms and their relationship to one another.

According to one interpretation, CI resilience can be broadly defined as 'the ability to reduce the magnitude and/or duration of a disruptive event'.[128] However, there is no commonly agreed definition of resilience in the context of critical infrastructure. Rather, there exist a number of different definitions that vary in terms of their components, attributes, capacities and parameters.[129] On the one hand, some of the literature indicates that **'resilience' is understood as a separate concept from that of 'protection'** and more closely related to the functioning of a system than to the infrastructure.[130] Meanwhile, on the other hand and as discussed in Section 6.2.1, some of the literature states that **resilience (along with risk preparedness) is often seen as a more mature concept that in fact encompasses protection.** This is because the idea that a CI can be fully protected has become obsolete. Rather, it is argued that the protection of CI is subordinate to the maintenance of the CI's functionality, especially when they are subject

[125] Ramboll. (2012). Study into the potential impacts of options amending council Directive 2008/114/EC. Van Asselt, M. B. A., Vos, E., & Wildhaber, I. (2015). Some Reflections on EU Governance of Critical Infrastructure Risks. European Journal of Risk Regulation, 6(2), 185–190.

[126] Casalicchio, E., & Galli, E. (2008). Metrics for Quantifying Interdependencies. In Critical Infrastructure Protection II (ICCIP, Vol. 290, pp. 215–227). Springer. Ouyang, M. (2014). Review on modelling and simulation of interdependent critical infrastructure systems. Reliability Engineering & System Safety, 121, 43–60.

[127] Due to the confidentiality of information, it was not possible to gather specific data on the implementation of the pilot projects. Booz & Company GmbH. (2012). Study to support the preparation of the review of the Council Directive 2008/114/EC on the "identification and designation of European critical infrastructures (ECI) and the assessment of the need to improve their protection".

[128] Rehak, D., & Hromada, M. (2018). Failures in a Critical Infrastructure System. In System of System Failures (pp. 75–93). IntechOpen.

[129] Ibidem. Workshop: PoCs.

[130] Bach, C., Bouchon, S., Fekete, A., Birkmann, J., & Serre, D. (2013). Adding value to critical infrastructure research and disaster risk management: the resilience concept. S.A.P.I.EN.S, 6(1), 1–12. Lazari, A. (2014). European Critical Infrastructure Protection. Springer. Rehak, D., & Hromada, M. (2018). Failures in a Critical Infrastructure System. In System of System Failures (pp. 75–93). IntechOpen. Interview: 2 EC DGs and Agencies, 1 Academia and think tanks consider protection and resilience are separated and complementary.

to disruptions. Seen from this perspective, there is no need to draw a clear-cut distinction between the terms; any CIP directive or other legislative/regulatory instrument should include resilience elements.[131] It is worth noting that recent EU policy developments point towards the closer integration of protection and resilience.[132] This is confirmed by the recent work done within the European Defence Agency (EDA) in line with the priority of the EU Global Strategy of strengthening the protection and resilience of the Union networks and critical infrastructure.[133] Specifically, an expert group was set up within EDA to explore options for protecting defence-related critical energy infrastructure. The focus was both on protection and resilience.[134]

Generally speaking, **there is no agreement in the literature on CI concerning the relationship between protection and resilience**. However, it is clear that the **concept of resilience has become increasingly important** in response to the changing threat landscape. Equally clear is the fact that **any links that exist between the service-centred approach advocated by, for instance, the NIS Directive, and the notion of protection as defined in the Directive are under-explored**. For these and other reasons, the relationship between resilience and protection should be made more explicit in order to avoid confusion and duplication.

Additional definitions provided by individual MS (*Finding 2*) may also be an indicator of a lack of clarity on the part of/potential gaps in the Directive. This was also noted in the 2012 evaluation report, which pointed out that the Directive does not define what "essential services" in fact are. For this reason, RO (as an example) opted to provide an ad hoc definition in its transposition legislation.[135]

EQ 1.1.b. To what extent does the definition of critical infrastructure provided in the Directive fit with the sectors that is applied to?

The generality of the CI definition set out in the Directive makes it broadly relevant to the sectors in scope, namely energy (electricity, oil, gas) and transport (road, rail, air, inland waterways, ocean and shipping and ports). Generally speaking, CI operators and representatives from sectoral ministries consider that the definitions in the Directive are relevant to the identification of CI and ECI, and that they include all key elements and capture the range of risks facing CI. However, the proportion of those that consider the definition only moderately comprehensive (in terms of including all key elements to identify and protect CI) is particularly large.[136]

There are differences by sector, with transport operators being less convinced of the relevance of the Directive's CI definition. Specifically, operators in the transport sector are less likely than operators in the energy sector to find that the definitions in the Directive help in the process of identifying and protecting designated CI.[137] This may be due to the reference in

[131] Pursiainen, C. (2018). Critical infrastructure resilience: A Nordic model in the making? International Journal of Disaster Risk Reduction, 27, 632–641. The author noted that "in the resilience definition [used by the UNISDR i.e. the ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions] the verb 'resist' implies that protective measures are included. Resilience can thus be understood as an umbrella concept that also covers CIP". Interview: 6 EC DGs and Agencies; Workshop: PoCs and CI owners/operators. During the Workshop, energy operators stressed that protection is a limited concept, as the energy system has a built-in redundancy so that even if an asset of the system is damaged, the service can be delivered nonetheless.

[132] In the Joint Communication on hybrid threats, in the section entitled 'Protecting critical infrastructure', the proposed Action is "identify common tools, including indicators, with a view to improve protection and resilience of critical infrastructure against hybrid threats in relevant sectors" (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2016). The risk assessment approach for CIP proposed by the JRC includes resilience: Critical Infrastructures & Systems Risk and Resilience Assessment Methodology.

[133] Council of the European Union. (2016). Council Conclusions on implementing the EU Global Strategy in the area of Security and Defence. Foreign Affairs Council, Brussels.

[134] EDA. (2017). Protection of Critical Energy Infrastructure (PCEI). Conceptual Paper. Brussels.

[135] There is not sufficient data from interviews and desk research to formulate an evidence-based judgement on the relevance of the definition of 'sensitive CIP related information'.

[136] Survey: for CI owners/operators and Other ministries respectively, 81% (N=35) and 69% (N=11) consider that the definitions in the Directive are helpful to the identification of CI, 83% (N=35) and 87% (N=14) that definitions are helpful to the identification of ECI, 67% (N=28) and 67 (N=10) that the scope captures the range of risks facing CI, 77% (N=33) and 73% (N=11) that the definitions include all key elements to identify and protect CI to a moderate/high/very high extent.

[137] Survey: 54% (N=15) of CI owners/operators in the *energy* sector consider that the definitions in the Directive are

Step two of the ECI identification procedure (Annex III of the Directive) to the consideration of the availability of alternatives. In some cases, the lack of available alternatives has been interpreted as a necessary condition for the identification of CI. This might go some way in explaining why so few CI in the transport sector have been designated; many different means of transport can be counted as available 'alternatives'. In other words, this may have limited the relevance of the definitions to infrastructure in the transport sector, where it is easier to find alternatives than in the energy sector (*Finding 10*).[138]

6.1.1.3 Relevance of scope

EQ 1.2 To what extent do the scope, set of objectives, but also the formal means of implementation set out in the Directive correspond to the current and possible future threats facing critical infrastructure?

The Directive has mixed relevance regarding the current and possible future threats facing CI, which include terrorism, cyber-attacks from organised criminals and state actors, hybrid threats and insider infiltration. Annex I.7.3 summarises the threats to CI and analyses the relevance of the Directive to them.

As for the scope, there is no consensus among stakeholders on the relevance of the limited sectoral scope of the Directive. On the one hand, a small majority of stakeholders considers that the scope of the Directive is too narrow and hampers its relevance.[139] This is mainly due to increased interdependencies between CI in different sectors, especially in space and ICT, and related policy developments (most notably the NIS Directive). The text of the Directive itself acknowledged in 2008 the possibility of including other sectors in the future,[140] and highlighted that "effects resulting from cross-sector dependencies on other types of infrastructure"[141] should be taken into account when identifying ECI.

On the other hand, a minority of stakeholders consider that the scope of the Directive is appropriate.[142] A very small minority stated that the Directive should either cover the energy sector only, or the transport sector only.[143] While the sample size is small, it is possible to draw out the fact that while there is no consensus around whether to leave the sectoral scope as is, or to broaden it, the results clearly show that restricting the Directive to only the transport or the energy sectors is not acceptable to stakeholders.

Regardless of the policies and procedures in place at the level of individual CI, **a limited sectoral approach does not take into account the increasingly deep cross-sectoral interdependencies** (Section 6.1.1.2). These interdependencies can be both cyber-based (e.g. reliance on 'information transmitted through the information infrastructure') and logical (i.e. legal or regulatory),[144] but might also concern common modes of failures (i.e. a single event/incident

helpful to the identification of CI to a high/very high extent, vis-à-vis 30% (N=3) of CI owners/operators in the *transport* sector; and 36% (N=19) of CI owners/operators in the *energy* sector consider that the definitions include all key elements to high/very high extent, vis-à-vis 20% (N=2) CI owners/operators in the *transport* sector.

[138] Case study: 1 MS; Survey: 3 PoCs; Workshop: PoCs. Booz & Company GmbH. (2012). Study to support the preparation of the review of the Council Directive 2008/114/EC on the "identification and designation of European critical infrastructures (ECI) and the assessment of the need to improve their protection".

[139] Interview: 6 EC DGs and Agencies, 1 EU CI owners/operators, and 2 Academia and think tanks highlight the importance of expanding the coverage to additional sectors. Survey: 59% (N=13) of PoCs consider that the Directive should cover more sectors. 49% (N=20) of CI owners/operators consider that the Directive should cover more sectors. Case study: 2 MS (PoCs, other Ministries and CI owners/operators). PC: 37% (N=23) of respondents disagree and strongly disagree with the fact that the sectoral scope of the Directive is appropriate in light of the desired impact and 63% (N=37) of respondents think that the current scope of the Directive, limited to the energy and transport sectors, is not effective in protecting the most important CI in the EU.

[140] ECI Directive, preamble, paragraph 5.

[141] ECI Directive, Article 2(b).

[142] Survey: 32% (N=7) of PoCs and 46% (N=19) of CI owners/operators consider that the coverage of the Directive is adequate.

[143] Survey: 4.5% (N=1) of PoCs and 2.4% (N=1) of CI owners/operators consider that the coverage of the Directive should cover the energy sector only, and 4.5% (N=1) of PoCs and 2.4% (N=1) of CI owners/operators consider that the coverage of the Directive should cover the transport sector only.

[144] Montanari, L., & Querzoni, L. (2014). Critical Infrastructure Protection: Threats, Attacks and Countermeasures. TENACE.

affecting multiple CI).[145] As discussed in Section 6.1.1.2, these interdependencies can also affect CI or the services delivered across different sectors.[146]

Among the sectors excluded from the Directive, **the ICT and space sectors have become increasingly important over the past 10 years.** Infrastructure across Europe is increasingly managed electronically and through space-based systems. These and other related developments have increased the level of interdependency and interconnectivity between sectors.[147]

- Since 2008, CI have become increasingly reliant on the space sector, including space technology (e.g. satellites) in order to support their systems. The EU has over 30 satellites in orbit, and, as explained in the proposal for a new Space Programme, space technology plays an 'indispensable [role in] the daily lives of the public and [in] the EU's strategic interests'.[148] This space technology includes Galileo and the European Geostationary Navigation Overlay Service (EGNOS), which are used for geo-positioning and satellite navigation, and the EU space surveillance and tracking (SST). In the future, there will also be the Governmental Satellite Communications (GovSatcom) programme for satellite communications. However, the EU's space systems have a high level of vulnerability to cyber threats, due to the systems' reliance on ICT, which may impact on service provision[149] In 2013, Galileo, the EU's global navigation system, was identified as a potential vulnerability;[150]
- The energy sector is particularly reliant on ICT services, and on system control and data acquisition (SCADA) systems,[151] with SCADA managing and controlling the delivery of electric power.[152] In general, the ICT sector has become increasingly important with critical information infrastructures (CII). The importance of CII within the CIP has been widely recognised by the EU.[153] The 2016 European Union Global Strategy has further emphasised the importance of investment in digital capabilities in order to secure CI[154] due to the increased reliance in Europe on digital and computerised systems.[155] Other international organisations, such as the OECD, have also highlighted the importance of CII.[156]

[145] Nieuwenhuijs, A., Luiijf, E., & Klaver, M. (2008). Modeling Dependencies In Critical Infrastructures. In Critical Infrastructure Protection II (ICCIP, Vol. 290, pp. 205–213). Springer.
[146] Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. International Journal of Critical Infrastructure Protection, 8, 53–66. European Commission. (2013). Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union. SWD(2013) 32 final, Brussels.
[147] European Commission. (2005). Green Paper on a European Programme for Critical Infrastructure Protection. COM(2005) 576 final, Brussels. Peter, G. (2017, March 20). Critical infrastructures under daily attack. Horizon - The EU Research & Innovation Magazine. Interview feedback: 3 EC DGs and Agencies, and 2 Academia and think thanks.
[148] European Commission. (2018). Proposal for a Regulation of the European Parliament and of the Council establishing the space programme of the Union and the European Union Agency for the Space Programme. COM(2018) 447 final, Brussels.
[149] ESPI Workshop. (2018). Shared challenges, varying angles; developing a common understanding of cyber threats and tools for space operations.
[150] European Commission (2013). COMMISSION STAFF WORKING DOCUMENT on a new approach to the European Programme for Critical Infrastructure Protection. SWD (2013) 318 final, Brussels.
[151] OSCE. (2013). Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace.
[152] Lazari, A. (2014). European Critical Infrastructure Protection. Springer.
[153] ENISA (n.d.), 'Critical Information Infrastructure', Enisa.europa.eu, which states that 'identification of Critical information infrastructure is the first step in the process to secure and protect the availability of critical assets. European Commission. (2009). Communication on Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. COM(2009) 149 final, Brussels. European Commission. (2011). Communication on Achievements and next steps: towards global cyber-security. COM(2011) 163 final, Brussels. European Parliament. (2012). European Parliament Resolution of 12 June 2012 on Critical Information Infrastructure Protection: towards global cyber-security. P7_TA(2012)0237, Strasbourg.
[154] European Union. (2016a). A Global Strategy for the European Union's Foreign and Security Policy, European Union Global Strategy. Publications Office of the European Union, Luxembourg. Interview: 1 CI owners/operators.
[155] Castellon, N., & Frinking, E. (2015). Securing Critical Infrastructures in the Netherlands: Towards a National Testbed. The Hague Security Delta. OSCE. (2013). Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace. Interview feedback: 2 EC DGs and Agencies.
[156] Montanari, L., & Querzoni, L. (2014). Critical Infrastructure Protection: Threats, Attacks and Countermeasures. TENACE. The OECD describes CII as playing a large role in the interdependency of sectors, in terms of both services provided through it, and information and data held.

The limited sectoral scope of the Directive does not appear to be appropriate in light of national and EU policy developments occurring after 2008 and affecting a wider range of sectors. Out of the 11[157] MS that introduced new laws and measures when transposing the Directive, the overwhelming majority (ten)[158] took a more comprehensive approach, which included a broader range of sectors in their CIP framework than those two identified by the Directive. The majority of MS (six)[159] that had CIP measures in place before the Directive was adopted also currently pursue a broader approach (*Finding 4*). Meanwhile, at EU level, the 2016 NIS Directive on the security of network and information systems covers five additional sectors[160] in addition to the energy and transport sectors.

Stakeholders' views differ on what additional sectors could be included in the Directive.[161] The sectors that were most often mentioned in the course of the consultations were ICT,[162] water, finance and health.[163] Two CIP PoCs suggested aligning the scopes of the ECI and NIS Directives, respectively.

6.1.1.4 Relevance of formal means of implementation

EQ 1.2 To what extent do the scope, set of objectives, but also the formal means of implementation set out in the Directive correspond to the current and possible future threats facing critical infrastructure?

The 'means of implementation' foreseen by the Directive include: the identification and designation of ECI and the relevant criteria; the OSP; the SLO function; and reporting (Articles 3 to 10 of the Directive).

Regarding the **identification and designation process**, **the bilateral and/or multilateral discussion format initiated by one MS to designate ECI appears to not be fully relevant in identifying and designating ECI**. This format does not allow for the **involvement of the private sector**, which would be beneficial "given the very significant private sector involvement in overseeing and managing risks, business continuity planning and post-disaster recovery".[164] Several EC documents highlight the benefit of undertaking CIP initiatives in partnership with the private sector, including, for instance, CI owners/operators.[165] Examples of PPPs can be found in several MS (e.g. ES, PL, RO).[166] Meanwhile, some MS operators provide the first input to the identification process, flagging their infrastructure as potential CI (*Finding 5*).[167] In ES, for example, the National Centre for Critical Infrastructure Protection – the national body in charge of promoting, coordinating and supervising all CIP-related activities – involves public and private actors in the protection of identified NCI in activities, including the development of Sectoral

[157] BE, BG, ES, HU, IT, LU, MT, PL, RO, SI, SK.
[158] BE, BG, ES, HU, LU, MT, PL, RO, SI, SK.
[159] AT, CZ, DE, EE, FR, HR.
[160] Banking, financial market infrastructures, health sector, drinking water supply and distribution, digital infrastructure.
[161] Workshop: there was no conclusive vision from the workshop on the sectors that might be relevant to include in a possible revision of the Directive. Booz & Company GmbH. (2012). Study to support the preparation of the review of the Council Directive 2008/114/EC on the "identification and designation of European critical infrastructures (ECI) and the assessment of the need to improve their protection".
[162] PC: 67% (N=35) of respondents disagree and strongly disagree with the fact that the exclusion of the ICT sector from the scope of the Directive has not limited its impact.
[163] Among the stakeholders suggesting to widen the scope, the most spontaneously mentioned sectors were ICT/telecommunications (Survey: 10 PoCs and 8 CI owners/operators, Workshop: PoCs, Case study: 2 MS; Interview: 1 EC DGs and Agencies and 3 Academia and think tanks), water (Survey: 7 PoCs and 10 CI owners/operators, Interview: 1 EC DGs and Agencies), finance (Survey: 8 PoCs and 2 CI owners/operators, Workshop: PoCs, Case study: 1 MS. Interview: 1 EC DGs and Agencies, and 1 Academia and think tanks), health (Survey: 6 PoCs and 4 CI owners/operators, Workshop: PoCs, Interview: 1 EC DGs and Agencies and 1 Academia and think tanks), space and research (Survey: 2 PoCs each, Case study: 1 MS).
[164] ECI Directive, Preamble 8. Ramboll. (2012). Study into the potential impacts of options amending council Directive 2008/114/EC.
[165] CoESS. (2016). Critical infrastructure security and protection: the public-private opportunity. European Commission. (2013). Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union. SWD(2013) 32 final, Brussels. European Commission. (2017). Commission Staff Working Document Comprehensive Assessment of EU Security Policy. SWD(2017) 278 final Brussels. Interview: 1 Academia and think tanks.
[166] Workshop: CI owners/operators.
[167] Workshop: PoCs.

Strategic Plans. The Directive, however, does not seem to reflect these working relationships and sees MS as being the sole primary players involved in identifying and designing ECI.[168]

Moreover, **the identification and designation process relies too much on the initiative of MS, which may not necessarily have an interest in identifying and designating ECI**. MS differ in terms of the maturity of their respective CIP frameworks, institutional arrangements, and vulnerability to different kinds of threats. National specificities affect the inclination of MS to identify and designate ECI.

For instance, individual MS may not see any added value in the identification and designation of ECI. MS with mature CIP frameworks may deem that the protection of their NCI and the resilience of their systems is sufficient,[169] may consider the obligations deriving from the designation as being unclear, or may not be able to differentiate between existing CIP requirements and those included in the Directive.[170] In other cases, MS with established co-operation with neighbouring countries may consider that cross-border co-operation is already in place and/or may favour inter-governmental commitments over the procedures spelled out in the Directive.[171] Furthermore, even where deep cross-border co-operation is absent, the Directive does not necessarily take measures that would remove specific obstacles that might hamper any efforts to designate ECI (e.g. a lack of trust among MS, a lack of capability from the side of authorities in one MS,[172] the existence of different assessments in different MS as to the criticality of an infrastructure).[173] Some stakeholders have emphasised that a networked approach could more effectively promote co-operation between MS than the current, MS-centred approach.[174]

The criteria for identification and designation outlined in the Directive are broadly defined and can be interpreted in different ways by different MS.[175] Despite the limited availability of certain types of confidential information (*Finding 6*, *Finding 7*, *Finding 8*, *Finding 11*, *Finding 13*), there is evidence to suggest differences in how these criteria are interpreted (*Finding 9*). Some stakeholders consider these criteria to be of little relevance; despite being further articulated by the JRC in the form of non-binding guidelines, the criteria remain too broad to be practically useful to MS, and fail to account for interdependencies (Section 6.1.1.2).[176]

Finally, **some key terms in the identification and designation process are not explained, and this limits the overall relevance of the Directive to national authorities that do not know how to interpret the specific terms**. For instance, the identification procedure stipulates that the "availability of alternatives" should be taken into account for infrastructure "providing an essential service". However, it fails to specify what 'alternatives' and 'essential service' mean in this context. It is perhaps for this reason that when implementing the identification procedure, MS have signalled a lack of clarity as to whether they are allowed to identify alternatives that are operated outside the EU (*Finding 10*).[177] The lack of clarity around the notion of 'alternatives' has arguably hampered the ECI identification procedure, leading to a low level of candidate infrastructure as ECI.[178] As mentioned earlier, the reference to 'available alternatives' in Step two of the identification procedure (Annex III of the Directive) seems to have decreased the relevance of the Directive, but especially in the transport sector, where there is the assumption that CI in different sub-sectors can be considered alternatives to one another (i.e. if there is a disruption in the rail sub-sector, roads can be used as an alternative).[179] With regard to 'essential service', the

[168] Giannopoulos, G., & Schimmer, M. (2011). Memorandum on the results of the sixth Workshop on the Implementation and Application of the Directive. JRC.
[169] Workshop: PoCs; Case study: 1 MS (PoC).
[170] Workshop: PoCs, CI owners/operators.
[171] Case study: 2 MS.
[172] Case study: 1 MS (PoC).
[173] Workshop: PoCs.
[174] Giannopoulos, G., & Schimmer, M. (2011). Memorandum on the results of the sixth Workshop on the Implementation and Application of the Directive. JRC. Interviews: 4 EC DGs and Agencies.
[175] Lazari, A. (2014). European Critical Infrastructure Protection. Springer.
[176] Interview: 1 Academia and think tanks, 1 EC DGs and Agencies; Case study: 1 MS.
[177] Giannopoulos, G., & Schimmer, M. (2011). Memorandum on the results of the sixth Workshop on the Implementation and Application of the Directive. JRC.
[178] Lazari, A. (2014). European Critical Infrastructure Protection. Springer.
[179] Case study: 1 MS (CI owner/operator); Interview: 1 EC DGs and Agencies. Booz & Company GmbH. (2012). Study to support the preparation of the review of the Council Directive 2008/114/EC on the "identification and designation of European critical infrastructures (ECI) and the assessment of the need to improve their protection".

fact that the Directive does not provide a definition might partially explain why, as discussed in Section 6.2.2, MS face difficulties in reconciling the ECI Directive's requirements with those stemming from the NIS Directive, where 'essential service' is at its core.

The descriptions of the OSP and the SLO lack clarity, thus limiting their relevance, especially from an operational standpoint. For instance, while the Directive mentions that an OSP or 'equivalent measures' should be put in place and provides a general description of its content in the accompanying annex to the Directive (III), it does not describe in detail what is required of an OSP or what can be considered an equivalent measure. The OSP is in principle very useful,[180] but the lack of details in the definition of 'risk analysis' (Section 6.1.1.2) and the low level of detail of the content of the OSP makes it too vague to be operationally relevant.[181] This is noteworthy, given that CI operators in most MS already have in place a security plan that functions as an equivalent to the OSP called for in the Directive. In many instances, sectoral legislation may in fact impose stricter requirements than those imposed by the Directive.

Similarly, the Directive requires MS to assess whether a SLO has been designated for each ECI. However, a recent EC study points out that there is 'no specific indication […] provided to characterise [her/his] competences, roles and background'. In other words, the wording in the Directive ('or equivalent') to describe SLOs is ambiguous.[182] While in principle the SLO provision is useful,[183] its overall operational relevance appears limited, given that sufficient guidance in terms of implementation is lacking.

Regarding **reporting**, the biannual reports on risks, threats and vulnerabilities that are requested of MS by the EC meet neither operator nor MS needs in defining relevant protection measures at national level, nor do they enable the EC to generate an overview of the existing threats facing the MS (*Finding* 20). This illustrates the limited relevance of this provision in improving CIP across the MS. Moreover, the frequency of the reporting also appears not to be fully aligned with the changing nature of the threats/risks/vulnerabilities facing CI in Europe today and into the future.[184]

6.1.1.5 Obsolescence

EQ 1.5 Are there provisions contained in the Directive that might be considered obsolete?

None of the provisions in the Directive can be considered obsolete. However, as highlighted in the previous Sections, **there is agreement among stakeholders that the approach taken by the Directive should be updated.** More specifically:

- The **sectoral scope of the Directive is too narrow** and does not reflect wider contextual developments, particularly regarding increasing interconnectedness and interdependencies between sectors and possible 'domino effects' in the event of CI failure (Section 6.1.1.3);
- The **definitions are too general** and sometimes vague, limiting the relevance of the Directive in creating a common approach (Section 6.1.1.2); and
- The **concept of ECI and related protection measures has currently lost added value** compared to 2008. Some MS might not see an added value in designating their NCI as an ECI, as they may feel that national measures are sufficient.[185] In turn, this might disincentivise MS to initiate the ECI identification process (*Finding* 12).The recent development of EU legislation impacting on NCI, most notably the NIS Directive, further illustrates to which extent the ECI-focused approach of the Directive might be outdated.

[180] Survey: 86% (N=18) of PoC, 87% (N=13) of Other ministries, 91% (N=39) of CI owners/operators considered the OSP relevant to the protection of CI to a moderate, high or very high extent.
[181] Workshop: CI owners/operators (with the exception of railways operators).
[182] Setola, R. (2014). Security Liaison Officer Project - Final Report.
[183] Survey: 86% (N=18) of PoCs, 93% (N=14) of Other ministries, 84% (N=36) of CI owners/operators considered the SLO relevant to the protection of CI to a moderate, high or very high extent.
[184] Interview: 1 EU CI owners/operators.
[185] Workshop: PoCs.

6.1.2 Relevance of the Directive to stakeholders' needs, recent developments and EU priorities

6.1.2.1 Relevance to stakeholder needs

EQ 1.3 Is the Directive suitable to the needs/interests of the relevant industries and other stakeholders?

Generally speaking, the Directive is partially relevant to the needs of the main categories of stakeholders. Annex I.7.2 provides an overview of the needs of MS, the EC and CI owners/operators, and a detailed assessment of the extent to which the Directive addresses each stakeholder group. This Section presents the main findings from this assessment.

CI owners/operators

The Directive has sufficient flexibility to allow adaptation to changes in the wider context, given that procedures and definitions are described in a general way. It also provides an overarching framework for CIP, thereby supporting CI owners'/operators' efforts to protect transport and energy infrastructure, though not at a particularly granular level.[186] In general, CI owners/operators that responded to the survey found the provisions in the Directive relevant to the protection of CI. While respondents from the energy sector were far more positive about the provisions than their counterparts in the transport sector, respondents from both sectors found that the Directive's provisions were generally relevant (*Finding 14*).

There is evidence from a previous study that some CI owners/operators consider the OSP requirement in particular to be an 'additional measure' that may result in undesirable business pressures and economic costs.[187] However, none of the stakeholders consulted as part of this Evaluation raised such a view.

MS

The Directive is partially relevant to the overarching need of many MS. It is relevant with regards to ensuring that CIP is included in the national agendas. It does this by providing a definition of CI and requiring that the process of identification and designation of ECI should be repeated on a regular basis (Article 4(6)). Most national authorities consider the Directive relevant to CI protection, especially in its provisions concerning the OSP, the SLO, and the creation of CIP PoC group.

However, the Directive does not address the need on the part of some MS to coordinate with third countries on which their CI depend. Indeed, the Directive contains no provision concerning the exchange of information or co-operation with third countries. The recent involvement of third countries in CIP PoC meetings and the initiatives undertaken with third countries within the wider EPCIP context illustrate growing interest on the part of MS to liaise with third countries in order to exchange experiences.

EC

In addressing the relevance to the EC's needs, it is important to compare the current situation to that in 2008, when the Directive entered into force (see Section 2.3). With this in mind, it appears that **the Directive has to some extent addressed the need to tackle the different levels of protection for CI whose disruption or destruction could affect other MS, but also the need to clarify rights and obligations for stakeholders**. As discussed in more detail in Section 6.3.1 below, the Directive increased CIP awareness among policymakers at both the EU and MS levels, and offered MS an overarching framework and a relevant set of definitions. That being said, the analysis of the implementation state of play (Section 5) reveals considerable variance in terms of definitions (*Finding 1*), details regarding certain requirements (e.g. OSP, SLO) (*Finding 16*, *Finding 19*), and perceptions of risk (and, hence, the criteria and thresholds used in order to assess the significance of the impact of different risks). As a result of this inconsistent application of the Directive across MS, it is likely that there are differing levels of protection of both CI and ECI across MS.

[186] Workshop: PoCs.
[187] Lazari, A. (2014). European Critical Infrastructure Protection. Springer.

6.1.2.2 Relevance to recent developments

EQ 1.6 How well-adapted is the Directive to the various technological/scientific, economic, social, political and environmental advances that have occurred since it was passed?

The period since 2008 has seen a range of contextual changes as the result of technological/scientific, economic, social, policy/political and environmental shifts, all of which have implications as regards CIP. Some of these key developments, and the relevance of the Directive in relation to these changes, are summarised below and described in more detail in Annex I.7.4.

Technological developments have progressed apace in the last decade. Examples include the expansion of the Internet of Things (IoT),[188] artificial intelligence (AI),[189] and Next Generation Internet (NGI).[190] While the growing accessibility of technology has led to greater reliance on networked resources, these developments have also contributed to greater CI vulnerabilities to cyber threats. The Directive has **partial relevance** in relationship to these changes; the limited sectoral scope of the Directive limits its ability to address the cross-sectoral interdependencies that certain technological developments have and continue to generate.

Economic shifts in the last decade include the 2008 financial crisis and the 2010 European sovereign debt crisis, both of which have contributed to an underinvestment in CI. Another development is the rise of new forms of currencies such as cryptocurrencies, which in turn have led to a new form of threat, namely 'cryptojacking' (the unauthorised use of someone else's connected device/system to 'mine' cryptocurrencies. However, reports of CI falling victim to cryptojacking are thus far few in number. Therefore, the Directive remains **relevant** in light of these economic changes. This is supported by the majority of the survey respondents. While the Directive does not currently address economic developments, such as the increased prevalence of cryptocurrencies, the generality of the procedures and definitions provided by the Directive is such that CI owners/operators are able to adapt to wider changes to the economic environment.

Social changes in Europe since 2008 include increased urbanisation, leading to more dense concentrations of interconnected CI. As a result, CI failures risk affecting large numbers of people, especially where they have cascading effects. The use of social media and communications technologies both in Europe and globally has also increased since 2008. The Directive has **partial relevance** in light of social change, but especially as it relates to changes population pressures on urban areas. Given its limited sectoral scope, it is less relevant in other respects, such as social change brought about by new technologies.

Policy/political developments include continued and, more recently, renewed focus on CIP as part of the EU policy agenda. At the same time, CIP has increasingly become a component of MS national strategies and action plans. This has occurred in part as a result of the Directive (see Section 5). The Directive has **partial relevance** to these developments; while the Directive has helped to ensure that CIP is high on both EU- and national-level policy agendas, the procedures provided through the Directive are not fully adapted to recent policy change. In particular, the bilateral/multilateral meeting format as part of the ECI designation process in Article 4 does not account for third country involvement, or differences in CIP practices that could impact on MS.

Environmental changes have been a feature of the last decade and are predicted to continue into the future. Failure to tackle climate change and extreme weather events has been highlighted as a global risk by the World Economic Forum. These changes manifest themselves in the form of more frequent and extreme climate events, including heatwaves but also erratic weather (e.g. alternating droughts and thunderstorms, flooding, widespread fires, major snowfalls). These and other types of weather events can be highly disruptive to CI. The importance of securing CI against extreme weather events has become apparent since the adoption of the EU Strategy on Adaptation to Climate Change in 2013. The need for climate-resilient infrastructure was reinforced in the 2018 Evaluation of the EU Strategy on adaptation to climate change, where particular attention was paid to energy and transport infrastructure. As highlighted in the Evaluation of the EU Strategy, there

[188] IoT is the process of connecting everyday objects to the Internet so they can communicate with the users and between themselves.
[189] AI is a computer or robot's ability to process tasks to the same level or beyond the abilities of a human.
[190] NGI, otherwise known as the Internet of the future, is an initiative to ensure increase privacy, openness, and inclusion in an increasingly connected society.

is a need to guarantee the climate resilience of existing and future CI in order to ensure reliability of service provision and increased asset life. The Directive has **limited relevance** in the face of these changes. On the one hand, most of the survey respondents indicate that environmental changes have made the Directive more relevant. On the other hand, the Directive's provisions regarding ECI identification and designation do not appear to be fully adapted to the changing climatic context as they offer only limited criteria (the 'cross-cutting criteria' mentioned in Article 3) for use in assessing the significance of the effects of events, including ones related to climate change. Additionally, the OSP procedure described in Annex II of the Directive only focuses on security measures, as opposed to more general safety measures concerning ECI themselves.

6.1.2.3 Relevance to EU priorities

EQ 1.4 To what extent does the Directive contribute to stated EU priorities?

The EU continues to prioritise CIP. As such, the Directive continues to contribute to stated EU priorities. The protection of CI is a continued priority and is identified as such in key EU policy documents. These include the 2009 Stockholm Programme, which recognises the potential vulnerability of CI, and the importance of ensuring that CI are protected from attacks and resilient where they nevertheless succeed, as well as the EU Internal Security Strategy for the 2015-2020 period, which recognises the 'necessity to strengthen protection of critical infrastructures'.[191] CI resilience was also mentioned in the 2016 Joint Framework on countering hybrid threats a European Union document.

Moreover, the Directive remains a key element of the EU's counterterrorism strategy. The protection of CI remains of high importance as part of the EU's counter-terrorism strategy. For instance, the Directive was mentioned as one key element in the 'Protect' strand of the 2005 EU Counter-Terrorism Strategy.[192] The protection of CI against terrorist attacks was subsequently raised as a priority in the 2016 Global Strategy for the European Union's Foreign and Security Policy.[193] Additionally, the 2017 Comprehensive Assessment of EU Security Policy states that wider consideration of CI and how CI vulnerabilities can be reduced is necessary in the EU in general.[194]

However, **the EC adopted in 2013 a wider EPCIP approach, without making corresponding changes to the Directive**. Following the publication of the Communication from the EC on EPCIP in 2006, and the publication of the Directive in 2008, the EPCIP approach was updated in 2013 so as to emphasise interdependencies that exist between CI, industry and state actors.[195] This updated version of EPCIP also introduces the concept of 'resilience' as part of CI protection.[196] In 2017, the Eleventh progress report towards an effective and genuine Security Union declared the need to adapt EPCIP to new, emerging threats.[197] However, these developments – on resilience and new threats – are not reflected in the Directive, which has not been updated since 2008. In the context of the 2013 review, it was argued that it was too early to amend the Directive, seeing as only two years had passed since the transposition deadline at the national level; more time was needed in order to assess to which extent any improvements had been made at national level.[198] While waiting for more substantial policy interventions, the EC launched in 2013 four pilot projects as a way to test and develop new tools as part of the revamped EPCIP approach. In conclusion,

[191] Council of the European Union. (2015). Draft Council Conclusions on the Renewed European Union Internal Security Strategy. 2015-2020, Brussels.
[192] Council of the European Union. (2005). The European Union Counter-Terrorism Strategy. 14469/4/05, Brussels. European Commission. (2017). Commission Staff Working Document Comprehensive Assessment of EU Security Policy. SWD(2017) 278 final Brussels.
[193] European Union. (2016). A Global Strategy for the European Union's Foreign and Security Policy. European Union Global Strategy.
[194] European Commission. (2017). Commission Staff Working Document Comprehensive Assessment of EU Security Policy. SWD(2017) 278 final Brussels.
[195] European Commission. (2013). Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union. SWD(2013) 32 final, Brussels.
[196] European Commission (2013). COMMISSION STAFF WORKING DOCUMENT on a new approach to the European Programme for Critical Infrastructure Protection. SWD (2013) 318 final.
[197] European Commission. (2017). Communication Ninth progress report towards an effective and genuine Security Union. SWD(2017) 278 final.
[198] Interview: 1 EC DGs and Agencies. Booz & Company GmbH. (2012). Study to support the preparation of the review of the Council Directive 2008/114/EC on the "identification and designation of European critical infrastructures (ECI) and the assessment of the need to improve their protection".

while the Directive contributes to the continued prioritisation of CIP and counterterrorism at the EU level, it does not reflect the wider EPCIP approach adopted by the EC in 2013.

6.2 Coherence

The protection of CI has been the object of an increasing number of policy interventions at different levels (i.e. national, EU, and international) since 2008. In this view, the analysis of coherence between initiatives is key to laying the groundwork for future policy interventions in the CIP policy area.

For the assessment of the coherence, the Evaluation team considered the following criteria: i) absence of conflict/contradiction and overall consistency; ii) presence of complementarities; iii) absence of overlaps (especially those leading to duplication *at the level of national implementation)*; and iv) presence of coordination mechanisms that allow for different pieces of legislation to work in synergy.

This Section addresses the coherence of the Directive with other EU and international initiatives in the energy and transport sectors (Section 6.2.1), but also with relevant national initiatives (Section 6.2.2). The Section ends with an analysis of the coherence of the EU's CIP framework in relation to existing national frameworks as they pertain to sectors besides energy and transport (Section 6.2.3).

The list of the pieces of legislation and relevant policy documents that have been considered as part of this analysis has been initially compiled in agreement with the Commission, and has been integrated based on the results of the desk research and on the basis of suggestions provided by EC DGs during the consultative interviews. Each piece of legislation and policy document has been carefully reviewed by the Evaluation team, assessed against a number of elements (highlighted in **light blue** in the Sections below), and then compared with the Directive. Annex I.8 includes a detailed analysis of these documents, with the Sections below summarising the main findings.

6.2.1 Coherence of the Directive with other EU and international policy interventions

EQ 2.1 To what extent the Directive is coherent and complementary to other policy interventions with similar objectives at EU and international levels?

6.2.1.1 EU level

Legislation in the energy sector[199]

Overall, the ECI Directive and legislation in the energy sector[200] are somewhat coherent.[201] While they are consistent (i.e. non-contradictory), the ECI Directive partially overlaps with and is partially complementary to legislation in the sector. Table 6 summarises the Evaluation team's assessment of the overlaps and complementarity of the ECI Directive in relation to legislation in the energy sector.

Table 6 - Overlaps and complementarities between the ECI Directive and legislation in the energy sector

Elements	Assessment
Objectives	Overlap and complement
Object to protect	Overlap and complement
Gas and electricity	
Threat assessment/risk analysis	Overlap and complement
Risk management	Complement
Crisis management	Complement
Oil	

[199] In the coherence Section, the term 'sectoral legislation' is used to refer to a number of pieces of legislation.
[200] Some of the acts considered are the Gas Supply Regulation, the Oil Stocks Directive and the proposal for the Risk-preparedness in the electricity sector Regulation, for the complete list and details on the analysis see Annex I.8.3.1.
[201] PC: 34% (N=19) of respondents consider the Directive coherent with/complementary to existing measures aimed at enhancing CIP in the energy sector to a fairly large and large extent.

Elements	Assessment
Threat assessment/risk analysis	Complement
Risk management	Complement
Crisis management	Complement

Source: Authors' elaboration

The objectives of the ECI Directive are consistent with existing energy legislation. The sectoral legislation focuses mainly on resilience and security of supply/continuation of services so as to ensure sufficient supplies of gas, oil and electricity in the event of a crisis. It considers the *functioning* of gas and electricity systems, but also the availability of oil stocks, and aims at ensuring the *resilience* of the aforementioned systems. The ECI Directive focuses on the protection of specific CI, defined as assets or systems (or parts thereof). While this definition includes consideration of vital societal CI *functions*, the objective is to ensure that they are adequately protected, not that they remain functional.

The extent to which the objectives of the ECI Directive and energy legislation are complementary or overlap depends on how resilience and protection are interpreted. Indeed, as Section 6.1.1.2 demonstrated, disentangling the two concepts is not easy. Protection focuses on preventing a disaster from happening, while resilience is a matter of minimising the impact of disruptive incidents and guaranteeing continuity of service in the event that elements of the system are rendered inoperable or otherwise disabled. In this sense, the objectives of the sectoral pieces of legislation in scope can be considered complementary with the Directive and mutually reinforcing. Indeed, when systems/assets are well-protected, the likelihood of identifying the need for resilience legislation is arguably lower. However, achieving full protection is unlikely. This is a crucial point, as security of supply "depends on a chain of well-functioning infrastructure and networks".[202] Seen in this light, the objectives of resilience and protection may be overlapping, meaning that they entail similar measures in terms of implementation (see discussion on risk analysis and management below).

In terms of objects to protect, both the sectoral legislation and the ECI Directive cover systems (hence there is overlap), but the ECI Directive is also focused on specific assets, while the sectoral legislation covers these only to a limited extent and insofar as they are concerned by measures to ensure the security of supply (hence there is a possible complementarity). As mentioned elsewhere, the list of designated ECI is not public, making it impossible to assess the relative importance of the complementarity and overlap that is observed.[203] That being said, there is a general perception among stakeholders that the ECI Directive is more focused on assets than on systems,[204] and two interviewees reported that only some MS have designated the whole energy transmission system as an ECI.[205] This would appear to suggest the complementarity of the ECI Directive to the relevant sectoral legislation, but, again, this finding is made without knowledge as to which ECI have been designated.

In terms of specific obligations in *the gas* and *electricity sub-sectors*, **the ECI Directive overlaps with and complements sectoral legislation**. Meanwhile, **the ECI Directive is complementary to the relevant sectoral measures** in the *oil* sub-sector.

Legislation in the transport sector

The ECI Directive is partially coherent with existing transport legislation.[206] **While they are generally consistent with one another, there are several significant areas of overlap.** Transport legislation (specifically in the aviation and maritime sub-sectors) goes beyond the Directive, as it is broader in scope and the provisions are more detailed.

[202] Melchiorre, T. (2018). Recommendations on the importance of critical energy infrastructure (CEI) stakeholder engagement, coordination and understanding of responsibilities in order to improve security. NATO Energy Security Centre of Excellence.
[203] The fact that 88 out of 93 designated ECI are in the energy sector further highlight the relevance of this assessment.
[204] Interview: 3 EC DGs and Agencies; Workshop: PoCs; CI owners/operators. Case study: 1 MS. Given the unknown identity of ECI, this perception cannot be verified.
[205] Interview: 1 EC DGs and Agencies, Case study: 1 MS (CI owner/operator).
[206] PC: 36% (N=15) of respondents consider the Directive coherent with/complementary to existing measures aimed at enhancing CIP in the transport sector to a small extent or not at all.

Aviation

The ECI Directive overlaps to a great extent with existing aviation legislation, which is more detailed than the Directive. EU sectoral legislation in aviation was put in place in the wake of the 9/11 terrorist attacks, well before the introduction of the Directive.[207] This might explain the apparent limited awareness concerning the Directive among the relevant aviation sector stakeholders,[208] but also the finding that the Directive is considered redundant given existing legislation on aviation security. Table 7 summarises the assessment of the complementarity and overlap of the ECI Directive with aviation legislation.

Table 7 - Overlaps and complementarities between the ECI Directive and aviation legislation

Elements	Assessment
Objectives	Overlap
Object to protect	Overlap
Threat assessment/risk analysis	Overlap
Risk management	Overlap
Crisis management	Overlap

Source: Authors' elaboration

Maritime

The ECI Directive overlaps with maritime legislation. The latter is in general more detailed, pre-dates the ECI Directive and stems from the International Ship and Port Facility Security Code (ISPS Code), which was developed by the International Maritime Organisation in 2004. Table 8 summarises the assessment of the complementarity and overlap of the ECI Directive with maritime legislation.

Table 8 - Overlaps and complementarities between the ECI Directive and maritime legislation

Elements	Assessment
Objectives	Overlap
Object to protect	Overlap
Threat assessment/risk analysis	Overlap
Risk management	Overlap
Crisis management	Overlap

Source: Authors' elaboration

Rail

The rail sector is not yet covered by the EU *security* legislation.[209] The EC recently (2018) adopted an Action Plan to protect rail passengers and staff. There may be some overlap between the ECI Directive and certain future measures related to the Action Plan.[210]

At the EU level, there are several *safety* measures relevant to the rail sector that include requirements for risk analysis and risk management. At the operational level, the distinction between safety and security is not entirely clear-cut. Indeed, the "European railway industry uses no common definition of the word 'security'".[211] While in the academic literature, security is generally understood to relate specifically to malicious/wilful acts and safety strictly to (the prevention of) accidents,[212] this does not apply in the context of the ECI Directive. Here, a comprehensive approach to security is taken, which covers all types of hazards including natural,

[207] The EU has established common rules in the field of aviation security since 2002, when the Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security was adopted.
[208] Interview: 1 EC DGs and Agencies, 1 EU CI owners/operators (both relating to the aviation sector).
[209] In the past, the EC preferred to cover this sector with non-binding instruments, such as collecting good practices or funding research activities. See for instance, European Commission (2012), Commission Staff Working Document on Transport Security, SWD(2012) 143 final, Brussels.
[210] Currently there are no obligations on MS, as the document is not legally binding. However, the Action Plan invites MS to develop specific security measures.
[211] Steer Davies Gleave. (2016). Study on options for the security of European high-speed and international rail services.
[212] Albrechtsen, E. (2002). *A generic comparison of industrial safety and information security*. Norwegian University of Science and Technology, Trondheim. Ministry of Transport, Public works and Water Management of the Netherlands. (2010). The Railways: safety of transport, safety of work and safety of life. The Hague. Steer Davies Gleave. (2016). Study on options for the security of European high-speed and international rail services.

non-antagonistic threats. Moreover, as highlighted by one interviewee, the procedures to prevent and deal with a problem are often similar, regardless of whether it is a safety or security problem. As a consequence, the **obligations deriving from safety legislation in the rail sector may overlap with those spelled out in the ECI Directive in terms of risk analysis and risk management**. [213]

The fact that the Directive appears to be redundant in light of existing safety measures may be explained by some distinctive features of the rail sub-sector that make the task of distinguishing between security and safety measures difficult. For instance, the same rail networks, platforms and stations are used for international, national, regional and local service at the same time. The extent to which passengers use the service, often in 'turn-up-and-go' mode, is much higher than in other sub-sectors. This, according to rail operators, makes "a security-based distinction of the services and passengers unrealistic".[214]

Table 9 - Overlaps and complementarities between the ECI Directive and railway safety and security measures

Elements	Assessment
Objectives	Overlap
Object to protect	Complement
Threat assessment/risk analysis	Overlap
Risk management	Overlap
Crisis management	Overlap

Source: Authors' elaboration

The NIS Directive

The NIS Directive is a cross-sectoral security instrument that was adopted in 2016. Even though the NIS Directive is without prejudice to the ECI Directive,[215] strong relationships between the two exist.[216]

Generally speaking, the ECI Directive partially complements and partially overlaps with the NIS Directive.[217] Table 10 summarises the assessment of these overlaps and complementarities.

Table 10 - Overlaps and complementarities between the ECI Directive and the NIS Directive

Elements	Assessment
Objectives	Complement and overlap
Object to protect	Complement and overlap
Threat assessment/risk analysis	Overlap
Risk management	Overlap
Crisis management	Overlap

Source: Authors' elaboration

The ECI Directive both complements and overlaps with the NIS Directive in terms of objectives and object to protect. The objective of the ECI Directive is the protection of ECI, while the objective of the NIS Directive is to ensure the security of network and information systems. The ECI Directive defines ECI as assets or systems, while the NIS focuses only on a single type of system (i.e. network and information systems). Thus, the ECI Directive overlaps with the

[213] Steer Davies Gleave. (2016). Study on options for the security of European high-speed and international rail services. Interview: 1 EU CI owners/operators in the rail sector confirms that safety provisions cover all relevant security aspects; Workshop: CI owners/operators.
[214] CER. (2018). CER answers to the Consultation on improving security of rail passengers accompanying the document Commission Decision setting up the EU Rail Passenger Security Platform. Brussels. Interview: 1 EU CI owners/operators in the rail sector. Workshop: CI owners/operators.
[215] NIS Directive, Article 1(4).
[216] European Commission. (2013a). Commission Implementing Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009. Official Journal of the European Union. Interview: 8 EC DGs and Agencies and 3 EU CI owners/operators mention that there are potentially overlaps between the ECI and NIS Directives and their coherence should be further analysed.
[217] PC: 42% (N=14) of respondents consider the Directive coherent with/complementary to existing measures aimed at enhancing CIP in the land-based digital infrastructure to a small extent and not at all.

NIS Directive on the network and information systems, but complements it where it focuses on other types of systems and on assets.

With regard to scope, the ECI Directive overlaps with the NIS Directive, given that the energy and transport sectors both fall within the scope of both instruments. The NIS Directive goes beyond the ECI Directive as it encompasses five additional sectors.[218] Moreover, the NIS Directive operates mostly at the national level, and the identification of operators of essential services is primarily a national-oriented process (though it includes some trans-boundary elements).[219] On the contrary, the ECI Directive has a clear focus on trans-boundary externalities and implies an exercise aimed at strengthening infrastructures with a clear European dimension (ECI). In this sense, the NIS Directive has a wider scope than the ECI Directive and covers also national CI.

The ECI Directive imposes obligations on operators of ECI, while the NIS Directive focuses on operators of essential services. For this reason, it may be the case that **ECI operators and operators of essential services**[220] **are one and the same when the service they provide relies on network and information systems**. The increasing interconnectedness between digital and physical infrastructures makes the distinction between ECI operators and operators of essential services increasingly blurred (see discussion on the relevance of the scope in Section 6.1.1.3). Modern CI in the energy sector, for instance, are controlled by and function thanks to vast network and information systems. Seen in this light, operators may meet the requirements of both Directives (though, again, it is impossible to know given the confidentiality of information regarding designated ECI).[221]

The requirements for risk analysis, risk management and crisis management imposed by the two Directives on operators of ECI and of essential services overlap.

As for the requirements imposed on national authorities, both the ECI and NIS Directives call for the appointment of contact points that should serve a liaison function, linking national authorities with authorities from other MS, and with the Co-operation Group in the case of the NIS Directive. The contact points should also ensure that operators comply with their obligations. In addition, the NIS Directive requires that the MS develop national strategies on the security of network and information systems, and designate a computer security incident response team (CSIRT), tasked with **risk analysis** and **crisis management**. **These latter requirements contained in the NIS Directive go beyond what is contained in the ECI Directive**.

Synergy between the ECI Directive and sectoral legislation

It has not been possible to conclusively determine whether the overlaps highlighted in the previous Sections resulted in duplications or instead were mutually reinforcing. Making such a determination requires insights into how EU requirements have been implemented at the national level, something which goes beyond the scope of the Evaluation at hand. However, as discussed later in Section 6.2.2, national authorities and operators consulted as part of the Evaluation have expressed that when there is overlap between the requirements of the ECI Directive and sectoral legislation, it does not create major difficulties. This is probably due to the fact that national authorities have taken steps to ensure that the ECI Directive and sectoral legislation are coherent and that no duplication of obligations is generated concerning implementation at national level.[222] This is arguably made possible by the fact that the obligations contained in the ECI Directive are described in general terms, making them easily adaptable to different national contexts (Section 6.1.1.4).

[218] The NIS covers: banking, financial market infrastructures, health sector, drinking water supply and distribution, digital infrastructure.
[219] For instance, before the identification of operators of essential services, MS shall consult each other if an entity provides an essential service for the maintenance of critical societal and/or economic activities in more than one MS, (Article 5(4)) of the NIS Directive. Trans-boundary effects are also taken into account in co-operation between MS.
[220] "Services essential for the maintenance of critical societal and/or economic activities, dependent on network and information system, and for which an incident would have significant disruptive effects" (Article 5(2) of the NIS Directive). The ECI Directives mentions 'essential services' only in relation to the 'public effect criterion' (Article 3(2c) and step 2 of the identification process (Annex III of the Directive).
[221] Interview: 2 EU CI owners/operators.
[222] Workshop: PoCs.

There are potential synergies between sectoral legislation and the ECI Directive. Indications of as much are especially evident where overlaps exist. This is particularly true in the case of **risk analysis** (e.g. the prospects for adopting common methodologies and sharing risk and threat analyses) and **risk and crisis management**. While these obligations are described at a very general level in the ECI Directive, relevant sectoral measures provide more detail.

However, the Directive explores these **synergies only to a limited extent.** Indeed, the Directive does not define clear roles and responsibilities for sectoral authorities and mechanisms to coordinate CIP sectoral activities at either the national or the EU level. Moreover, it is worth noting that the JRC developed non-binding guidelines to support the MS in implementing the Directive refer to sectoral legislation to a very limited extent.[223]

At the *national level*, the extent of co-operation between PoCs and sectoral authorities (and hence synergy between the requirements of the Directive and that of sectoral legislation) is dependent on organisational structures in each MS (see Section 5.8).[224] At the *EU level*, meetings and information exchange between DGs responsible for the different sectoral legislation tend to take place on an ad hoc basis; there is no formalised co-operation structure.[225] Similarly, both European operators' associations and national/multinational CI operators are not directly consulted on the implementation of the Directive.[226] Moreover, CIP PoCs do not always represent sectoral authorities (*Finding 21*, *Finding 22*), and their involvement and familiarity with sectoral legislation seems to be generally limited.[227] At the same time, the ECI Directive does not foresee or provide allowances for variable or sector-specific formats in the context of the CIP PoC meeting format. This is in contrast to the Co-operation Group created through the NIS Directive.[228]

6.2.1.2 International level

At the international level, there is no comprehensive policy on CIP. **There are, however, international standards and initiatives that apply to CI and that are generally coherent with the ECI Directive**.

6.2.2 Coherence of the Directive with national policy interventions

EQ 2.2 To what extent the Directive is coherent and complementary to other policy interventions with similar objectives at MS level?

National policy interventions stemming from EU sectoral legislation in the energy and transport sectors

The overlap between the requirements of the ECI Directive and those of other pieces of sectoral EU legislation does not appear to create major difficulties at the national level. When considering the implementation of EU legislation in the energy and transport sectors at the national level, the overlaps (especially in relation to risk analysis/threat assessments and risk management) (highlighted in Section 6.2.1.1) is confirmed by most of the PoCs.[229] However, this

[223] In Annex 2 presenting a non-exhaustive list of references for equivalent measures to the OSP and SLO.
[224] In Germany the Constitution imposes a strict division of policy competence per sector, and that sectoral authorities are fully in charge of CIP in their relevant sector. PoC is not directly involved in ECI procedures, although there is a semi-formal co-operation with sectoral authorities. Similarly, the DK, SK, SE PoC pointed to the fact that sectoral authorities are the primary responsible for the implementation of the ECI Directive in their relevant sector, with limited involvement of the PoC.
[225] There are examples of sectoral and cross-sectoral fora of exchange of information such as the European Reference Network for Critical Infrastructure Protection (ERNCIP) which aims to link together existing European laboratories and facilities, in order to carry out critical infrastructure-related security experiments and test new technology, or the Thematic Network on Critical Infrastructure Protection (TNCEIP), an initiative of DG Ener, made up of European owners and operators of energy infrastructure in the electricity, the gas and the oil sectors
[226] Interview: 1 EU CI owners/operators; Case study: 1 MS.
[227] The affiliation of PoCs to different types of institutions suggests that they might not have specific sectoral expertise. This has been confirmed during the Workshop with CIP PoCs in November 2018, where limited feedback was collected in relation to specific sectoral aspects (e.g. risk assessment criteria, thresholds).
[228] Article 11 of the NIS Directive. Interview: 1 EC DGs and Agencies stressed the importance of the 'variable geometry' format of the Coordination group, which, depending on the topic to be discussed, allows the relevant expertise to be involved. Case study: 1 MS (authorities pointed at the fact that the Directive did not facilitate co-operation and exchange of information across MS sectoral authorities).
[229] Survey: 71% (N=12) of PoCs found that the ECI Directive overlaps with existing EU legislation to a moderate or high extent with obligations created by other relevant EU legislation.

overlap does not appear to pose problems in terms of implementation, be it on the part of authorities (PoCs and sectoral ministries) or operators.[230] This finding is well supported as it relates to the energy sector (*Finding 14*).[231] On the other hand, the limited number of ECI (five) in the transport sector limits the likelihood of duplication or inconsistencies in those MS that are concerned.

Overlaps might bring potential inconsistencies or duplication insofar as i) the requirements to be met are detailed, and, when this is the case, ii) there is limited/no coordination among the relevant stakeholders that are either charged with overseeing their implementation or that are subject to the requirements themselves.

Seen in this light, **the absence of any significant operational difficulties reported by stakeholders vis-à-vis existing overlaps may be explained by: i) the generality of the obligations deriving from the ECI Directive, and ii) the nature of the coordination practices implemented at national level**.

As for the generality of the obligations, the lack of detail of the Directive (previously highlighted in Section 6.1.1.2) has allowed national authorities to implement practices that are coherent with existing national legislation. As for the nature of the coordination practices at national level, evidence shows that national authorities systematically organise meetings and consultation activities in order to facilitate co-operation between the stakeholders involved in the implementation of different but related policy measures (see Box 4).

Box 4 – Examples of coordination practices at the national level

In **Poland**, forums to facilitate the exchange of information are organised at the national, sectoral and regional level, and involve law enforcement authorities, operators and other stakeholders. The purpose of these forums is to identify key problems in the CIP sector and to develop solutions.[232] In addition, a regular exchange exists between CI operators and intelligence services.[233]

In **Slovakia**, sectoral authorities have regular exchanges with operators to discuss issues that operators may encounter, as well as suggestions as to how to improve CIP. The outcome of these exchanges feeds into regular meetings between sectoral authorities, the PoC and other security authorities. Here, potential amendments to existing national-level CIP legislation are discussed.[234]

In **Spain**, co-operation between relevant national stakeholders is facilitated by the existence of the National Centre for Critical Infrastructure Protection (CNPIC) within the Ministry of Interior. The CNPIC is charged with promoting, coordinating and supervising all CIP-related activities in Spain. The centre is also responsible for the implementation of the NIS Directive, and involves all the relevant stakeholders according to their respective fields of competence.[235] The centre promotes a security model based on mutual trust and PPPs. It covers multiple sectors, and organises national coordination groups around relevant sub-sectors, with meetings to share information, needs, threats and good practices. It also generates newsletters.[236] Other instruments exist at national level to foster co-operation. These include working groups that are organised regularly (approximately every two months) and involve experts from different ministries in order to set sectoral plans and avoid duplication of work.[237] Co-operation is also facilitated through the Interdepartmental Working Group for CIP within the CNPIC, which elaborates specific Sectoral Strategic Plans (PES) with the participation of CI operators.[238]

In **Malta**, Sectoral Fora made up of the SLOs in the designated critical sectors are set up and meet on a regular basis to discuss sectoral issues and interdependencies arising between different sectoral CI. These

[230] Survey: 89% (N=16) of PoCs, 89% (N=8) of representatives from Other ministries, 86% of CI owners/operators reported that they have not experienced any difficulties in applying the rules/procedures called for in different pieces of EU legislation. Workshop: PoCs, CI owners/operators.
[231] Survey: in the energy sector, 100% (N=5) representatives from Other ministries and 89% (N=17) of CI owners/operators reported that they have not experienced difficulties, while in the transport sectors the shares are respectively 75% (N=3) and 72% (N=8).
[232] The National Critical Infrastructure Protection Programme 2015.
[233] Workshop: PoCs and CI owners/operators.
[234] Case study: 1 MS (PoC).
[235] Case study: 1 MS (PoC).
[236] Workshop: PoCs and CI owners/operators.
[237] Case study: 1 MS (PoC and other Ministry).
[238] Sectoral Strategic Plans identify the essential services in all sectors, their general functioning, the system vulnerabilities, and the potential consequences of their unavailability.

Fora also aid in facilitating collaboration and co-operation between SLOs ahead of possible crisis/emergency situations. Cross-sectoral issues that are raised within a specific Sectoral Forum are addressed in Cross-Sectoral Fora meetings. The Maltese CIP Directorate is authorised to intervene in the event of conflict between CI and/or critical sectors arises.[239]

There is consensus among the PoCs that the ECI Directive overlaps to some extent with the NIS Directive. This confirms the findings presented above concerning the comparative analysis of the legal texts. **However, it is too soon to assess the effects of these overlaps.** The NIS Directive is the piece of legislation that was cited most frequently by survey respondents when asked about other EU legislation that overlap with the ECI Directive.[240] Interestingly, this view is not shared by CI owners/operators, most of whom find no or only limited overlap.[241] This divergence is probably due to the fact that the transposition deadline of the NIS Directive (9 May 2018) has only recently expired. Before operators can be required to comply with the obligations contained in the Directive, authorities have still to identify who in fact these operators of essential services are. Another possible explanation relates to the fact that there are few ECI, most of them located in a small number of MS (*Finding 15*) and in the energy sector (*Finding 14*). Box 6 illustrates the overlaps of the ECI Directive with the NIS Directive at the national level.

Box 5 – The potential consequences at national level of the overlap between the ECI Directive and the NIS Directive

As highlighted in Section 6.2.1.1, there is potential overlap between the ECI Directive and the NIS Directive that may result in duplications of obligations on the part of operators. While it is not possible to systematically assess to which extent this is the case (as comparative data are not available yet given the ongoing transposition analysis),[242] data from the survey and field research as part of the case studies suggests that the transposition of the NIS Directive at national level might result in three different situations, namely:

- **The creation of parallel frameworks** tackling the same issue, but with different authorities involved. These risks creating incoherence and a situation where operators must deal with multiple interlocutors at national level;
- **The development of a comprehensive and inclusive framework** where the NIS Directive trumps the ECI Directive. This would be the case where the NIS Directive is seen to be more in line with the national approach to CI (i.e. more oriented towards the protection of essential services).[243] In this case, the relevance of the ECI Directive is diminished;[244]
- **The adoption of complementary national measures**, in a MS context where the ECI and NIS Directives are seen as complementary insofar as they are focused on European and national critical infrastructures/essential services, or on physical and cyber threats, respectively.[245]

National policy interventions stemming from local initiatives in the energy and transport sectors

There is agreement among stakeholders on the overall coherence of the ECI Directive with national policy initiatives. More specifically, coherence has been pointed out in relation to:

- The **provisions** of the Directive that do not overlap, or only overlap to a limited extent with existing national-level legislation and/or measures.[246] The extent to which the Directive and national initiatives are contradictory/in conflict with one another is minimal;[247]

[239] The Malta Critical Infrastructure Protection Directorate website.
[240] Interview: 5 EU CI owners/operators and 5 EC DGs and Agencies; Survey: 9 out of 11 PoCs mentioned the NIS Directive when asked to list the relevant EU pieces of legislation overlapping with the ECI Directive. Moreover, when specifically asked about the NIS Directive, 78% (N=14) of PoCs and 75% of Other ministries (N=3) found overlap/duplication.
[241] Survey: 76% (N=16) of CI owners/operators found no overlap.
[242] Interview: 1 EC DGs and Agencies.
[243] MS that already mention the word 'service' in the definition of CI are: EE, FI, SE, ES.
[244] Workshop: PoCs; Case study: 1 MS (Other ministry).
[245] Workshop: PoCs; Case study: 1 MS (PoC, Other Ministry and CI owners/operators).
[246] Survey: 59% (N=13) of PoCs and 58% (N=7) of Other ministries answered that there is no or limited overlap.
[247] Survey: 81% (N=17) of PoCs, and 90% (N=9) of Other ministries answered that conflict/contradiction is not present or present to a limited extent.

- The **definitions** contained within the Directive, which are in most cases in line with those contained in national measures.[248] Where there are misalignments, these mainly concern the ECI definition contained in the Directive;[249]
- The **procedures** provided by the Directive, which are in most cases in line with national measures.[250] Few misalignments have been identified concerning the criteria to be used in determining impacts and in carrying out the threat assessment. This has been confirmed mainly by sectoral authorities,[251] who are often intimately involved in the implementation of sectoral legislation.[252]

On the question of **definitions**, some MS (but especially the Nordic countries) use a definition of CI that is more in line with that contained in the security of supply legislation insofar as it reflects attention to resilience (*Finding 1*) and emphasises essential services. Some countries (e.g. ES) integrated the protection-oriented provisions of the Directive into a more comprehensive approach which also includes resilience-oriented measures, while others (e.g. the Nordic countries) did not modify their existing approaches. While the Nordic stance not to make any adjustments was made in light of the view that their resilience-oriented measures already encompassed the protection-oriented measures required by the Directive, they did result in certain misalignments (see Box 6).

Box 6 – Consistency of the Nordic countries' CIP approach with the ECI Directive

The Nordic countries have adopted an approach to CI which is only partially consistent with the ECI Directive. In **Denmark**, national legislation does not consider the criticality of individual infrastructures. Instead, it focuses on the interconnected network of infrastructures (not necessarily confined to one sector) and the services that they are expected to provide in the interest of vital societal functions.[253] This focus on vital societal functions is also present in **Finland**, where the approach is based on a comprehensive security concept. The main emphasis of the Finnish approach is on the functioning of society and government in all circumstances, and not just on protecting its individual critical infrastructures against untoward events. Similarly, **Sweden** does not have a formal system for designating NCI. Rather, governmental stakeholders at all levels are tasked with identifying 'vital societal functions'. The focus of this work is on the functioning of the system as a whole and in relation to the provision of service. Generally speaking, the Nordic approach is more resilience-oriented and focused on critical or vital societal functions rather than on the individual CI that support them.[254]

Moreover, the general Nordic CIP approach does not consider criticality to be a binary concept (whereby a given infrastructure is deemed critical only if certain criteria are met). Instead, criticality is seen as existing to one degree or another and is used as a more general term, a view that does not appear to be fully aligned with the Directive's procedures regarding sectoral and cross-sectoral criteria.

While the Directive does refer to CI as 'systems', this term is vague (Section 6.1.1.2); the procedures provided by the Directive are perceived to relate more to assets.[255] The fact that the JRC's non-binding guidelines from 2008 do not account for interdependencies reinforces the perception that the Directive is indeed more oriented towards individual assets. Similarly, the sectoral approach contained in the Directive limits the possibility to designate CI from a societal function/service standpoint (which would inherently involve many interlinked CI across sectors). Moreover, the focus of the Directive is entirely on protection (rather than on resilience), and criticality is defined in terms of significance of the expected impact and protection measures are implemented only when the expected impact exceeds a certain quantitative

[248] Survey: the definitions of CI, ECI, risk analysis, sensitive critical infrastructure related information, owners/operators of ECI are considered to be in line with those in the national legislation to a high or very high extent by on average 75% of PoCs and 65% of Other ministries.
[249] Survey: 21% (N=4) of PoCs consider the definition of ECI in line with the definition in the national legislation/measures to no or to a low extent.
[250] Survey: criteria to determine the significance of the impact, the sectoral threat assessment, the regular risk analysis and co-operation with CI operators are considered to be in line with those in the national legislation to a high or very high extent by on average 65% of PoCs and 55% of Other ministries.
[251] Survey: 14% (N=3) of PoCs and 31% (N=4) of Other ministries answered that the criteria to determine the significance of the impact of a potential disruption are in line with the procedures in the national legislation/measures to no or to a low extent; 14% (N=3) of PoCs and 15% (N=2) of Other ministries consider that the sectoral threat assessment is in line with the procedures in the national legislation/measures to no or to a low extent.
[252] Workshop: PoCs.
[253] Case study: 1 MS.
[254] Pursiainen, C. (2018). Critical infrastructure resilience: A Nordic model in the making? *International Journal of Disaster Risk Reduction*, *27*, 632–641.
[255] Interview: 3 EC DGs and Agencies; Workshop: PoCs and CI owner/operators; Case study: 1 MS.

threshold. These differences serve to illustrate a certain misalignment between the Directive and the Nordic approach.

National policy interventions stemming from international initiatives in the energy and transport sectors

As for international initiatives implemented at national level, the available evidence is scant. Most authorities did not express any view on the coherence between the Directive and any such initiatives. Meanwhile, operators pointed to some overlap,[256] but especially in the aviation and maritime sub-sectors. In most cases, however, any such overlap was not shown to generate any conflict.[257] One exception could be the obligations arising in the NATO context,[258] where there have been discussions concerning the possible need to identify and designate CI in the energy sector.[259]

6.2.3 Coherence of the EU's legislative CIP framework with national CIP frameworks

EQ 2.3 To what extent are there synergies, inconsistencies, gaps, or overlaps between existing EU legislative framework and the respective legislative frameworks that exist at the MS level?

There are two different interpretations of the EU's legislative framework on CIP. Strictly speaking, the EU's CIP framework covers the energy and transport sectors through the ECI Directive. In practice, though, there are other pieces of EU legislation (either with a different sectoral scope or that are cross-sectoral) that address certain aspects of CIP. These can be considered to be part of a wider interpretation as to the contours of the EU's CIP legislative framework. This view is further strengthened by the importance given to cross-sectoral interdependencies in the EPCIP Communication, as part of the recent review of the Programme,[260] and in the academic literature on this topic. As discussed in Section 6.1.1.3, there are other sectors that are relevant to ECI in the energy and transport sectors. Furthermore, the disruption of CI in other sectors might have cross-border impacts (similarly to CI in the energy and transport), thus qualifying them as potential 'critical' sectors. When taking this into account, the EU's legislative framework on CIP might also include sector-specific initiatives in a range of sectors, including: space (reflected in the 2013 EPCIP review and the launch of the pilot project on Galileo); finance; health; and civil protection. It might also include various cross-sectoral initiatives like the Seveso III Directive and the NIS Directive.

The sectoral EU legislation not specific to energy and transport complements the ECI Directive (see Annex I.8.3). In the **space** sector, for instance, legislation is in general more developed and imposes stricter requirements than those contained in the ECI Directive. As per the Galileo Regulation, MS need to have in place measures for the protection of Galileo ground components. These measures must be at least equivalent to the measures required to protect ECI. In the **financial** sector, meanwhile, legislation is well-developed and mainly addresses cyber threats. In the **health** sector, legislation on cross-border threats is focused on resilience, preparedness and crisis management activities; water contamination legislation in particular imposes risk assessment and risk management requirements on MS.

However, feedback gathered through the PC does not appear to support the finding that other sectoral legislation outside the energy and transport sectors complements the ECI Directive. Indeed, around half of the PC respondents indicated that they consider the Directive coherent with/complementary to existing sectoral measures only to a small extent or not at all. However, when asked to clarify this view, the responses suggested that this view was more in relation to the Directive's scope, rather than its coherence with other measures.

There are overlaps and complementarities between the ECI Directive and cross-sectoral legislation. For instance, the Seveso III Directive requires operators to carry out regular

[256] Survey: 36% (N=8) of CI owners/operators see high of moderate overlap of the Directive with international initiatives.
[257] Survey: 85% (N=17) CI owners/operators do not see any conflict or only to a low extent.
[258] Case study: 2 MS (PoCs and Other Ministries).
[259] Melchiorre, T. (2018). Recommendations on the importance of critical energy infrastructure (CEI) stakeholder engagement, coordination and understanding of responsibilities in order to improve security. NATO Energy Security Centre of Excellence.
[260] European Commission. (2013). Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union. SWD(2013) 32 final, Brussels.

inspections of facilities/installations where dangerous substances are used, and to develop emergency plans. These obligations could duplicate the OSP obligation in the ECI Directive. The **Civil Protection Mechanism**, meanwhile, adopts a resilience- rather than protection-centred approach. However, this presupposes that CI will function in order to deliver a certain level of functionality. The Mechanism introduces risk analysis, risk management and crisis management practices, as well as a system of co-operation between MS, all of which could complement the requirements of the ECI Directive (or potentially result in overlaps).

Despite the potential for synergies generated by the existence of complementarity and overlaps between the ECI Directive and sectoral and cross-sectoral legislation, there is no evidence that these are exploited at EU level. Rather, measures to protect CI seem to run in parallel with the ECI Directive. For instance, in the space sector, the obligation concerning protection for the ground component of Galileo presupposes that it is considered to be NCI at national level. However, there is no provision at the EU level that ensures that this is the case, potentially generating a misalignment.

The limited integration between CIP measures at EU level does not seem to have negative effects on national CIP frameworks, where protection measures in different sectors coexist smoothly. While this might be to some extent also the result of the limited number of ECI, most national CIP frameworks have a wider sectoral scope than that of the ECI Directive (*Finding 4*) which served to facilitate cross-sectoral co-operation. Moreover, most of the PoCs that responded to the survey reported that the various procedures/roles in the different sectors are synergistic.[261] This finding is further supported by the fact that requirements applied to protect NCI in different sectors are in general at least equivalent to those set out by the ECI Directive,[262] thereby creating generally consistent national CIP frameworks.

The existence of coordination practices within MS has contributed to the overall coherence of national CIP frameworks and prevented duplication.[263] For instance, in SK, CI operators that have to draft emergency plans as per the Seveso III Directive are exempted from the requirement to develop an OSP per the ECI Directive. Other coordination practices are described in Box 4.

6.3 Effectiveness

This Section aims to assess: to what extent the Directive has achieved its objectives and any obstacles that have been encountered (Section 6.3.1); the contribution of the Directive to the identified results vis-à-vis external factors (Section 6.3.2)' and the spill-over effects of the Directive as regards enhancing the level of protection of national CI that have not been designated as ECI (Section 6.3.3).

6.3.1 The achievement of objectives

EQ 3.1 To what extent has the Directive achieved the stated objectives?

As illustrated in the intervention logic in Section 2.1, the **general objective** of the Directive was to improve the protection of transnational CI in the energy and transport sectors by i) establishing a procedure for the identification and designation of ECI, and ii) establishing a common approach to the assessment of the need to improve their protection (the Directive's **specific objectives**). Annex I.9 provides a detailed analysis of the contribution of all Directive provisions to these specific

[261] Survey: 84% (N=16) of PoCs consider that the EU and national CIP frameworks work in synergy in terms of procedures, and definition of roles.

[262] Workshop: PoCs (All ECI are in principle NCI, with the same designation process (e.g. for the power plants) and level of protection). Case study: 3 MS (PoCs and CI owners/operators) underline that there is no difference in the level of protection between NCI and ECI. Moreover, based on the information included in the Implementation tables (see Annex II), in some countries (AT, BG, CZ, ES, HR, HU, RO, SK) the rules applied for the OSP to ECI (in the energy and transport sectors) are common to those for NCI, both in the same and other sectors (e.g. health, finance, ICT, etc.), and are covered by the same legislation. It was not possible to verify to what extent requirements are common to all sectors as OSP are not publicly available.

[263] Survey: in the event the EU policy and national framework do not work in synergy, MS take measures to minimise the extent of overlap according to 35% (N=7) of PoCs and 25% (N=3) of Other ministries. There have been measures to strengthen co-operation within the MS according to 40% (N=8) of PoCs and 42% (N=5) of Other ministries. Measures to streamline procedures were put in place according to 10% (N=2) of PoCs and 25% (N=3) of Other ministries.

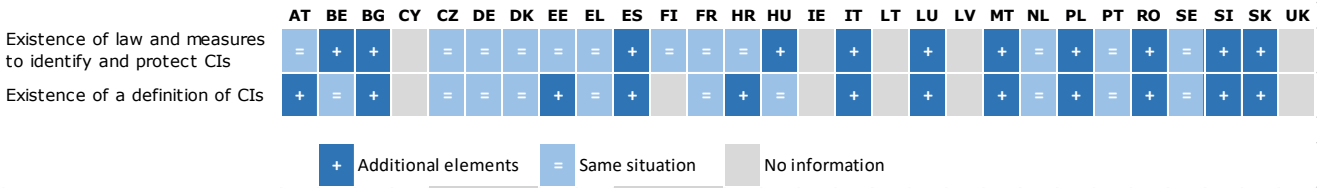
objectives. The Sections below provide a summary of the main findings together with an assessment of the extent to which the Directive achieved its general objective.

6.3.1.1 Establish a procedure for the identification and designation of ECI

The Directive has partially achieved the objective of establishing a common procedure for the identification and designation of ECI.

The Directive set out an outline of the steps needed to be taken by relevant stakeholders in order to identify potential ECI and then to designate them as such. This procedure was subsequently transposed by all MS (Section 5). In so doing, the ECI Directive also contributed to the introduction for the first time of a definition of CI in around half of MS (12), and to the adoption of laws and measures to identify and protect CI in 11, therefore filling a potential security gap. Figure 7below illustrates the changes that were made at MS level as compared with the situation prior to 2008.

Figure 7 – Change at MS level as compared with prior to 2008



Source: Authors' elaboration based on survey answers and implementation tables

However, **the extent to which this common procedure contributed to the implementation of a truly common and harmonised framework across MS is less clear**. Only half of PoCs and representatives from other ministries that responded to the survey held that the Directive resulted in a common and agreed-upon procedure for the identification and designation of ECI.[264] Perhaps unsurprisingly, the perception of stakeholders is more positive in those MS with at least one designated ECI,[265] as the very presence of ECI can be seen as an indication that the procedure introduced by the Directive is in place and has been applied by the MS involved in the designation. This confirms the finding of the previous review of the Directive, which found that a coherent approach to CIP/European CIP among the MS was lacking.[266]

When considering the various provisions contained in the Directive, the **most significant differences between MS are in regard to definitions and the identification process**. As highlighted in the implementation state of play, the generality of the definitions contained in the Directive leaves room for different interpretations that affect how different MS approach the identification process. Other issues involving the identification process relate to the application of the transboundary element and reaching an agreement with neighbouring MS.[267] Differences in these respects could be explained by:

- *The difference in the perception of risks facing a particular CI*, which may result in different definitions in different MS as to the sectoral and cross-sectoral criteria, as well as different thresholds that the effects of a disruption/destruction should meet in order for the infrastructure to be considered critical (*Finding 9*). While the JRC has produced guidelines that could support a common interpretation of the Directive, these are non-binding. The MS may choose to use the guidance as is, or alter it as they feel appropriate (e.g. the methodology for use in calculating the thresholds and for performing the threat analysis). This situation may result in diverging approaches, thereby reducing the harmonisation of the identification process across MS;
- *The difference in MS attitude towards co-operation*. For instance, some MS have applied a so-called "principle of reciprocity" when implementing discussions with neighbouring MS on

[264] Survey: 50% (N=11) of PoCs and 47% (N=7) of Other ministries stated that the Directive resulted in the establishment of a common and agreed-upon procedure for the identification and designation of ECI to a high or very high extent.
[265] Survey: 70% (N=7) of PoCs and 50% (N=4) of Other ministries in MS with ECI considered that the Directive resulted in the establishment of a common and agreed-upon procedure for the identification and designation of ECI to a high or very high extent.
[266] Ramboll. (2012). Study into the potential impacts of options amending council Directive 2008/114/EC.
[267] Survey: 61% (N=11) of PoCs consider the application of the transboundary element of the definition of ECI as one of the main difficulties in the implementation of the identification process to a moderate, high and very high extent.

the identification of an ECI. According to this principle, the level of the information shared will be balanced and proportional to the information/feedback received by the counterpart;

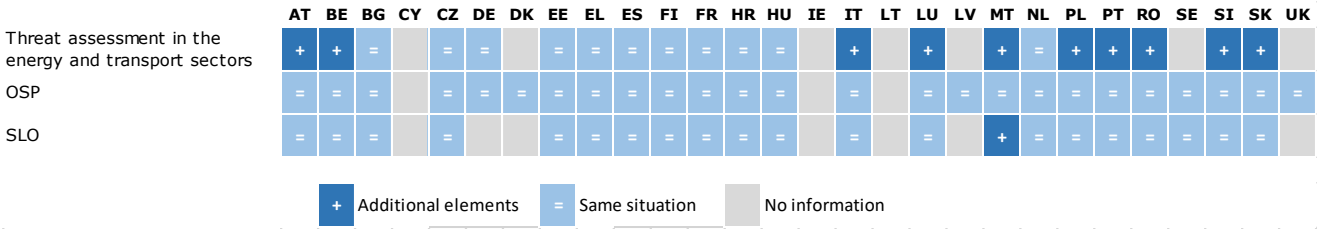
- *The difference in capabilities across MS*, both in terms of type of involved actors and human resources allocated to CIP-related activities. While the Directive serves to create similar CIP roles/responsibilities in all MS (especially by formalising the PoC),[268] CIP governance at MS level is still fragmented and heterogeneous (*Finding* 21, *Finding* 22, *Finding* 25). This may create a certain unbalance in the context of any discussions on identification and designation. For instance, MS with strong capabilities that share a border with MS with limited capabilities may not see significant added value from co-operation and, as a result, may pursue a unilateral approach instead;
- *The share of roles and responsibilities* does not reflect the stakes that MS have in the identification and designation process.[269] As an example, the identification process is initiated in MS one, where a specific potential ECI is located. The very fact that the CI is located in another MS limits the ability for MS two to take the initiative on identification. Furthermore, the relevant CI in MS one is in most cases already an NCI. Assuming the level of protection of ECI and NCI is the same, the added value of initiating the designation procedure appears to be limited to MS one.

6.3.1.2 Establish a common approach to the assessment of the need to improve the protection of ECI

The Directive has achieved the objective of establishing a common approach to the assessment of the need to improve the protection of ECI only to a limited extent.

The Directive introduced provisions relating to the OSP, the SLO and reporting that were formally transposed by all MS. However, as shown in Figure 8, the impact of the Directive on national practices was limited, given that in most cases the Directive requirements were already part of the existing national/operator approaches to NCI protection. Indeed, prior to 2008, operators in 25 MS already had an OSP in place. Meanwhile, the SLO function existed in 20 MS.

Figure 8 - Change compared with the situation prior to 2008



Source: Authors' elaboration based on survey answers and implementation tables

Moreover, **the limited details related to certain provisions** (e.g. the risk analysis in the OSP, the characteristics of the SLO, the threat assessment to be communicated to the MS) **hampered the extent to which the approach introduced by the Directive was truly common**. For instance, only half of PoCs and other ministries considered that the Directive resulted in a common approach to the assessment of the need to improve the protection of ECI.[270] Similarly, operators highlighted the current variety of approaches across MS, which arguably points to the limited harmonising effects of the Directive.[271]

When considering specific provisions of the Directive, the **support provided by the EC has been particularly effective** in establishing a common approach insofar as it facilitated the sharing of

[268] PC: 52% (N=30) of respondents agree with the statement that the Directive has contributed to defining similar and clear responsibilities and obligations for CIP stakeholders in all MS.
[269] PC: 30% (N=19) of the respondents consider that the current approach based on the designation of ECI by MS is appropriate and effective to a fairly large and large extent. 31% (N=18) of respondents consider that the current approach calling for MS to designate ECI in agreement with those MS that may be significantly affected is appropriate and effective to a fairly large and large extent.
[270] Survey: 45% (N=10) of PoCs and 44% (N=7) of Other authorities considered that the Directive resulted in a common approach to the task of assessing the need to improve the protection of ECI to a high or to a very high extent. Restricting the same to MS with ECI only, the shares are higher: 60% (N=6) of PoCs and 50% (N=4) of Other authorities.
[271] Workshop: CI owners/operators; Case study: 1 MS; Interview: 1 EU CI owners/operators. Given the impossibility to identify ECI and ECI operators, this finding should be considered in relation to the CIP framework in general.

good practices and methodologies across MS through guidelines and workshops. On the other hand, **the requirements for an OSP, an SLO, and reporting to the Commission proved to be partially effective**. While all MS that have designated ECI have put in place the OSP and SLO provisions and regularly report to the EC, the generality of these provisions makes it difficult to argue that the Directive has resulted in a common approach in all MS (*Finding* 16, *Finding* 17, *Finding* 19).

To conclude, while it would be too ambitious to establish a direct causal link between the introduction of the Directive and the changes described in Figure 7 and Figure 8 above, it is at least possible to infer that the Directive did not cause any significant steps backwards in the CIP sectors that the Directive concerns. Therefore, while the number of confounding variables and external factors is too large to be able to conclusively state that the Directive brought about the observed changes relative to the pre-Directive 2008 baseline, it is possible to argue that the Directive provided a positive contribution, especially in terms of helping to codify clear and interoperable definitions of CI.

6.3.1.3 Improve the level of protection of CI with EU relevance in the energy and transport sectors

The assessment of the contribution of the Directive to the overall objective of an improved level of protection of CI with EU relevance is inconclusive. The creation of or further strengthening of national CIP frameworks in half of the MS, as well as similarities between the EU and national requirements concerning the protection of ECI and CI, respectively, seems to suggest that those CI with European relevance are protected in equal measure, no matter if they are designated as ECI or not. While this could be seen as proof that the Directive's overall objective has been achieved,[272] available evidence does demonstrate that requirements for both CI and ECI protection do vary from one MS to another. Therefore, the possibility that actual levels of protection vary as well cannot be excluded.

Generally speaking, a secure Europe is also the result of a stable internal market where industry operators face similar rules irrespective of which MS they are based/operate in. By introducing a minimum common framework for the protection of ECI, the Directive also aimed at preventing the creation of an uneven level playing field for CI owners/operators and the subsequent competitive advantages/disadvantages related to where they choose to do business in Europe. Some regulatory improvements occurred with around half of MS that have adopted specific measures for the protection of CI.

Evidence gathered throughout the Evaluation and summarised in previous Sections highlights the existence of heterogeneous interpretations of the definitions and provisions of the Directive that might suggest that CI owners/operators in different countries face different requirements and costs. This consideration seems to be confirmed by the results of the PC where only a limited share of respondents reported that the Directive strongly contributed to a higher level of protection of the internal market from the effects of any disruption/destruction of CI.[273] Moreover, few CI operators reported being subject to different obligations depending on the MS that they operated in.[274] That being said, the actual content of the protection measures adopted by operators is unknown (for reasons of confidentiality) as are the ECI that they operate. This makes it impossible to assess conclusively to what extent operators of ECI in different MS are in fact subject to the same requirements and bear the same costs, and eventually to assess to which extent there is currently a level playing field among MS.

6.3.1.4 Main obstacles

EQ 3.4 Are there any factors that limit the effectiveness of the Directive? If so, what are these, where do they stem from, and which stakeholders do they involve?

[272] PC: in the energy sector, 78% (N=45) of respondents see an increase in the level of protection of CI in the EU in the last decade, with 54% (N=25) considering this level increased to a fairly large and large extent; in the transport sector, 67% (N=29) of respondents see an increase in the level of protection of CI in the EU in the last decade, with 50% (N=17) considering this level as increased to a fairly large and large extent.
[273] PC: only 33% (N=18) of respondents agree or strongly agree with the statement that the Directive has contributed to a higher level of protection of the internal market from the effects of any disruption/destruction of CI.
[274] Interview: 1 CI owner/operator. Case study: 1 MS (CI owners/operators).

A series of factors have hindered the process of identification and designation of ECI, both specifically linked to the Directive and external to it.

Limitations of the Directive

The Directive appears to suffer from two weaknesses which are in apparent contradiction with one another:

- On the one hand, **the Directive appears to be too vague** in defining key terms and how certain elements of the Directive should be implemented. This provides too much leeway as to how certain essential provisions should be interpreted. For instance, the definitions of CI, ECI, 'protection', 'risk analysis' and 'owners/operators of ECI' are very general, and as a consequence, have been interpreted and implemented differently in different MS (*Finding 1*). Furthermore, some key terms in the identification and designation process lack operational detail (e.g. availability of alternatives, essential service, SLO, OSP (*Finding* 19, *Finding* 18) or are non-binding (e.g. sectoral and cross-cutting criteria). Taken together, these weaknesses serve to limit their usefulness in contributing to a common approach (Section 6.1.1.4, Section 6.3.1.1, Section 6.3.1.2);
- On the other hand, **the identification of ECI is difficult because of the complexity of the procedure that has been put in place and the criteria that have to be met.** This is particularly true with regards to the application of the transboundary element and reaching an agreement with other MS. According to many PoCs, both tasks entail meeting certain criteria that it is difficult to achieve agreement on (Section 6.3.1.1 on the identification process).

Though they may appear in contradiction to one another, these limitations are in fact related. The Directive is an attempt to introduce common/harmonised procedures in an area that many MS would prefer to manage autonomously or through voluntary co-operation measures.[275] It is for this reason, so as to ensure that national practices are accounted for, that the Directive provides ample margin for interpretation in terms of definitions. Nevertheless, the tension that exists at the "political" level creates difficulties in operationalising the Directive, not least the provisions concerning the identification and designation of ECI.[276]

In addition, the Directive lacks a monitoring and evaluation mechanism, comprising indicators of outputs, results/outcomes and impacts. The analysis carried out as part of this Evaluation shows that there are few indicators that can be used to assess the effective implementation of the Directive beyond how many ECI have been designated, and in which countries these designations took place. Furthermore, the Directive requires MS to report on the types of threats, risks and vulnerability that they face. However, this requirement has been used for general compliance purposes rather than to support the creation of EU-level knowledge, or to support continued MS efforts to protect designated ECI (*Finding* 20). The absence of a monitoring and evaluation component to the Directive may be explained by the reluctance of MS to share sensitive information, but also some resistance to any deeper involvement by the EC in what was at the time of adoption considered to a competence reserved to the MS. As a consequence, there is currently no mechanism in place enabling the EC to monitor the application of the Directive, let alone to see *whether* and *how* the MS have in fact complied with its provisions. In the absence of such indicators, there is no rigorous way to check whether the provisions of the Directive have led to an increase in the protection of designated ECI. This in turn limits the evidence base for future decision-making and policy development in this regard.

There is limited awareness about funding available to support implementation of the Directive by MS. This may limit its effectiveness, given current pressure on resources deriving from the economic crisis. Some stakeholders, mainly operators, showed a limited awareness of the EU funds available for general CI protection and subsequently perceives a lack of funding as a factor that negatively affects the level of CI protection, as well as the

[275] Interview: 1 Academia and think tanks, 1 EU CI owners/operators. Ramboll. (2012). Study into the potential impacts of options amending council Directive 2008/114/EC.
[276] Survey: 40% (N=7) of PoCs indicated that they encountered difficulties in the identification process due to the complexity in applying sectoral and cross-cutting criteria.

implementation of the Directive.[277] This issue has grown in significance in times of economic crisis, which have a particular impact with limited resources (see Section 6.1.2.2). While funding for CIP-related actions is available at EU level, the overall funding landscape is neither specific to CIP[278] nor particularly visible.[279] The same is true of funded CIP-related projects, many of which are not distributed, and if they are, are distributed with delays. In some instances, these delays are due to confidentiality issues.[280] Moreover, there is no formal link between the funding that is available and the Directive. This means that the European work programmes designed to allocate funds do not necessarily take into account the needs of stakeholders involved in the implementation of the ECI Directive.[281]

Obstacles which are external to the provisions of the Directive

The protection of CI is a national priority and a responsibility of MS. When the Directive was introduced in 2008, 9 MS already had all or most of the elements introduced by the Directive in their national CIP frameworks, albeit with different ways of management, different priorities and heterogeneous governance systems (see Section 2.3). These differences represent an external obstacle on both an operational and political level:

- At the *operational level*, the Directive had to "find a place" within and adapt to **existing national CIP frameworks that may be working in pursuit of different priorities/goals**, and can be more or less structured. As shown in Section 5, the focus of CIP frameworks in some MS is on law enforcement aspects, others on defence and state security, and still others on civil protection. These different frameworks and perceptions imply both that it is difficult for the Directive to cater to the needs of all MS, but also that MS may experience difficulties in communicating with one another;
- At the *political level*, **there is little appetite** at the MS level for more EU support in this area, as some MS seem to prefer less structured, voluntary bilateral co-operation.[282] While this consideration applied at the time that the Directive was proposed, the respective positions of MS on this question seems to be more mixed; while some MS still view CIP as a unique national competence, others acknowledge the added value provided by the EC in this policy area and accept a certain competence at European level.

These considerations help to explain why the current distribution of designated ECI is skewed towards a handful of MS. It appears that a small number of MS "championed" the Directive, while the remaining MS (a large majority) either designated no ECI, or only one/a few.

The presence of a pre-existing framework seems to be among the factors explaining how the Directive was implemented in different MS. Generally speaking, designation is more frequent in MS with pre-2008 CIP frameworks that did not include any of the Directive's provisions. Meanwhile, MS whose pre-existing frameworks already included all or most of the elements of the Directive typically did not designate any ECI.

Within the group of MS that had no, partial or different provisions for the protection of CI as compared with those included in the Directive, **the Directive resulted in an ECI designation where it constituted an opportunity to develop or improve the national CIP framework rather than simply an instrument by which to identify ECI**.

Looking more specifically at the number of ECI, large MS with significant transportation (*Finding* 3) and energy distribution hubs collectively designated only few ECI. Conversely, countries with

[277] Case study: 1 MS (PoC, Other Ministry, CI owners/operators); Survey: 1 PoC, Workshop: CI owners/operators. Interview: 1 CI owners/operators.
[278] There are different funding streams that could be used to fund CIP related projects such as the Internal Security Fund - Police (ISF-P) 2013-2020 (the successor of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme in the current Multi annual Financial Framework), and Horizon 2020 with the Secure Societies Programme whose aim includes "to enhance the resilience of our society against natural and man-made disasters, ranging from the development of new crisis management tools to communication interoperability, and to develop novel solutions for the protection of critical infrastructure".
[279] Interview: 1 EC DGs and Agencies, involved in the management of security funds.
[280] Interview: 1 EC DGs and Agencies. Workshop: CI owners/operators. Survey: 1 PoC and 1 CI owner/operator.
[281] Interview: 1 EC DGs and Agencies.
[282] Interview feedback: 1 Academia and think tanks and 1 EU CI owners/operators. Ramboll. (2012). Study into the potential impacts of options amending council Directive 2008/114/EC.

a less mature energy market compared to other MS account for the majority of ECI. **The uneven distribution of ECI across the Union might suggest uneven buy-in from MS, and does not necessarily reflect needs "on the ground". Furthermore, it points to the importance of the appetite at the MS level in certain MS for greater EU support.**

Moreover, **a reluctance to share sensitive information relating to CI at European level could also be observed among all the categories of stakeholders involved in the study.** This is primarily due to security implications as well as certain market/corporate implications.[283] For instance, gas distributors are reluctant to share information concerning how much gas is carried through a given pipeline, let alone to whom it is sold. As highlighted in the literature,[284] barriers to information sharing among operators may also stem from other considerations, including: financial hinders (possible negative impacts on the value of the operator's stock); reputation/image concerns (i.e. information to suggest vulnerabilities may damage the public's perception of the MS or operator); simple denial (i.e. that they in fact are possible targets); perceived lack of value in having an exchange with counterparts; and/or and a lack of mutual trust between and among operators.

6.3.2 Degree of the Directive's contribution to results

EQ 3.2 To what extent can any observable achievements regarding the enhanced security of ECI[285] be attributed directly to the Directive, or rather to other developments (i.e. the introduction of other instruments, actions at the Member State level, on the part of operators, etc.), linked to, or independent, form the Directive?

It is extremely difficult to disentangle the effects of the Directive on the security of ECI from the effects deriving from independent MS actions, the introduction of other EU-level instruments, or voluntary actions on the part of operators.[286] Put another way, **the security of ECI is the result of the interplay of a number of external factors**, some of which are described below. The task of identifying the effects of the Directive specifically is made all the more difficult for the fact that the identity of the various ECI is not known; this makes it impossible to compare the level of protection of designated ECI as per the provisions of the Directive with the level of protection of NCI. With knowledge of the ECI, it would have been possible to isolate the contribution of the Directive from the contribution of other instruments and measures. Some of the external factors that may contribute to the protection of designated ECI include:

- *National legal initiatives and/or measures taken by national authorities*, such as the production of guidelines, establishment of networks involving operators (e.g. the European Energy Information Sharing & Analysis Centre (EE-ISAC)[287]), setting up dedicated CIP centres, and exchanging good practices. These are viewed by PoCs, other national authorities and operators as the most important external factors;[288]
- *Measures taken voluntarily by CI owners/operators*,[289] such as participating in various CIP-related fora and producing internal procedures. Relevant industry associations are also seen to take measures, which include producing common guidelines, white papers and position papers.[290] Approximately half of operators and national authorities considered these measures relevant;

[283] Interview: 1 EC DGs and Agencies.
[284] Giroux, J., & Melkunaite, L. (2013). Information Sharing for Critical Energy Infrastructure Protection: Finding value & overcoming challenges. *Energy Security Forum*, (8), 20–22.
[285] The original formulation of this evaluation question read CI instead of ECI. The focus has been narrowed to ECI to avoid overlap with the following question, EQ 2.3, that looks at the impact of the Directive on CI in general.
[286] Workshop: PoCs and CI owners/operators; Case study: 1 MS.
[287] The EE-ISAC is an industry-driven network launched in 2015 and composed of public and private actors to exchange experiences and information about incidents and attacks within their own organisation in order to protect the industry as a whole. The network involves academia, governmental and non-profit organisations and, albeit at a smaller extent, CI owners/operators.
[288] Survey: 69% (N=11) of PoCs, 67% (N=6) of Other ministries, and 38% (N=15) of CI owners/operators indicate that national measures contributed to an increased level of protection of ECI to a high or very high extent.
[289] Survey: 54% (N=7) of PoCs, 50% (N=5) of Other ministries, and 54% (N=22) of CI owners/operators indicate that measures taken by CI owners/operators contributed to an increased level of protection of ECI to a high or very high extent. Case study: 2 MS.
[290] Interview: 2 EU CI owners/operators.

- *Other EU level initiatives*,[291] including: sectoral initiatives that impose stricter requirements on MS and operators than those imposed by the ECI Directive (e.g. in energy, aviation and maritime); cross-sectoral initiatives focusing on specific CI aspects (e.g. the NIS Directive on network and information systems); or arrangements/activities (e.g. the Civil Protection mechanism, certain activities within EPCIP facilitated through the CIWIN platform);
- Initiatives taken in *intergovernmental settings*, such as bilateral agreements,[292] or regional forums of co-operation, one example being the Nordic Council.[293]

Besides these factors, it is worth recalling that the implementation of the ECI Directive is part of and relates to *EPCIP*. Voluntary initiatives and exchanges of good practices that have come as part of this framework have also had an impact on the protection of designated ECI.[294]

6.3.3 Spill-over effects

EQ 3.3 To what extent, if at all, has the Directive impacted on the protection of CI at the MS level that was not designated as ECI during the reference period?

The Directive brought about effects that went beyond its scope (referred to here as spill-over effects). These effects involved CI that were not designated as ECI and were not necessarily in the energy and transport sectors.[295]

Specifically, **the Directive brought increased awareness of and created political momentum concerning the protection of CI** in almost all of the MS, including MS with pre-existing national CIP frameworks. This effect was observed regardless of whether or not these MS in fact designated ECI. Stakeholders' views converge on this point.[296] This was the case because the Directive provided legitimacy and a sense of urgency to new/renewed national-level attention to and action on CIP.

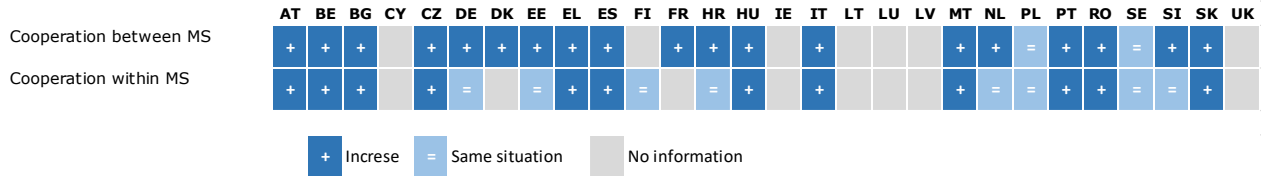
In the majority of MS that had no, partial or different provisions concerning the protection of CI (as when compared with the provisions included in the Directive), this increased awareness resulted in the introduction of comprehensive legislation covering a wide variety of sectors.[297] This is particularly true of those MS that recently joined the Union (i.e. BG, RO), but also of some 'older' MS (i.e. BE, ES, MT, SK).[298] Awareness was raised both among national authorities and operators. Where operators already had in place security measures, the introduction of new national legislation helped to explain why these measures were needed. It also increased awareness among company CEOs,[299] resulting in a change in company culture in ways that served to benefit CIP-related work.[300]

[291] Survey: 44% (N=7) of PoCs, 71% (N=5) of Other ministries, and 31% (N=10) of CI owners/operators indicate that other EU level initiatives contributed to an increased level of protection of ECI to high or very high extent. Case studies: 2 MS.
[292] Case study: 1 MS.
[293] The Nordic Council facilitates co-operation between DK, FI, NO and SE in the fields of safety and security. In practice, this entails regular high-level meetings, crisis decision-making workshops and trainings, as well as projects addressing cross-border crisis-management issues (Pursiainen, C. (2018). Critical infrastructure resilience: A Nordic model in the making? *International Journal of Disaster Risk Reduction*, *27*, 632–641. Case study: 1 MS.)
[294] Case study: 2 MS (PoCs and Other Ministries).
[295] Methodologically, as it is difficult to disentangle the effects of the Directive on the protection of ECI from other factors, so it is problematic to assess the effects of the Directive that went beyond its intended effects and that can be attributable to the Directive alone. Subsequently, the reported spill-over effects can be attributed to the Directive as well as to intertwine national initiatives.
[296] Survey: 65% (N=15) of PoCs consider that the Directive increased awareness on the importance of CI and their protection to a high or very high extent. 75% (N=36) of CI owners/operators and 71% (N=19) of Other ministries consider that it did so to a moderate/high/very high extent. Workshop: PoCs and CI owners/operators. Interview: 3 EC DGs and agencies, 4 EU CI owners/operators, 4 Academia and thinks.
[297] Out of 14 MS that had no, partial or different provisions for the protection of CI compared with those included in the Directive, 11 introduced laws and measures to identify and protect CI (BE, BG, ES, HU, IT, LU, MT, PL, RO, SI, SK) and nine introduced a definition of CI (BG, ES, IT, LU, MT, PL, RO, SI, SK) and nine a threat assessment in the energy and transport sectors (BE, IT, LU, MT, PL, RO, SI, SK).
[298] Workshop: PoCs, Implementation tables in Annex II.
[299] Workshop: CI owners/operators.
[300] Case study: 1 MS.

In those MS[301] where most of the elements of the Directive were present prior to 2008, the Directive served to further formalise them. For instance, some MS codified the OSP and SLO obligations on operators,[302] while others formalised the CI definition[303] or the threat assessment requirement pertaining to the energy and transport sectors.[304] In these cases, MS saw the transposition of the Directive as an opportunity to formalise, strengthen and/or overhaul existing national CIP frameworks. In FR, for instance, the Directive resulted in a shift from a terrorism-focused approach to one that was all-hazards in nature, and raised awareness among the relevant stakeholders concerning the importance of CIP.

The increase in CIP awareness generated an increase in co-operation both between and within MS. As shown in Figure 9, co-operation of different kinds increased in most MS.

Figure 9 - Changes occurred to the baseline since 2008



Source: Authors' elaboration based on survey answers and implementation tables

- **Co-operation between authorities in potentially affected MS** was already present in about half of the MS prior to the introduction of the Directive (Section 2.3). In these MS, co-operation deepened after 2008, and took place for the first time in the remaining MS.[305] The fact that this increase in co-operation is perceived more strongly by PoCs than by other national authorities[306] suggests that the Directive contributed in encouraging co-operation outside the remit of sectoral authorities. This arguably came about as part of the discussions that MS had during the identification process, no matter if it ultimately generated an ECI designation or not. Workshops organised by the JRC as part of the Directive implementation phase[307] also spurred co-operation at a more technical level across MS. Finally, in some countries, the Directive served to "elevate" discussion on CIP to the ministerial level, making co-operation with other MS easier;[308]
- **Co-operation within the various MS** also increased, both between authorities and between authorities and operators. In around half of the MS, *competent authorities* already co-operated prior to the 2008;[309] the Directive simply spurred on more co-operation.[310] Just as in the case of co-operation between MS, the increase in national-level co-operation on CIP was particularly felt by PoCs, suggesting again that the Directive contributed in encouraging co-operation outside the remit of sectoral authorities. The Evaluation finds that this was in some cases due to the definition of more clear roles and responsibilities[311] thanks to the Directive.

  The Directive also increased co-operation and the exchange of good practices between *authorities and operators.*[312] In ES, for instance, the creation of a centre dedicated to CIP

[301] AT, CZ, DE, EE, EL, FR, HR, NL, PT.
[302] Booz & Company GmbH. (2012). Study to support the preparation of the review of the Council Directive 2008/114/EC on the "identification and designation of European critical infrastructures (ECI) and the assessment of the need to improve their protection".
[303] AT, EE, HR.
[304] AT, PT.
[305] PC: 51% (N=27) of respondents agree on the fact that the Directive has enhanced co-operation between MS on matters relating to CIP.
[306] Survey: 90% (N=19) of PoCs, 40% (N=4) of Other ministries report that co-operation with other competent authorities in potentially affected MS increased after the Directive.
[307] Giannopoulos, G., & Schimmer, M. (2011). Memorandum on the results of the sixth Workshop on the Implementation and Application of the Directive. JRC.
[308] Case study: 1 MS (PoC).
[309] Survey: 59% (N=13) of PoCs, 75% (N=9) of Other ministries report that co-operation with other competent authorities in their country existed before the Directive.
[310] Survey: 60% (N=12) of PoCs, 43% (N=6) of Other ministries report that co-operation with other competent authorities in their country increased after the Directive.
[311] Survey: 60% (N=12) of PoCs consider that the increase in co-operation was due to clearer definition of responsibilities to a high or very high extent.
[312] Survey: 67% (N=14) of PoCs, 50% (N=7) of Other ministries, and 72% (N=26) of CI owners/operators notice an

made communication at the national level easier insofar as the centre created a unique reference point for and facilitated co-operation between the relevant national stakeholders. The centre provided operators with a platform for them to share experiences, technical know-how and approaches with national authorities and other operators.

Co-operation between MS on ECI laid the groundwork for the implementation of the NIS Directive at MS level. Some MS reported that they used the experience and organisational structure developed for the implementation of the ECI Directive when transposing the NIS Directive.[313] For instance, ES integrated the transposition of the NIS Directive into its existing national CIP framework, suggesting that the ICT sectoral focus of the NIS Directive was viewed in a Spanish context as a necessary element of CIP.[314] To signal this, ES's CIP reference authority, the National Centre for the Protection of Infrastructures, became the National Centre for the Protection of Infrastructures and Cybersecurity upon the transposition of the NIS Directive. Moreover, Spanish authorities found the experience gathered from CIP transferable to the task of identifying and designating digital service providers and operators of essential services.[315]

The Directive also served to some extent to shed new light on the provision of security services in a CIP context. The renewed interest in CIP spread by the Directive laid the groundwork for improved co-operation between CI owners/operators and private providers of security services/solutions.[316] However, as highlighted by two interviewees, current co-operation might be improved. Specifically, the role of providers of technological security solutions in contributing to the protection of CI is only considered to a limited degree. Similarly, providers of security services are usually involved once the OSP has been drafted and only as security providers. According to the interviewees, private security expertise in the analysis of risks and the knowledge of security threats could be useful during the OSP drafting phase.

Finally, **the Directive had a positive effect on co-operation with third countries in some cases**. The Directive prompted the creation of comprehensive CIP frameworks in certain MS that elicited the interest of some third countries interested in launching similar initiatives. This was true of both neighbouring and non-neighbouring countries.[317] When taken together with the co-operation activities with third countries that are part of EPCIP, this evidence would appear to suggest that the Directive has prompted work at MS level that is of relevance beyond the borders of the Union and in some instances facilitates new forms of co-operation with third countries.

6.4 Efficiency

This Section addresses the efficiency of the Directive. This evaluation criterion aims at understanding whether stakeholders sustained any costs as a result of the introduction of the Directive, and, if so, how significant these were when compared with the benefits that were achieved by the Directive's implementation (as described in Section 6.3). The Section includes an overall assessment of the cost-effectiveness ratio of the Directive (Section 6.4.1) and briefly describes key factors that are seen to affect this ratio (Section 6.4.2).

6.4.1 Overall cost-effectiveness

Q 4.1 Have the results that can be attributed to the Directive been achieved at a reasonable cost? Is the regulatory burden on MS, industry and other relevant stakeholders created by the implementation of the Directive (i.e. specific requirements/procedures) commensurate with observable results?

The introduction of the Directive created a set of obligations for all categories of stakeholders. As with all EU legislation that requires transposition at MS level, the Directive created an obligation for stakeholders involved in the process to act. This entailed different types

increase in public-private co-operation for the protection of NCI form a moderate to a very high extent after the introduction of the Directive. Survey: 72% (N=26) of CI owners/operators notice an increase in the exchange of good practices with relevant national stakeholders after the introduction of the Directive.

[313] Interviews: 2 EC DGs and Agencies.

[314] Interviews: 2 EC DGs and Agencies.

[315] Case study: 1 MS.

[316] Interviews: 2 EU CI owners/operators,

[317] Several Latin American countries contacted Spanish authorities to transfer the national CIP framework to their countries. Similarly, Serbia, Georgia and Moldova co-operated with Romanian authorities to transfer the Romanian CIP framework.

of costs. Based on the outcomes of the analysis, these included: substantive compliance costs[318] for MS authorities and CI operators/owners; administrative costs[319] for MS authorities and CI operators/owners; and to a lesser extent enforcement costs[320] for MS authorities.

MS authorities are subject to most of the obligations created by the Directive; almost all these obligations entail a recurring cost insofar as the process of identification and designation of ECI must be reviewed on a regular basis.

The **data that has been collected and that can be used to suggest efficiency is quite limited and did not allow for a quantification of costs incurred**. Moreover, as ECI are not known due to confidentiality reasons, it was not possible to distinguish between operators of national CI and European CI. This made the analysis of the costs associated with Directive implementation complex. Due to a lack of certain data, the Evaluation team chose to focus on the incidence of these costs, and specifically on the number of MS that might be affected by the specific obligations introduced by the Directive.[321] This was used as a proxy for assessing the scale of the costs that can be attributed to the Directive under the assumption that the higher the number of obligations involving significant costs, the wider the scale of the overall costs incurred on account of the Directive. Annex I.10 includes a detailed analysis of the obligations and the related costs introduced by the Directive, the categories of stakeholders concerned, and the incidence of costs.

Generally speaking, the incidence of costs relating to the implementation of the Directive is between low and medium, given that most of the requirements introduced by the Directive had already been met when the Directive went into force in 2008. The analysis of the implementation of the Directive at national level (see Section 5) shows that the scale of costs brought by the Directive is limited, given that several requirements contained in the Directive had in fact already been implemented at national level prior to 2008. The only new costs that the Directive entails for stakeholders come in relation to reporting obligations (data on risks, threats and vulnerabilities per ECI sector) and to inform the EC as to the designation of ECI.

- With regard to *MS authorities,* the designation of CIP PoCs appears to have taken place within the context of EPCIP. Meanwhile, the general contours of the ECI identification and designation process resembled pre-existing processes in around half of MS, and the dialogue between MS authorities providing a platform to discuss Directive-related matters was already in place in some countries (eight);
- As for *CI owners/operators*, most of the costs incurred in drafting OSPs and designating SLOs were likely borne before 2008. This is due to the fact that equivalent practices were typically already in place. As highlighted by one CI owner/operator stakeholder interviewed as part of the Evaluation, the SLO's function and responsibilities are very similar to those of a chief security officer, albeit with a somewhat broader range of responsibilities (e.g. liaising with national competent authorities). Furthermore, venues/channels for co-operation between CI owners/operators and MS authorities existed in around half of the MS prior to 2008.

Moreover, **certain costs brought about by the Directive are only applicable in the event of ECI designation**, and, as discussed in Section 5.4, this has only happened in a limited number of instances (*Finding 15*) in a small number of MS.[322] In other words, the costs associated with actual ECI designation are incurred by a small number of MS and CI owners/operators.

There is no agreement as to whether the Directive brought actual costs. The majority of PoCs and CI owners/operators answering the online survey reported that procedures and

[318] Substantive (compliance) costs are created by legal obligations to act. Such costs encompass those investments and expenses that are faced by businesses and other parties in order to comply with substantive obligations or requirements contained in a legal rule (Better Regulation Toolbox #58).
[319] Administrative burdens (or costs) are costs borne by businesses, citizens, civil society organisations and public authorities as a result of administrative activities performed to comply with information obligations included in legal rules (Better Regulation Toolbox #58).
[320] Enforcement costs are associated with activities linked to the implementation of an initiative such as monitoring, enforcement and adjudication (Better Regulation Toolbox #58).
[321] The incidence is high insofar as the requirement is new and few MS had equivalent measures before 2008. The incidence is low when several to all MS already had similar measures before 2008.
[322] Considering the present conditions and current form of the Directive, it is likely to remain the same, with only a minority of MS having designated an ECI on their territory by 2030. Ramboll. (2012). Study into the potential impacts of options amending council Directive 2008/114/EC.

requirements introduced by the Directive entailed additional costs as compared with the situation prior to the existence of the Directive. Meanwhile, the majority of other ministries considered that the Directive did not entail additional costs,[323]and the stakeholders consulted as part of the case studies viewed the costs associated with the Directive were generally limited or null.[324] Interestingly, no major difference can be pointed out between responses of stakeholders located in MS that designated ECI and MS that have not designated any ECI.

Among stakeholders that reported the existence of costs, there seems to be consensus on the fact that costs brought by the Directive are minor. The majority of PoCs and CI owners operators answering the online survey highlighted that costs brought by the Directive represent a limited share (0-5%) of the total cost usually borne by PoCs and CI owners/operators for the protection of CI.[325] This feedback reinforces the findings of the 2012 study, which concluded that the costs incurred by MS and CI owners/operators were virtually null; once the Directive was transposed and the framework for identification and designation of ECI was in place, the MS' compliance costs were negligible.[326]

Stakeholders' feedback and the fact that several requirements of the Directive were already implemented before 2008 seem to suggest that costs generated by the implementation of the Directive's provisions represent a minor issue when compared with other aspects highlighted by this study (such as the relevance of the provisions to current needs and challenges). As the total costs incurred due to the Directive remain unknown, the Evaluation team is precluded from carrying out **a conclusive cost-benefit analysis of the Directive**.

Similarly, **the assessment of the proportionality of the results achieved in relation to the costs borne by stakeholders is not entirely conclusive**. On one hand, the low-medium incidence of costs brought about by the Directive, and the fact that only a limited number of MS had to bear most of them appears to be proportionate to the limited results achieved by the Directive (see Table 11). On the other hand, a lack of quantifiable data makes it difficult to carry out a sound assessment of the regulatory burden that the Directive entailed. The results of the online survey and the PC suggest that stakeholders' views on the proportionality of costs in relation to results is mixed.[327]

Table 11 - Costs and results related to different provisions in the Directive

Provision	Contribution to the specific objective	Costs
CIP PoC	Effective	Low incidence, not recurrent, and occurring also when an ECI is not designated
Identification process	Partially effective	Medium incidence, recurrent, and occurring also when an ECI is not designated
Designation process	Partially effective	Medium incidence, recurrent, occurring in part when an ECI is not designated
OSP	Partially effective	Low incidence, recurrent, occurring only when an ECI is designated
SLO	Partially effective	Low incidence, recurrent, and occurring only when an ECI is designated
Reporting	Partially effective	Medium incidence, recurrent, occurring only when and ECI is designated

Source: Authors' elaboration

[323] Survey: 78% (N=14) of PoCs and 70% (N=30) of CI owners/operators consider that the Directive entailed additional costs, 64% (N=7) of other Ministries consider that the Directive did not entail additional costs.
[324] Case study: 3 MS (PoCs, Other Ministries, CI owners/operators).
[325] Survey: 71% (N=5, note that 16 answered I do not know) of PoCs and 61% (N=19) of CI owners/operators consider that the costs introduced by the Directive represent only a share between 0% an 5% of their total cost for CI protection; Interviews: 3 EC DGs and Agencies, 2 Academia and think tanks and 2 EU CI owners/operators. No major differences can be seen between responses of stakeholders located in MS with ECI and with no ECI.
[326] Booz & Company GmbH. (2012). Study to support the preparation of the review of the Council Directive 2008/114/EC on the "identification and designation of European critical infrastructures (ECI) and the assessment of the need to improve their protection".
[327] Survey feedback: 36% (N=12) of CI owners/operators consider the costs reasonable and proportionate to the results to a large extent, 24% (N=8) not at all or to a small extent. PC: in the energy sector, costs are considered proportionate and very proportionate to the results by 50% (N=16) of respondents, while the same share consider them disproportionate and very disproportionate; in the transport sector, 53% (N=10) of respondents consider the costs proportionate and very proportionate, and 47% (N=9) of respondents disproportionate and very disproportionate.

6.4.2 Factors affecting efficiency

Q 4.2 What factors have influenced the efficiency of the Directive? To what extent?

Besides certain costs associated with the implementation of the specific requirements of the Directive, a number of other factors were seen to have affected the overall efficiency of the Directive. These include:

- The **generality of the provisions contained in the Directive** (as discussed in Section 6.1.1.2). On one hand, said generality allowed national authorities to leverage existing practices/structures/functions at national level that were already in place, rather than creating new ones. On the other hand, the vagueness of the provisions created some uncertainties, and especially where national frameworks were less developed, thereby hindering efficiency. For instance, the lack of precise guidance on risk assessment methodologies increased the cost for CI operators;[328]
- **Differences in the operationalisation of the OSP across MS**. In one case study, operators mentioned that different OSP requirements in different MS can limit competition across Europe and create an uneven playing field. Specifically, the different MS requirements concerning the formulation of OSPs (and, by extension, the overarching security elements associated with the protection of specific ECI) entail different costs for different owners/operators. Thus, owners/operators in MS with less stringent requirements may find themselves with a competitive advantage over those with more stringent requirements imposed on them (as they would have fewer security-related costs). CI operators in the energy sector interviewed as part of two case studies confirmed that in their view there is still no homogeneity in this respect across the MS. This means that owners/operators operating on a cross-border basis will encounter different security cultures and different OSP requirements when making investments in different MS. While the evidence gathered on this point is limited (relating only to the MS that were subject to case study scrutiny), it does point to an area that could be examined more closely in order to evaluate the de facto evenness of the playing field in Europe as it relates to CIP;
- **The fragmented organisational set-up of the CIP policy field**. Despite widely acknowledged improvements in cross-border co-operation brought about by the designation of CIP PoCs in each MS, the substantial number of actors involved at the different stages of the ECI process (*Finding* 25, *Finding* 23, *Finding* 24) nevertheless entails significant information costs for some authorities and CI operators where they encounter difficulties in identifying relevant counterparts in other MS.[329] Similarly, the existence of partially overlapping EU sectoral legislation and the related share of competences at the EU level may create some confusion on the part of CI operators;[330]
- **Differences in national data protection and confidentiality laws**. Differences in the specific national legislative frameworks appear to have an impact on the costs associated with carrying out security checks (e.g. background checks).[331] This serves to create an uneven playing field for CI operators and makes the exchange of security-relevant information between authorities and operators more complicated.

6.5 EU added value

EQ 5. To what extent has the Directive achieved EU added value as opposed to what could have been achieved at either the national or the international level?

The EU added value question aims to ascertain whether, in the absence of the Directive, the results achieved to date would nevertheless have been achieved through national, EU, international, and other initiatives. After an initial description of the hypothetical scenario regarding the absence of the ECI Directive and such related consequences, this Section investigates if and how the Directive added to that scenario and therefore brought EU added value.

The hypothetical no-Directive scenario

[328] Workshop: CI owners/operators.
[329] Survey: 1 PoC. Interview: 2 EU CI owners/operators.
[330] Interview: 1 EU CI owners/operators.
[331] Survey: 1 PoC. Case study: 1 MS; Workshop: CI owners/operators.

If there was no ECI Directive, one could assume that the baseline situation outlined earlier would have persisted. This means that half of the MS would be without any formal definition of CI or dedicated measures to protect them. In a field like CIP, where competence rests at national level, these MS would not have modified their national framework unless faced with an obligation to do so. In this light, MS would have continued to adopt their national measures, where present, to protect without any distinction all CI on their territory, each one adopting its own definition of "critical" and without systematically assessing the risks that a potential disruption or destruction of a national CI might have on other EU MS. Therefore, without the Directive there would be a heterogeneous approach to CIP across the EU with subsequent grey areas of risk for the security of EU citizens.

Differences in the measures applied nationally to protect CI would also have maintained an uneven playing field where CI operators are requested to bear different costs depending on the maturity of the national CIP framework and the existing requirements. This situation would therefore have created a competitive advantage for operators located in MS with fewer, less restrictive rules.

Such differences would have contributed to limited mutual trust among MS, reduced transparency in the way CI were protected nationally, and created obstacles to co-operation between MS. They would have continued to use their own vocabulary, while the heterogeneous arrangement of different national CIP frameworks would have added another layer of complexity at MS level. While EPCIP might have prompted some MS to identify a CIP PoC to act as a "unique point of contact" for internal and external requests related to CIP, others might have maintained their initial set-up. This fragmentation of competences might have constituted an obstacle to effective cross-border co-operation, not least in swiftly identifying appropriate interlocutors for inter-MS exchanges of different kinds.

In addition to this, the absence of the Directive would have made the exchange of information at EU level more difficult. EPCIP would have continued to provide a valuable platform for that purpose, though participation in its various dimensions would have been on a voluntary basis. For this reason, it is fair to assume that at least some MS would have continued to use it occasionally, especially those that have developed over the years ad-hoc communication channels with neighbouring MS. Seen in this way, MS with limited resources dedicated to CIP would rely primarily on the information shared within EPCIP, including through CIWIN. This is noteworthy, given that based on the evidence gathered as part of the Evaluation, the amount of information shared in this way is generally quite limited.

The EU added value of the Directive

The comparison of the results achieved by the Directive (as illustrated in Section 6.3) with the aforementioned scenario shows that the Directive had some EU added value.

Generally speaking, **stakeholders agree with this finding, albeit with certain qualifications.** For instance, most of the PoCs and CI owners/operators that responded to the survey reported that the Directive provided EU added value compared to what Member States might have achieved in terms of CIP without the legislation.[332] Responses to the PC further confirmed this finding; perhaps predictably, a slightly higher level of EU added value was seen within the energy sector than in the transport sector (where far fewer ECI are designated) (*Finding 14*).[333]

Specifically, the Directive showed EU added value insofar as it served to achieve results that:

- National or other EU initiatives alone would have not achieved; and/or,
- National or other EU initiatives would have achieved anyway, albeit through longer, costlier and less well-defined processes.

The distinctive results of the Directive

[332] Only 2 PoCs and 9 CI owners/operators consider that the Directive did not help achieving anything different compared to what they could have achieved alone.
[333] PC: in the energy sector 64% (N=38) of respondents consider that the Directive brought EU added value to some, a fairly large and large extent. In the transport sector, 58% (N=26) of respondents consider that the Directive brought EU added value to some, a fairly large and large extent.

The Directive provided the basis for a common framework for the protection of ECI. Faced with a diverse set of approaches to CIP at MS level (see Section 5), the Directive **introduced a common vocabulary**, arguably a prerequisite for establishing cross-border dialogue and mutual understanding.[334] Specifically, the Directive for the first time introduced a common definition of CI as well as **minimum requirements** for the protection of specific CI in specific sectors. The number of MS with a definition of CI codified in their national framework rose from nine prior to 2008 to 20 after adoption. Similarly, 11 MS for the first time introduced legislation and other measures aimed at identifying CI; 10 MS began carrying out threat assessments within the energy and transport sectors. The Directive therefore constituted an important first step within the field of CIP. Despite the limited number of ECI that have been designated since 2008, most MS now have specific national legislative measures in place aimed at addressing the need to protect ECI. Furthermore, they have allocated CIP responsibilities to specific ministries, and have designated PoCs responsible for liaising both with other MS and the EC, thereby easing the cross-border exchange of information. Seen in this way, the Directive created a first piece of common ground on which to stand in conducting certain activities aimed at reducing to some extent the exposure of the EU to transboundary risks associated with CI disruption/destruction.

However, **the potential EU added value that may be derived from this achievement is limited by the vagueness of the definitions and procedures contained in the Directive.** Such vagueness has given the MS considerable leeway in how they interpret and operationalise these, resulting in a high degree of heterogeneity of approach (as demonstrated in Section 5).

Moreover, **the additional value brought by the Directive is unevenly perceived at the national level.** Views on this question are particularly positive among those MS that saw in the Directive an opportunity to introduce for the first time a comprehensive CIP framework. Such was the case in ES, RO and BE. While MS where the national CIP framework already included measures that covered and went beyond the requirements of the Directive face difficulties in understanding the differences between national measures and the Directive's provisions and therefore difficulties in seeing the EU added value brought by this piece of legislation.

The Directive's OSP, SLO and reporting provisions proved to have limited EU added value. As mentioned in Section 2.3, most MS (25) already had OSP-equivalent requirements in place prior to the introduction of the Directive. The Directive provided minimal description as to how to draft the OSP and to perform the risk analysis. In this respect, its added value is limited. Attempts were made to supplement the provisions in the Directive, including the risk assessment methodologies for CIP that were developed by the JRC in 2015.[335] These may have increased the EU added value of this specific provision assuming they were taken up at a national level. However, the Evaluation finds that these non-binding guidelines were considered complicated by some MS, which went on to draft alternative national guidelines as a result.[336]

Similarly, several MS had in place prior to 2008 functions equivalent to the *SLO*. These served as a link between CI owners/operators and competent national authorities (see Section 2.3). While in some MS the Directive has formalised this function,[337] the Directive provided no specific details as to the SLO's role, suggested competences/background, etc. (*Finding* 18). As such, the EU added value of this specific provision is assessed as being limited.

The same appears to be equally true with regard to the *obligation for MS to report* to the EC the number of designated ECI and which sector they belong to, as well as a summary of the types of risks, threats and vulnerabilities in the relevant sectors. While all MS are obligated to report did so, the information they provided was very general (see Section 6.3.1.2) and could hardly be used by the EC to create an EU-wide situational picture[338] (that might then have been fed back to the MS for their own purposes), let alone assess the need for additional measures at EU level. In

[334] Survey: 14 PoCs and 27 CI owners/operators agree that the Directive created common terms of reference for the protection of CI in the EU and that this would have not been possible in absence of the Directive.
[335] JRC. (2015). Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. Ispra.
[336] Case study: 1 MS (PoC).
[337] Booz & Company GmbH. (2012). Study to support the preparation of the review of the Council Directive 2008/114/EC on the "identification and designation of European critical infrastructures (ECI) and the assessment of the need to improve their protection". The identity of these MS is not provided.
[338] Booz & Company GmbH. (2012). Study to support the preparation of the review of the Council Directive 2008/114/EC on the "identification and designation of European critical infrastructures (ECI) and the assessment of the need to improve their protection". Interview: 2 Academia and think tanks, 1 EC DGs and Agencies, 1 EU CI owners/operators.

conclusion, the EU added value of the reporting and information sharing requirement appears to be limited.

However, assessing EU added value on an overall level should be assessed with a systemic EU perspective which draws on and recognises any benefits that it had in individual MS. In this respect, it is worth highlighting that in an increasingly interconnected Europe, where sectors are interdependent and geographical borders are of less practical importance than in decades past, systems as a whole are only as strong as their weakest links. Seen in this way, the adoption of new measures by only a limited number of MS appears to be overcome by the benefits deriving in terms of security for the EU as a whole.

As of today, all MS[339] have a CIP framework or sectoral measures to secure CI; in all MS, specific CIP responsibilities are allocated to national-level ministries charged with coordination and exchange of information, be it internally (with other relevant ministries), or externally (with other MS and the EC). Every MS for which information is available initiated discussions with other MS concerning possible ECI identification[340] and attends, in the majority of cases regularly, the CIP PoC meetings. Within this context, **the EU added value of the Directive today appears less visible**. The level of generality of the Directive's provisions are of limited use in relation to similar/equivalent national CIP measures. A lack of detail also makes it difficult for MS to understand the criteria by which ECI should be granted a higher protection level than NCI.

While acknowledging that the Directive brought some EU added value and contributed in achieving an improved situation compared with the one in the case of the no-Directive scenario, any future discussion concerning the Directive should reflect the finding that the legislation offers limited added value over existing national practices as they exist today.[341] It should also reflect continued questions concerning the extent to which the Directive's has in fact achieved a 'common approach' amongst the MS. Indeed, as highlighted in Section 6.3.1.2, this cannot be confirmed given that the analysis has not examined national CIP frameworks in detail, nor does it have the benefit of access to sensitive documents including OSPs. Without such data, it is difficult to come to any conclusive findings. What is clear is that stakeholders' views on the matter are not entirely aligned. Even though some MS still consider CIP to be a matter of exclusive state sovereignty and are not willing to see an expanded role of the EC in this field,[342] there is an appetite on the part of several MS and CI owners/operators to further develop some provisions and move towards deeper harmonisation across the Union, thus confirming and to some extent widening the EC scope of action.

The Directive as a catalyst for change

The Directive added value to national and international initiatives by increasing awareness concerning the need to protect CI. In other words, **it generated political momentum that led to the prompt adoption or revision of national CIP measures**, but also more general discussions concerning the need to protect CI and the possible ways to do so.

Before the introduction of the Directive, CIP was mainly a national matter, with different degrees of priority depending on the MS. Prior to 2008, MS had considerable room to decide how to protect their national CI; the EU via EPCIP had very limited influence. The importance given to CI owners/operators in the energy and transport sectors also varied between MS.

The Directive served to convey the importance of CIP at EU level, and framed CIP in a wider EU context by giving considerable visibility to some key threats (e.g. terrorism) and stressing the importance of cross-border co-operation and PPPs with operators. This was reflected at the national level.[343] Some MS that had limited or no CIP frameworks introduced specific

[339] DK, FI, SE have a peculiar approach (as shown in Box 6), but could still be counted as having a CIP framework.
[340] Survey: 91% (N=20) of PoCs answered that the MS they represented did start the identification process. The PoC of one country, answered Do not know, but ECI have been designated in its country. Only 2 PoCs mentioned that the identification process was not started, though information provided in the Implementation tables clarifies that the responses in these cases are to be intended merely that the identification process was not fruitful in identifying potential ECI. No information available for CY, IE, LT, LV and UK.
[341] Case study: 1 MS (PoC, Other ministries).
[342] Case study: 1 MS (PoC). Interview: 1 CI owner/operator.
[343] Survey: 12 PoCs and 31 CI owners/operators agree that the Directive helped in framing national policy, measures and initiatives, thereby fostering the creation of a harmonised framework and approach and that this would have not been possible in absence of the Directive.

legislation on CIP; in some cases (e.g. ES, RO) they developed comprehensive approaches with dedicated agencies tasked with managing/co-ordinating CIP-related matters at national level. For almost all MS that fall in this group, national-level co-operation increased thanks to the Directive (see Section 6.3.3). Meanwhile, the Directive prompted other MS to make changes to existing CIP practices. For instance, the scope of the national CIP framework in FR was expanded to mirror the all-hazard approach of the Directive, while the Directive gave legitimacy to the requests made by authorities in SK on CI owners/operators. While these effects could have been achieved through EPCIP, the existence of EU legislation on CIP arguably made implementing such changes easier.

Co-operation with the private sector has increased, as shown in Section 6.3.3. While this cannot be fully attributed to the existence of certain specific requirements contained within the Directive (given the relatively general nature of the SLO and OSP requirements and their limited operational impact), there is nevertheless evidence that this has occurred as a consequence of the Directive and the work on CIP that it has spurred.[344] At least in some MS, this may certainly have taken place even in the absence of the Directive, either within the context of or because of EPCIP and/or national initiatives. However, the Directive has generated an impetus for this in both these and other MS, and encouraged more and deeper communication between operators and national competent authorities.[345]

The adoption of a legally binding instrument like the Directive (instead of the voluntary measures contained within EPCIP) also served to trigger the **creation of an EU-wide cross-border dialogue and operational co-operation** in a field which was traditionally the exclusive competence of the MS.[346]

Specifically, the procedures facilitating discussions on cross-cutting criteria in the identification process, the appointment of CIP PoCs, and the organisation of regular meetings between MS have contributed to mutual understanding and trust between MS, something which was first initiated via EPCIP. By taking part in the identification process, MS identified specific interlocutors in other MS and established suitable communication channels for bilateral or multilateral co-operation. The Directive triggered co-operation in the majority of MS and where there already were exchanges taking place, it served to further strengthen these (Section 3.3). Given that MS have been traditionally reluctant to share information on CIP, it can be assumed that co-operation would not have occurred with the same frequency and depth in the absence of the Directive. MS would have had fewer occasions to meet, exchange good practices, and co-operate on more technical (and potentially quite sensitive) operational issues.

Moreover, during regular CIP PoC meetings, the EC and Agencies are provided with an opportunity to present legislative developments and other initiatives (including pilot projects and activities involving non-EU countries), while PoCs in turn may present their own national initiatives.[347] For this reason, it is fair to say that **the co-operation that came as a result of the Directive is pan-European in nature**. Prior to the Directive, the co-operation that existed took place within smaller groups of MS, interacting either bilaterally or multilaterally. To some extent, a more pan-European form of co-operation would certainly have been possible without the Directive. (After all, CIP Contact Points in all MS were created as part of EPCIP, not the Directive).[348] However, the Directive provided a much stronger legal basis and a specific role for CIP PoCs. This, in turn, created a self-sustaining forum for co-operation with a basis firmly grounded in a Directive rather than the political will of MS.

[344] Case study: 1 MS (PoC). Booz & Company GmbH. (2012). Study to support the preparation of the review of the Council Directive 2008/114/EC on the "identification and designation of European critical infrastructures (ECI) and the assessment of the need to improve their protection".
[345] Interview: 1 EC DGs and Agencies and 2 Academia and think tanks. Case study: 1 MS (PoC, Other Ministries).
[346] Survey: The Directive facilitated the development and exchange of good practices for 16 PoCs and 20 CI owners/operator, supported the emergence of a European forum for CIP-related issues for 14 PoCs and 15 CI owners/operators and supported the development of cross-border consultations and collaboration among CIP stakeholders for 11 PoCs and 15 CI owners/operators.
[347] Sample of CIP PoC meeting minutes provided by DG HOME (December 2010, February 2010, October 2011, February 2012, January 2013, July 2014, November 2014, February 2016, November 2016, May 2018).
[348] European Commission. (2006). Communication on a European Programme for Critical Infrastructure Protection. COM(2006) 786 final, Brussels.

6.6 Sustainability

EQ 6. Are the effects already achieved on account of the Directive likely to be long-lasting?

As shown in Section 6.3, the Directive had both direct and spill-over effects. The sustainability question[349] aims to assess whether and to what extent these effects are dependent on the continued existence of the Directive, or, put another way, whether the Directive's effects to date would persist in the event that the Directive was repealed and not replaced, while other EU and national initiatives were kept in place.

Generally speaking, **there is no consensus among stakeholders** on this question. In the case of both the online survey and the PC, stakeholders' opinions on the matter are mixed, highlighting both the negative and positive consequences of a hypothetical repeal.[350]

Direct effects

A repeal of the existing Directive would have partially negative consequences vis-à-vis its direct effects. One direct effect of the Directive was the **introduction of new provisions** in national legislation concerning ECI protection (see Section 6.3.1). **These provisions are likely to be maintained and no major legislative changes are expected in the event that the Directive were repealed**. This finding is based on the following considerations:

- Most MS have transposed the Directive; changing the relevant implementation measures that are now in place would entail an opportunity cost. In addition, some MS did not have national protection measures prior to the entry into force of the Directive that could be taken as a reference in case of a repeal;
- In many respects, MS had the opportunity to tailor the implementation of the Directive's provisions on the basis of existing national approaches. It follows that the hypothetical repeal of the Directive would not represent an incentive to amend national legislation;
- The degree of enforceability of the Directive is limited. Little oversight authority is provided to the EC for reasons of confidentiality. As such, considerable discretion is left to MS concerning the degree to which they implement the Directive.

The Directive also resulted in the **designation of some ECI and the implementation of specific requirements to ensure their protection** (see Section 6.3.1). **Repealing the Directive would have limited effects on the level of protection of ECI**, **given the fact that current national legislation is unlikely to be changed as a result**. While currently designated ECI would lose their "E" status in the event of repeal, the fact that national measures to protect ECI tend to be equivalent with those to protect NCI[351] means that designated ECI would likely retain the same level of protection.

Repealing the Directive would only have moderate effects, mainly **due to the limited number of designated ECI and the presence of partially overlapping sectoral EU legislation**. The number of designated ECI, while increasing in recent years, is still relatively small, with slightly less than half of the MS (ten) designating an ECI, and with a single country (BG) designating almost half of the total (*Finding 15*).

- In the *energy sector*, a repeal of the Directive and a change in national legislation would have a negative effect on the designated ECI according to CI owners/operators[352] (but not affect the protection of those CI that have not been designated as ECI). However, the EU sectoral

[349] Sustainability is in general used as a positive concept, referred to the durability of the effects once the intervention (typically a financial intervention) ends. In the context of the present study, sustainability is used in neutral terms, and is referred to the dependence of the effects of the Directive on the continuous existence of the Directive itself.
[350] Survey: 39% (N=9) of PoCs, 36% (N=5) of Other ministries, 70% (n=26) CI owners/operators consider that repealing the Directive would have either a negative or moderately negative effect on the protection of ECI in their country. PC: 32% (N=31) of respondents consider that in case of repeal of the Directive the effects would not be long-lasting.
[351] Case study: 2 MS (PoC, Other Ministries and CI owners/operators). Workshop: CI owners/operators. Interviews: 1 EU CI owners/operators.
[352] Survey: 67% (n=14) of CI owners/operators replied that repealing the Directive would have either a negative or moderately negative effect on ECI in their country. PC: 27% (N=15) of respondents think the effects would not remain or remain to a small extent and 33% (N=18) of respondents think that the effects of the Directive would be likely to remain to a fairly large and large extent.

legislation in the energy sector would continue to exist and would cover, at least to some extent, some of the obligations of the ECI Directive (Section 6.2.1.1).

- In the *transport sector*, meanwhile, a repeal of the Directive would arguably have more limited effects (as only 5 CI have been designated as ECI). Sectoral legislation, which imposes stricter security requirements (especially in maritime and aviation) would remain in place (Section 6.2.1.1). However, here too, stakeholder views on the matter vary.[353]

Moreover, EPCIP and relevant cross-sectoral legislation (e.g. the NIS Directive) developed after the introduction of the Directive would continue to exist, thereby continuing to contribute to CIP in different areas using different means. Particularly the NIS Directive imposes requirements concerning protective measures for providers of essential services, some of which presumably provide ICT services to CI.

The Directive also contributed to increased operational co-operation and information exchange between MS (see Section 6.3.1), for instance during the ECI identification process. Security generally and CIP specifically have traditionally been matters of national competence. The Directive established specific roles and procedures that have opened up communications channels between MS that were not in place before 2008. Furthermore, it 'elevated' the CIP issue to the ministerial level in many MS, thereby promoting inter-MS communication between MS on the topic.[354] The fact that the majority of MS entered into discussions with other MS concerning the cross-cutting criteria for ECI identification[355] shows that this communications channel has been used. **Repealing the Directive is likely to have a negative effect on cross-border co-operation and information exchange**, as MS, traditionally reluctant to share sensitive information, would have no incentive or obligation to do so.

Finally, the Directive introduced **reporting obligations on MS** (e.g. number and sectors of ECI, summary of risks, threats and vulnerabilities encountered), which could potentially serve to achieve common situational awareness on a pan-European level. This could hardly be achieved by MS alone, as they are in general reluctant to share sensitive information. While the extent to which any such situational awareness actually exists appears to be limited (Section 6.5), **repealing the Directive, and hence its reporting requirements, would entirely preclude this possibility.**

Spill-over effects

As shown in Section 6.3.3, the Directive has created a number of spill-over effects. For instance, it has increased awareness of and generated political momentum around CIP, while spurring co-operation of different kinds (between MS, between authorities at MS level, between competent authorities and private actors). This in turn has led to increased information/good practice exchange and fostered mutual trust and common understanding.

Such **spill-over effects would probably continue to exist within different frameworks in the absence of the Directive**. Such frameworks might include CIP PoC meetings (the basis for which would then be EPCIP), sectoral initiatives, the NIS Directive, and/or different activities organised by the JRC that aim to generate guidelines.

However, **these same frameworks might be weakened by a hypothetical repeal of the Directive insofar as they would lack certain momentum and a horizontal perspective** where they only focus on specific sectors or the scope of the NIS Directive, for example.

Moreover, **repealing the Directive might serve to convey a de-prioritisation of CIP at EU level**.[356] With the Directive, CIP is a European priority and gives legitimacy for CIP-related actions at national level.[357] Repealing the Directive without doing something else instead might be

[353] Survey: 67% (N=8) CI owners/operators consider that a repeal of the Directive would have a negative effect on the level of protection of ECI. PC: 38% (N=16) of respondents consider that effects of the Directive would not be long lasting or only to a small extent in case of a repeal and 26% (N=11) consider that effects would continue to fairly large or large extent.
[354] Case study: 1 MS (Other Ministry).
[355] Survey: 15 PoCs declared that their MS entered into discussions with other MS concerning the cross-cutting criteria for ECI identification.
[356] Workshop: repealing the Directive would send a wrong signal and would deprive CIP authorities of some legitimacy in the action they take vis-à-vis other national authorities (break-out gas pipelines).
[357] Case study: 1 MS (PoC, Other Ministries).

interpreted by MS to mean that CIP/the protection of ECI is no longer an EU priority. This, in turn, might potentially have negative consequences regarding various national initiatives.

In general, the Directive was part of an incremental trust-building process involving the MS and the EC.[358] The Directive has been the impetus for a range of activities, many of which have become more consolidated over time. At the same time, new initiatives, sectoral and more broad-based, have been developed. In the process, the effects of the Directive are less reliant on the Directive itself.

7 CONCLUSIONS

7.1 Relevance

Ten years after its entry into force, **the Directive appears today to have partial to limited relevance**, notably in view of recent **technological, economic, social, policy/political and environmental developments and current challenges.**

The increased interconnectedness of and interdependencies between sectors, and the transboundary nature of threats and the potential consequences of the disruption/destruction of CI illustrates the continued need for the EU to be involved in this policy area. Seen in this light, it also seems to confirm the continued relevance of the concept of ECI itself. However, the emergence of the concept of resilience in the EU policy discourse, the changing threat landscape, including the emergence of new threats, and ever-tighter linkages between the physical and cyber dimensions raise questions as to relevance of the current Directive and indeed point to the need for an update. The widespread adoption by MS of the minimum requirements introduced by the Directive and the appetite for further guidance on certain elements of CIP seem to suggest that this is the ideal moment to take a step forward in the EU's approach to CIP policy.

While the Directive is based on an all-hazards approach, it has only partial, and in some cases, limited, relevance to recent technological, economic, social, policy/political and environmental developments and current challenges. For instance, the limited sectoral scope of the Directive does not account for cross-sectoral interdependencies. Similarly, the Directive is only partially adapted to recent social change. For instance, it appears to be more relevant in addressing potential threats stemming from certain types of change (e.g. urbanisation) but not others (e.g. new and evolving technologies).

The Directive continues to contribute to **stated EU priorities**, including CIP. This is reflected in policy documents including the EU Internal Security Strategy (2015-2020) and the 2016 Joint Framework on countering hybrid threats. However, **the Directive does not reflect the revised EPCIP approach** that was adopted by the EC in 2013, and which placed a greater emphasis on **interdependencies** between CI, industry and state actors, as well as a notion of CI protection that incorporates **resilience** thinking.

The **objectives** of the Directive remain relevant considering that the threats to CI (from natural hazards, terrorism, cyberattacks, hybrid actions, insider threats, etc.) persist. The nature of these threats, which span beyond the sectoral scope of the Directive, and the increasing interconnectedness of CI across Europe and in third countries highlight the need for a common approach to protecting ECI, which the Directive sets out to achieve. While the objectives remain relevant, there is **room to clarify what 'a common approach' means** today. Any such effort must reflect the fact that views differ as to whether the common approach outlined in the Directive should be strategic and high level, or instead operational and detailed.

At a general level, the **definitions** contained in the Directive are relevant insofar as they provide a foundation for a common CIP framework, support the identification of both CI and ECI, and can be adapted to CIP-related goals in specific sectors. This flexibility is closely linked to the nature of the Directive, which gives the MS much more room to manoeuvre in how they implement the Directive at national level as compared with what any CIP-related Regulation might. In opting for a Directive over a Regulation, a balance was struck between the need for a legal basis in support of EU-level action and respect for the subsidiarity principle. In the Directive that the EC put forth,

[358] Ramboll. (2012). Study into the potential impacts of options amending council Directive 2008/114/EC. Interview: 2 EC DGs and Agencies.

terms such as 'CI' and 'ECI' were defined. This Evaluation finds that these definitions today **lack practical detail necessary for implementation** and, as a result, have resulted in different interpretations at MS level. This, in turn, has limited their ability to adopt a common approach. For the same reason, the Directive does not define certain specific terms, such as 'asset' and 'system', and does not provide any guidance on how to apply the principle of 'criticality'. Instead, this decision is left to the MS. The Directive's definitions of 'protection' and 'risk analysis' omit key concepts – principally that of 'resilience', which has become an important concept within CIP within the last 10 years. Finally, in focusing on 'CI located in MS', the ECI definition provided in the Directive fails to account for CI that have a pan-European dimension or that provide an EU-wide service (e.g. Eurocontrol, Galileo).

The limited **scope** of the Directive, which is restricted to the energy and transport sectors, means that it does **not fully account for growing cross-sectoral interdependencies**. The narrow scope also limits the relevance of the Directive in relation to some emerging threats (such as hybrid actions) which by their nature are cross-sectoral and involve sectors beyond those covered by the Directive. Furthermore, the application of protection measures to only two sectors makes the Directive misaligned with a range of national and EU policy developments that have taken place since 2008 (e.g. NIS Directive) and that affect a wide range of sectors. In particular, ICT and space (which includes ground-based and space-based infrastructure, and the services that are delivered via this infrastructure) have become increasingly important for CI. However, these sectors are not covered by the Directive. There is no consensus among stakeholders concerning which sectors besides energy and transport might be included in any broader replacement to the existing Directive, though ICT, water, finance, health and space have been raised as possibilities.

While the generic nature of the description of the **means of implementation** allowed the Directive to be 'accepted' and implemented by all MS in 2008, this level of generality does **not appear to be in line with the current situation** where all MS have to varying degrees integrated their respective national CIP frameworks with the elements contained in the Directive. Specifically, the bilateral and/or multilateral discussion format initiated by one MS to designate ECI does not represent the most relevant configuration for discussing cross-border CI, seeing as it does not allow for private sector involvement or a networked approach across multiple MS. Furthermore, the OSP and SLO descriptions lack detail, thereby limiting their relevance from an operational perspective. Similarly, the cross-cutting criteria for the identification and designation of ECI outlined in the Directive are broadly defined, meaning that they can be interpreted in different ways by different MS. Regarding the ECI identification process, the lack of explanation of key terms (e.g. 'essential service', 'availability of alternatives') limits the Directive's relevance but especially in the transport sector; the process is also seen to rely heavily on MS (rather than EC) initiative. Finally, Member States are obligated to provide data to the EC every two years on risks, threats and vulnerabilities. However, the data that the EC receives is limited, meaning that it is difficult to generate a pan-European situational picture concerning risks/threats/vulnerabilities to CI. Without this, it is difficult to develop additional European protective measures in support of the MS.

The Directive's **relevance in relation to stakeholders' needs is mixed**. While the Directive provides CI owners/operators, MS and the EC with an overarching framework for CIP, it currently leaves room for differences in application that have the potential to generate costs. However, the Directive lacks relevance insofar as it does not address the need for MS to coordinate with third countries or to engage in a multi-stakeholder approach to CIP. While none of the provisions contained in the Directive are seen to be altogether obsolete, some definitions and the description of some means of implementation could be made more specific and the concept of ECI more relevant, at least when compared with NCI.

Main issues identified

- The current 'ECI' definition lacks a perspective on networks and interdependencies and is ill suited in the case of CI with a pan-European dimension;
- The 'protection' definition does not account for resilience thinking;
- The definition of 'risk analysis' is not clear and omits details explaining how it should be carried out;
- The Directive is not aligned with the 2013 review of EPCIP, which adopts a systematic approach and accounts for resilience and interdependencies;
- The current scope of the Directive limits its relevance, given increased interdependencies across sectors including ICT and space;

- The lack of detail concerning how to account for 'cross-sector dependencies' makes the Directive of limited relevance given current threats and creates implementation challenges;
- Criteria for the identification of ECI are neither fully conducive to the creation of a common approach nor are they aligned with MS needs;
- The lack of guidance on how to assess the 'availability of alternatives' contributed to the limited identification of ECI in the transport sector specifically;
- The template for the biannual reports from the MS to the EC does not grant the EC with a sufficient level of granularity, not does it facilitate comparisons between the situations in different MS;
- The bilateral and/or multilateral meeting format for designating ECI is not conducive to private sector involvement or to a networked approach;
- The Directive does not reflect the existence of PPPs and focuses only on MS as the main actors involved in the identification and designation processes;
- The identification and designation process relies too heavily on the initiative of individual MS;
- The Directive lacks consideration of MS dependencies on third countries' CI and is therefore not fully relevant to current threats content

7.2 Coherence

The ECI Directive is part of a complex and highly fragmented policy framework, which includes rich sectoral legislation that either pre-dated the entry into force of the Directive or which has been introduced after the ECI Directive came into force.

Within this framework, **the ECI Directive appears to be broadly consistent** with relevant sectoral legislation, with no conflicting objectives or obligations. **However, its coherence is limited by the existence of several overlaps with other pieces of legislation and policy documents.** While acknowledging that it has not been possible to conclusively determine whether these overlaps brought about duplications or instead mutually reinforced each other, their very existence strongly suggests that there is room to streamline the EU's overarching CIP legislative framework.

When looking at the implementation of the different relevant pieces of legislation, the fragmentation of requirements and the existing overlaps seem not to have created significant problems and were not seen as a source of confusion to national public authorities and CI owners/operators. With the notable exception of the NIS Directive, public authorities and CI owners/operators did not report facing any major obstacles in addressing similar requirements originating from the different pieces of legislation; they generally found ways allowing for the various requirements to coexist operationally. The task of increasing the overall coherence of the various European initiatives falls to the EU level, and should be done with a view to laying the groundwork for a more integrated and synergistic intervention in this policy field at all levels.

At the EU level, the ECI Directive is partially coherent with the main CIP policy interventions in the energy and transport sectors. As for the **energy sector**, the ECI Directive partially complements and partially overlaps with sectoral legislation. This is true especially in relation to the objectives of the ECI Directive and those of the sectoral legislation, respectively. While the former aims at protecting CI, the latter aims at ensuring resilience and continuity of service. The lack of a clear-cut distinction between the interpretations of resilience and protection makes it difficult to assess to which extent the objectives are overlapping or complementary. What is more apparent is that the ECI Directive overlaps and complements with sectoral legislation concerning the object that is to be protected and certain requirements imposed on authorities. Finally, the ECI Directive complements existing rules and regulations insofar as it assigns specific obligations to operators.

Overlaps appear to be more significant in relation to the **transport sector legislation**. Specifically, the ECI Directive overlaps with aviation and maritime security legislation, but also with certain pieces of rail safety legislation and rail security measures.

The analysis also highlighted complementarities and to some extent overlaps between the ECI Directive and **the NIS Directive** in terms of both objectives and the object to be protected. The objective of the ECI Directive is to improve the protection of ECI defined as assets or systems, while the NIS Directive focuses only on a particular form of system (network and information systems). Thus, the ECI Directive overlaps with the NIS Directive in the (likely) event that ECI

contain network and information systems, but complements it as well, by putting in place protections on systems and assets that are not ICT-based. Therefore, the obligations imposed by the ECI Directive on operators overlap with those imposed by the NIS Directive in the event that designated ECI operators in the transport and energy sectors are also identified as being operators of essential services.

Looking at more operational aspects of the ECI Directive, the analysis shows that **the risk management measures included in the OSP and the threat assessment/risk analysis to be carried out by national authorities are likely to overlap with sectoral EU legislation**. Specifically, obligations on operators to draft an OSP featuring a risk analysis and to define risk management measures tend to overlap with similar measures contained in aviation, maritime, and rail safety legislation, but also rail security measures and the NIS Directive. Meanwhile, the obligation imposed on national authorities to conduct a threat assessment/risk analysis overlaps with similar obligations in energy, aviation, maritime, and rail security legislation as well as with obligations contained in the NIS Directive.

Moreover, synergies seem to be underexploited, both in the governance structure of the Directive and in the JRC's non-binding guidelines to support the application of the Directive, neither of which foresees formalised opportunities for the exchange of information. This is especially true in the energy sector, where most of the ECI have been designated.

At the international level, there is no comprehensive policy on CIP, though there are international standards and initiatives that apply to CI; **generally speaking, the ECI Directive is coherent with these.**

At the national level, existing overlaps between different pieces of EU legislation did not seem to generate significant duplications or confusion among public authorities and CI owners/operators. This might be because the Directive defines obligations in general terms, so as to be easily adaptable to different national contexts, but also for the fact that national authorities have successively adopted coordination mechanisms. In light of this, the ECI Directive appears to be coherent with national CIP policy interventions in the energy and transport sectors.

Concerns were only raised by stakeholders in relation to the implementation of the NIS Directive. The deadline for transposing this Directive has just recently passed. Therefore, it is not possible to assess at this time how the overlap that has been identified and that is described above has in fact been translated at the national level. Coming months will demonstrate if this overlap in fact created inconsistencies or duplications. As of now, though, the available evidence points to three possible ways in which the NIS Directive could fit into existing national CIP frameworks: as a parallel framework; as a complementary framework; or as a new and more comprehensive framework.

The wider EU CIP legislative framework (consisting of the Directive on one hand and other CIP sectoral legislation (in finance, space, health, but also cross-sectoral) on the other) **appears to be coherent, though there is room for improved synergies between the different elements**. The ECI Directive mainly complements other initiatives, and few overlaps can be found in relation to the operators' and authorities' obligations set out by the ECI Directive and those introduced by Seveso III and the Civil Protection Mechanism, respectively. However, the ECI Directive tends to run in parallel with other existing CIP initiatives, a fact which highlights unexploited synergies and points to the need for a more holistic CIP approach. This is particularly true in the space sector.

Limited integration between CIP measures at EU level does not seem to be reflected at the national level where protection measures applied in different sectors coexist. Most of the national CIP frameworks already cover additional sectors to the energy and transport sectors (the scope of the Directive), and some MS have put in place national coordination practices or cross-sectoral CIP oversight bodies.

Main issues identified

- Synergies among the different components of the wider EU CIP legislative framework have been somewhat under-exploited;
- There are a number of overlaps between the ECI Directive and sectoral legislation in the transport and energy sectors;

- Overlaps with legislation in the energy sector are due to the lack of clear-cut distinction between protection as defined in the ECI Directive and resilience/security of supply;
- Directive provisions on risk analysis and risk management for operators overlap with similar measures in the aviation, maritime, rail safety legislation and rail security measures, and to lower extent with the NIS Directive;
- Directive provisions on threat assessment/risk analysis for national authorities overlap with similar obligations in the energy, aviation, maritime, rail security legislation and to lower extent in the NIS Directive;
- Synergies between different legislative sources in the energy and transport have been under-exploited, looking in particular at risk analysis and risk management. This is especially true in the energy sector, where most of the ECI have been designated;
- The ECI Directive overlaps with the NIS Directive insofar as network and information systems may be considered ECI;
- Synergies between the different components of the wider EU CIP legislative framework (covering also finance, space, health legislation and cross-sectoral measures) have also been under-exploited and there is potential for misalignment with norms in the space sector.

7.3 Effectiveness

The Directive has been partially effective in achieving its stated objectives. Specifically, **the Directive has partially achieved the objective of establishing a common procedure for the identification and designation of ECI**. On one hand, the Directive has indeed introduced elements of a common framework and for the first time established a procedure for the identification and designation of ECI. Specifically:

- It introduced a definition of CI that is now in place in all MS. (As a point of comparison, only nine MS had a formal CI definition before the Directive was introduced.);
- It introduced a procedure for the identification of ECI that is shared by all MS and that all MS have at least initiated;
- It ensured that CI in the energy and transport sectors were covered by such a procedure; and,
- It created requirements for the MS to designate CIP PoCs tasked with coordination within individual MS, between MS, and between MS and the EC.

On the other hand, the Directive has been less effective in making this procedure something that is truly common across all MS, or in creating a harmonised framework, as demonstrated by the small number of designated ECI.[359] While acknowledging that this is partly the result of the choice made in 2008 to adopt a Directive, thereby giving the MS considerable leeway as to how they should operationalise its provisions, evidence collected over the course of this study points to differences that reduce the actual level of commonality of the procedure adopted. The definitions contained in the Directive, but especially the definition of CI, are vaguely formulated, thereby leaving room for different interpretations and limiting the Directive's harmonising power. The identification process presented difficulties mainly in relation to the application of the transboundary criterion and in reaching agreement with other MS. In most instances, the inability to reach agreement was due to different perceptions of risk, different attitudes towards co-operation, and fragmented CIP administrative arrangements at national level. Assessing the designation process as part of this study has been complicated; although no specific difficulties have been identified, it is something of a black box due to the sensitivity of the subject matter.

The Directive has to a limited degree achieved the objective of establishing a common approach to the assessment of the need to improve the protection of ECI. The Directive has been effective in making sure that all MS have in place an OSP and a SLO for all designated ECI, and that all MS with ECI produce regular reports to the EC. The EC has supported the implementation of the Directive in terms of sharing good practices and methodologies, providing training, and exchanging information. However, operators in most MS already had in place measures equivalent to the SLO and OSP prior to the adoption of the Directive. As such, the impact of the Directive has been mainly in formalising already existing measures rather than contributing to the creation of any new, more common approach. As for the SLO function, this is a key role in

[359] Of which 88 out of 93 in the energy sector.

implementing a common approach to the assessment of risks at the operational level. However, the existing differences in terms of competences, roles and background are likely to result in different practices in different MS and in relation to different ECI. Similarly, the generality of Annex II of the Directive describing the OSP, taken together with the non-binding nature of the JRC's guidelines, left considerable room for different methodologies. Meanwhile, the reporting requirement is used solely for compliance purposes. Moreover, the generality of the common template that MS need to follow for their biannual reports on risks, threats and vulnerabilities for the designated ECI sectors to the EC, combined with the reluctance of the MS to share sensitive information, has limited the effectiveness of this provision, which might have been useful in generating an EU-wide situational picture of the situation facing ECI and what additional action might be taken to further enhance their protection.

Some of the obstacles in implementing the Directive stem from the Directive itself. Besides the generality of key provisions and definitions, the Directive lacks a *monitoring and evaluation framework* and *dedicated funding* to support its implementation. Currently the EC has a limited overview of the implementation of different provisions and lacks instruments to follow up on their implementation. A monitoring and evaluation framework would allow the EC to monitor more closely the application of the Directive and the MS to prove *whether* and *how* they have complied with it, and would provide an evidence base for future decision-making. As for the funding issue, even though EU funding streams for CIP are available (e.g. ISF – the successor of CIPS in the current Multiannual Financial Framework (MFF) and Horizon 2020), they do not appear to be particularly visible to stakeholders, while the results of projects are not systematically communicated within the CIP community. Dedicated CIP funding would support national authorities and operators facing specific challenges in making security-related investments.

Other obstacles are external to the Directive. In almost half of the MS, the Directive had to find its place within *national CIP frameworks that were already partially or fully formed*. This has limited the uptake of the Directive. Meanwhile, the absence of pre-existing CIP frameworks proved, generally speaking, to be a catalysing factor for MS to designate ECI. However, this has not been enough to prompt a wide-ranging effort across Europe to designate ECI. Indeed, almost half of the MS that lacked a fully-fledged CIP framework prior to the Directive entering into force have yet to designate an ECI. This suggests that *appetite* at the national level for an EU intervention in this policy area is another important factor to consider when looking at the implementation of the Directive, the absence of which may have played a role in limiting its implementation across the Union. This is also supported by the fact that the distribution of ECI does not seem to reflect the distribution of CI with particular EU relevance. Finally, *the reluctance of MS to share sensitive information with security implications* has also limited the extent to which the Directive has been implemented.

It is not possible to isolate the contribution of the Directive from that of other factors regarding the achievement of its objectives. Given that the identity of designated ECI in the MS are not disclosed, it is impossible to compare their respective levels of protection with that of NCI, which are not subject to obligations provided by the Directive. Rather, levels of protection in the case of NCI are impacted by other factors, including national legislative initiatives/measures, voluntary actions on the part of CI operators, EU initiatives besides the Directive, but also various intergovernmental initiatives.

The Directive has been particularly effective in bringing about effects that went beyond its intended objectives, i.e. spill-over effects. Even though the number of designated ECI might appear limited (93) and concerns only 10 out of 28 MS, the Directive generated awareness of and political momentum around the protection of CI in general, and not just in relation to ECI in the energy and transport sectors. Spill-over effects such this were witnessed in almost all MS, regardless of whether they ultimately designated any ECI, and impacted all relevant stakeholders.

In the case of MS that either had no pre-existing CIP framework or where it was only partially developed, the Directive prompted efforts to put in place dedicated national-level CIP legislation, definitions of CI, and obligations to carry out threat assessments. In some MS (e.g. ES, RO, BE), the Directive led for the first time to the creation of wide-ranging national CIP frameworks and (in the cases of particularly ES and RO) dedicated national CIP agencies. In MS where a full or partial CIP framework was already present, the Directive generated additional political momentum that

served to heighten CIP awareness and saw the formalisation of some heretofore informal CIP practices.

The Directive, both directly and indirectly via various CIP activities that it spurred, can be said to have contributed to the deepening of co-operation both between and within MS, and in some cases between MS and third countries. While the vast majority of MS already had in place various forms of bi- and multi-lateral co-operation, the frequency and depth of these contacts increased in almost all cases after the introduction of the Directive. Similarly, co-operation increased within MS, both between different national authorities and between authorities and operators. Moreover, authorities from third countries liaised with some MS to transfer to their countries specific CIP frameworks that had been developed as a result of the adoption of the Directive. Finally, in some MS, the existence of the ECI Directive supported the transposition of the NIS Directive thanks to already enhanced co-operation between and within MS, as well as the exploitation of national-level expertise that had been nurtured in the process of fulfilling the obligations derived from the Directive.

The Directive has primarily been effective in enhancing the protection of CI with EU relevance through associated spill-over effects. The specific objectives of the Directive helped support the general objective of increasing the protection of CI with EU relevance, or what the Directive defined as ECI; a specific procedure was put forth to help the MS identify and designate these infrastructures. However, as the Directive's specific objectives have been only partially achieved, the contribution of the Directive in enhancing the protection of CI with EU relevance occurred mainly through the political momentum that the Directive spurred concerning CIP, and which brought new energy to efforts aimed at further developing/refining national CIP frameworks.

Generally speaking, the assessment of the contribution of the Directive to the overall objective of an improved level of protection of CI with EU relevance is inconclusive. On one hand, the creation of or further strengthening of national CIP frameworks in half of the MS, as well as similarities between the EU and national requirements concerning the protection of ECI and CI, respectively, seems to suggest that those CI with European relevance are protected in equal measure, no matter if they are designated as ECI or not. While this could be seen as proof that the Directive's overall objective has been achieved,[360] available evidence does demonstrate that requirements for both CI and ECI protection do vary from one MS to another. Therefore, the possibility that actual levels of protection vary as well cannot be excluded. For this reason, it is worth considering whether common European procedures and a common European framework are in fact necessary in achieving high levels of protection across MS in different parts of the EU. An in-depth assessment of the measures included in individual OSPs (which are typically classified) would be needed in order to generate more insights on this and other related questions.

Main issues identified

- Differences in the SLOs' competence, role and background limit their contribution to the achievement of common approach and do not address challenges in sharing sensitive data;
- Differences in the content of different CI operators' OSPs limited the ability to achieve a common level of protection;
- The different interpretations of CI by MS might challenge the existence of a common starting point for the identification process;
- National biannual reports to the EC on risks, threats and vulnerabilities are of limited utility in assessing the need for additional protection measures;
- The security of the current channels used to communicate biannual reports to the EC are not commensurate with the information being requested;
- The lack of a sectoral view on the part of PoCs limits the exchange of information between MS and the fostering of mutual trust;
- National governance arrangements lack clarity;
- Different national authorities have different attitudes towards co-operation. This affects the identification process;
- Presence of a CIP framework prior to the adoption of the Directive and a lack of appetite at MS level have reduced the uptake of the Directive;

[360] PC: in the energy sector, 78% (N=45) of respondents see an increase in the level of protection of CI in the EU in the last decade, with 54% (N=25) considering this level increased to a fairly large and large extent; in the transport sector, 67% (N=29) of respondents see an increase in the level of protection of CI in the EU in the last decade, with 50% (N=17) considering this level as increased to a fairly large and large extent.

- The EC has a limited overview on the implementation of different provisions contained in the ECI Directive;
- The EC lacks instruments with which to follow up on the implementation of the Directive;
- Limited awareness of the available sources of funding to support the implementation of the Directive. In addition, available sources of funding are not visible enough;
- Results of EU-funded projects are not systematically communicated within the CIP community.

7.4 Efficiency

There is no conclusive evidence that the results attributed to the ECI Directive have been achieved at a reasonable cost.

The introduction of the Directive put in place a set of obligations pertaining to MS authorities and, to a lesser degree, CI owners/operators. Meeting these obligations entailed certain costs (mainly compliance and administrative costs). However, the actual amount of these costs remains unknown and the lack of hard data precludes the drawing of robust conclusions concerning the efficiency of the Directive.

On one hand the scale of costs brought by the Directive appears limited. Firstly, costs seem to have a limited incidence. This is due, *inter alia*, to the fact that most of the obligations introduced by the Directive pre-dated the entry into force of the Directive in several MS, but also that similar requirements were included in certain pieces of sectoral legislation. For instance, costs relating to the drafting of the OSP and the identification of a SLO were likely already borne prior to 2008 in consideration of pre-existing equivalent practices. Moreover, the designation of CIP PoCs also took place earlier, as part of the implementation of EPCIP in 2006. Finally, the costs associated with the identification and designation of ECI are apparent in certain instances. Given that measures to identify and protect CI were taken prior to the ECI Directive in around half of MS, the only new costs that the Directive entailed related to the obligation to inform the EC about the designation of ECI, and subsequent regular reporting of data on risks, threats and vulnerabilities per ECI sectors.

In addition, most of the costs associated with the implementation of the Directive only become material when an ECI is designated, which occurred in a limited number of cases and in a relatively small number of MS; stakeholders tend to agree on the fact that these costs represent a minor share of the overall budget allocated to the protection of CI.

On the other hand, the lack of quantifiable data prevents making a sound assessment of the regulatory burden brought by the Directive; stakeholders' views on the proportionality of the costs in relation to observable results is mixed.

Besides certain costs associated with the implementation of the specific requirements of the Directive, **a number of other factors were seen to have affected the overall efficiency** of the Directive, some which are inherently linked to the Directive and others that are external to it. The generality of the provisions contained in the Directive allowed MS to adapt existing national approaches without needing to create completely new procedures. This minimised some of the costs associated with transposition. At the same time, the lack of details concerning some provisions (such as the risk assessment requirement) generated costs, but especially where national CIP frameworks did not exist or were only partially developed prior to 2008. As for external factors, differences in how MS chose to implement some of the provisions of the Directive brought additional costs for operators with a presence in multiple MS. For instance, despite the fact that all MS that have designated ECI require ECI operators to adopt an OSP, the specific content and scope of these documents vary from one MS to another, thus generating certain information costs for operators and hinders to their business. The "opportunity cost" of not harmonising provisions such as this must therefore be taken into consideration.

Main issues identified

- The generality of the Directive's provisions created some costs for MS, especially where the CIP framework was poorly developed before 2008;
- Differences across MS concerning OSP content entailed costs for CI operators with a presence in multiple MS.

7.5 EU added value

The Evaluation found that the ECI Directive **generated some EU added value** insofar as it achieved results that national or other EU initiatives would not otherwise have achieved, as well as results that national or other EU initiatives would have achieved anyway, albeit through longer, costlier and less well-defined processes.

Firstly, the ECI Directive brought about EU added value by **paving the way for the creation of a common framework for the protection of ECI**. In a context of highly diversified approaches to CIP and different degrees of national programme maturity, the Directive managed in the not insignificant task of introducing a **common European vocabulary**, which is arguably a key prerequisite for effective cross-border dialogue and mutual understanding. As a case in point, the Directive introduced (for the first time in the EU legislative framework) a common definition of CI and minimum requirements for ensuring the protection of a specific type of CI (ECI). As a result, most MS now have specific national legislative measures providing for ECI protection, specific ministries responsible for CIP, and PoCs responsible for liaising with other MS on CIP-related matters. This is a result that MS would not likely have achieved on their own.

However, **the potential EU added value that may derive from this achievement is limited by the current high degree of heterogeneity** as to how different MS interpret these definitions and the procedures laid down by the Directive.

Moreover, **the EU added value of the Directive, especially in terms of its contribution in creating a common framework, is perceived differently by different MS**. Indeed, the Directive's added value is perceived as strong in the MS that saw in the Directive an opportunity to introduce a more comprehensive CIP framework, but is considered as being weaker in those MS that already had a proven CIP framework in place. In the latter instances, MS encountered difficulties in discerning between the requirements of the Directive with those already in place at national level.

Specifically, **the OSP, SLO and reporting requirements proved to have limited EU added value**. In the case of the OSP and the SLO, the Evaluation finds that a lack of granularity in terms of content left many MS feeling that these provisions were similar to national practices that were already in place and more thoroughly articulated. As for the obligation for MS to report to the EC, EU added value is limited by the fact that the EC did not more systematically exploit the data that was received in order to develop EU-wide knowledge or a situational picture concerning threats/risks to CIP. Such information would arguably have been useful in informing policy decisions at both national and European level.

In an increasingly interconnected Europe, where sectors are interdependent and geographical borders are of less practical importance than in decades past, systems as a whole are only as strong as their weakest link. Seen in this way, the adoption of new measures by only a limited number of MS appears to be outweighed by the security benefits generated for the EU as a whole, i.e. the reduction to some extent of the exposure of the EU to risks related to the transboundary effects caused by the disruption or destruction of CI located in MS that heretofore had taken few if any CIP measures.

Additionally, the Directive acted as a catalyst for change by generating political momentum concerning CIP and speeding up national decision-making processes and strengthening co-operation between MS. This result is closely linked to its binding nature. For instance, the creation of EPCIP in 2006 signalled the importance of CIP at the EU level and for the first time provided MS with a platform for the exchange of information, common practices and experiences. The availability of EU funding could also have supported initiatives in these areas. However, achieving the same results as those that can be attributed to the Directive would arguably have required more time, more coordinating efforts and more appetite at the national level. The Directive thus created both the impetus and a legal basis for the implementation of certain CIP actions, but also for the creation of a self-sustaining forum for co-operation that is not subject to political wills and agendas at national level.

The Directive can be seen as a step forward that served to underscore the fact that CIP was a priority at EU level. Simply put, the Directive "elevated" the discourse at the EU level, and made the argument that CI disruptions/failures in one MS could have cross-border

implications. This renewed interest in CIP trickled down to the national level in both those MS where there were no or only partial CIP frameworks in place as well as MS where robust CIP programmes already existed. In the first case, the Directive saw the introduction of specific legislation on CIP and in some cases (e.g. ES, RO) the development of a comprehensive approach with dedicated CIP agencies. In the second case, the Directive steered existing national CIP practices towards a more all-hazards approach (e.g. FR) and improved cross-border discussions by raising CIP awareness within all EU MS.

Moreover, the ECI Directive **triggered the creation of cross-border dialogue and operational co-operation** in a field that was traditionally viewed as the exclusive competence of the MS prior to 2008. Numerous provisions in the Directive (e.g. the procedures for discussing cross-cutting criteria in the identification process, the appointment of CIP PoCs, the organisation of regular meetings) contributed to processes generating mutual understanding and trust between MS (but that was already underway thanks to EPCIP). Taken together, these elements served to address the reluctance of MS to share information on CIP while at the same time increasing the frequency of opportunities for exchange. The MS were provided with a platform for discussion and for learning from one another, something that in the absence of the Directive would have taken more time and resources.

Whilst acknowledging that the Directive brought some EU added and achieved an improved situation compared to the one that would have resulted from the action of MS independently, any future decision concerning the Directive should adequately account of the fact that this piece of legislation in its current form now has limited EU added value compared to national practices and should draw on an assessment of the continuous need for a common approach.

Main issues identified

- Limited EU added value perceived by those MS with a CIP framework already in place prior to 2008;
- Most MS see limited EU added value in the OSP and the SLO descriptions provided in the Directive;
- The reporting requirement did not generate EU-wide knowledge on CIP threats and risks. Rather, it is used mainly for compliance purposes and therefore is of limited EU added value.

7.6 Sustainability

The Directive was part of a trust-building exercise that began with EPCIP in 2006 and continued via a number of incremental steps. The Directive has been the impetus for a range of activities, many of which have become more consolidated over time. At the same time, new initiatives, sectoral and more broad-based, have been developed. In the process, the effects of the Directive are less reliant on the Directive itself.

Overall, **several effects generated by the Directive are likely to be long-lasting and would continue to exist in the event that the Directive was repealed and not replaced**. Specifically, CIP-related spill-over effects brought about as a result of the Directive are likely to persist within different frameworks. These include regular CIP PoC meetings, sectoral initiatives, discussions related to the implementation of the NIS Directive (in light of the fact that the ECI Directive provided the foundation for the implementation of the NIS Directive in some MS), and JRC-organised activities, all of which provide venues for discussion, co-operation, awareness-raising and continued trust-building in the context of CIP. Similarly, some effects that directly stemmed from the implementation of the Directive can be considered now to be deeply rooted in most national practices and not subject to significant change were the Directive to be repealed. Those provisions that were adopted by MS in order to implement the Directive (e.g. more robust legislation, national CIP frameworks, dedicated CIP agencies) are likely to be maintained and indeed constitute one of the key legacies in the event of hypothetical repeal. Even where national legislation is altered as a result of repeal, the effects in terms of CIP protection would be limited, given the limited number of designated ECI across Europe and the existence of different pieces of partly overlapping sectoral EU legislation with similar requirements.

On the other hand, **some of the direct effects achieved by the implementation of the Directive would likely cease to be felt**. For instance, this would likely be the case regarding

operational co-operation and exchange of information between MS. As mentioned elsewhere, MS have historically been reluctant to share sensitive information relating to national security with one another. The Directive created a platform for exchange of if not sensitive than at least more information than previously was the case. Repealing the Directive is likely to have negative effects on intra-EU information sharing. Similarly, the flow of information from MS to the EC initiated thanks to the Directive's reporting requirement would also be interrupted in the event of repeal. While the EC has been found to have made limited use of this information in creating a pan-European view on CI threats, risks and vulnerabilities, repeal would further limit such a possibility in the future.

Just as the benefit of the Directive is not equally shared or experienced across the EU, there is no consensus among stakeholders as to whether or not the legislation should be repealed. While in principle the Directive appears to be an important cornerstone of European CIP policy, the changes in the policy context that have taken place over the past 10 years have reduced the Directive's relevance and highlighted the need for improvement. The negative effects resulting from a hypothetical repeal would likely outweigh any benefits. For instance, repealing the Directive would send the signal that the protection of ECI is no longer an EU priority, and might engender actions at MS level that could reduce the sustainability of the results achieved.

8 RECOMMENDATIONS

The findings of this Evaluation highlight the fact that while **some elements of the ECI Directive remain useful, others are of limited value today and could be improved**.

The analysis shows that **the context that today frames the implementation of the Directive has dramatically changed when compared to the situation in 2008**. The rise of the concept of resilience over protection, the cross-border and cross-sectoral nature of both new and evolving security threats (some of which are exacerbated by climate change-related risks), the progressive refinement of sectoral legislation and the introduction of the first Directive addressing specific types of national CI (the NIS Directive), the increasing penetration of the digital and cyber dimension in the functioning of CI, the increased involvement of the private sector in the debate around CIP and their distinctive knowledge of recent technological advancements, the acknowledgement that the security of EU citizens passes also through the protection measures applied by non-EU neighbours and third countries are among the primary developments that define the new context in which CIP is managed. In this view, the need for a broader perspective on the protection of CI, to exploit potential synergies and to facilitate the exchange of information at multiple levels appears quite clear.

Several options are identifiable that might contribute to the achievement of these aims.

The recommendations that follow pertain to the existing Directive and aim to improve the relevance of the Directive's existing provisions to current and emerging needs, while at the same time respecting the principle of subsidiarity (leaving the MS with primary responsibility for CIP). However, the recommendations also address certain elements (e.g. CIP governance, national practices, EU funding, EU legislative framework and relationship with third countries) that are external to the Directive, but that also might contribute in enhancing the existing Directive's overall effectiveness.

At the same time, **the evidence that has been collected over the course of the Evaluation does not exclude *ex-ante* more radical options for change.** However, these options can only be properly assessed in the context of an extensive impact assessment. Some key questions may steer such an exercise. Should the Directive be seen as a strategic document setting out high-level principles for CIP or should it instead serve as an operational document detailing how MS might practically assess risk and protect ECI? Should the Directive remain a separate piece of legislation or should it be integrated into other existing pieces of legislation? Should the Directive keep a sectoral scope or should it be replaced with something more cross-sectoral in nature? Should MS create national CIP agencies or should CIP-related competences instead be strengthened at EU level alongside appropriate mechanisms to encourage knowledge-sharing?

This Section presents a range of recommendations relating only to the existing Directive, each of which is accompanied by specific actions that could be taken by specific stakeholders. Some recommendations involve actions that might be taken by the EC, while others foresee a shared

and common effort involving Member States, the EC and/or other relevant stakeholders. When drafting the recommendations, their potential impact on the achievement of the objectives, their relevance to stakeholder needs and emerging challenges, and their feasibility have been duly accounted for with the aim of suggesting actions that could effectively address the identified problems, contribute to making the Directive's provisions more suitable to the current context, and eventually applicable by stakeholders.

As already highlighted throughout the analysis, CIP has historically been a distinctive national competence. When the Directive was first introduced, the reluctance of some MS towards EU action in this field prompted the narrowing down of the scope of the Commission's ambitious original proposal. Stakeholders' views on the hypothetical repeal of the Directive are mixed and it might be assumed that, at least for MS that see merit in keeping the Directive,[361] there is support for a continued role for the EC in this policy field. Together with the widespread interest among MS in clarifying certain aspects of the Directive and obtaining clearer guidance, alongside the recent introduction of the NIS Directive, this finding suggests that the attitude of MS towards the role of the EC has evolved somewhat. That being said, there are still some MS that highlight the relevance of national sovereignty in the field of national security, which in many MS includes CIP. In this view, any measure that the EC might decide to put forward will need to be carefully assessed against the principle of subsidiarity and provide clear EU added value to MS.

Table 12provides a summary of the suggested recommendations, along with an indication as to the issues that they seek to address. Subsequent Sections provide detailed descriptions of each recommendation, starting with those that address specific issues related to the Directive, followed by those addressing other more general, but still relevant issues.

Table 12 - Overview of recommendations

N.	Directive provisions	Focus of the issues	Recommendation
1	Definitions; Identification and designation; OSP SLO; Reporting	ECI Directive	Further define key **terms and provisions** contained in the Directive in order to improve its operationalisation at the national level while at the same time maintaining its strategic focus
2	Scope	ECI Directive	Assess the opportunity to extend the sectoral **scope** of the Directive
3	Reporting	ECI Directive	Strengthen the **monitoring and evaluation** framework in order to support future decision-making processes
4	Identification and designation; Reporting	CIP governance system	Re-balance **roles and responsibilities** assigned to the various stakeholders involved in the identification and designation of ECI
5	CIP PoC; Definitions	National practices	Address the key **differences** in national CIP frameworks that affect the identification of ECI
6		EU funding	Strengthen the link between the requirements of the ECI Directive and the available sources of **funding** at the EU level
7	Scope and definitions; Identification and designation; OSP SLO; Reporting	EU legislative framework	Streamline the EU CIP legislative framework and trigger **synergies** at the national level
8		Third countries	Facilitate the exchange of information and co-operation with **third countries**

1. Further define key terms and provisions contained in the Directive in order to improve its operationalisation at the national level while at the same time maintaining its strategic focus

Ten actions are proposed in order to implement this recommendation.

[361] Survey: 45% (N=9) of PoCs consider a repeal of the Directive would have a negative impact on the level of ECI protection in their country. Case study: 3 MS (PoCs and Other ministries).

Issue(s) addressed	Actions	Addressees
• The current 'ECI' definition lacks a perspective on networks and interdependencies and is ill suited in the case of CI with a pan-European dimension.	1.1 Better articulate the "E" factor of ECI and specify their minimum requirements	EC MS JRC
• The 'protection' definition does not account for resilience thinking. • The Directive is not aligned with the 2013 review of EPCIP, which adopts a systematic approach and accounts for resilience. • There are overlaps with legislation in the energy sector. This is due to the lack of clear-cut distinction between protection as defined in the ECI Directive and resilience/security of supply.	1.2 Refine the definition of 'protection' so as to include/account for the concept of resilience and its current use in relevant sectoral legislation	EC
• The definition of 'risk analysis' is not clear and omits details explaining how it should be carried out. • JRC risk assessment guidelines are considered to be relatively complex.	1.3 Set minimum elements to be covered when performing the risk analysis, and review the JRC risk assessment guidelines	EC CI operators JRC
• The Directive is not aligned with the 2013 review of EPCIP, which recognises interdependencies. • The lack of detail concerning how to account for 'cross-sector dependencies' makes the Directive of limited relevance given current threats and creates implementation challenges.	1.4 Develop criteria and methodologies to be used during the identification process so as to assess 'cross sector dependencies'	EC JRC
• Criteria for the identification of ECI are neither fully conducive to the creation of a common approach nor are they aligned with MS needs. • Limited EU added value perceived by those MS with a CIP framework already in place prior to 2008.	1.5 Set minimum criteria for the identification process	EC MS
• The lack of guidance on how to assess the 'availability of alternatives' contributed to the limited identification of ECI in the transport sector specifically.	1.6 Provide guidelines so as to assess the 'availability of alternatives'	EC MS
• Differences in the content of different CI operators' OSPs limited the ability to achieve a common level of protection • Differences across MS concerning OSP content entailed costs for CI operators with a presence in multiple MS. • Most MS see limited EU added value in the OSP description provided in the Directive.	1.7 Specify in more detail the minimum content that OSPs should include	EC CI operators JRC
• Differences in the SLOs' competence, role and background limit their contribution to the achievement of common approach and do not address challenges in sharing sensitive data.	1.8 Develop a competency framework for the SLO function	EC MS CI operators JRC
• Most of the MS see limited EU added value in the SLO description provided in the Directive.	1.9 Organise training sessions for security officers in relation to ECI and NCI	EC CI operators JRC
• The template for the biannual reports from the MS to the EC does not grant the EC with a sufficient level of granularity, not does it facilitate comparisons between the situations in different MS. • The security of the current channels used to communicate biannual reports to the EC are not commensurate with the information being requested.	1.10 Revise the template for the biannual report by the MS to the EC on risks, threats and vulnerabilities	EC MS JRC

The Evaluation found that there is interest on the part of MS authorities and CI owners/operators in obtaining a greater level of detail concerning some definitions and provisions contained in the Directive. The ambiguity of certain terms and the vagueness of some requirements has resulted in heterogeneous and in some cases difficult implementation processes, limited the added value of the Directive when compared with national CIP measures, and created room for different views on risk. Taken together, these issues have been shown to limit the effectiveness of the Directive's approach to identifying and designating ECI. While in 2008 the generality of the provisions allowed the Directive to be swiftly integrated into existing national CIP frameworks, the data suggests that

this same generality created some implementation challenges and limited the Directive's relevance to stakeholders' needs over time.

At the same time, the strategic nature of the Directive and the subsequent generality of some of its provisions allowed the MS the flexibility and adaptability necessary to transpose the Directive to their national contexts. This aspect of the Directive is keenly appreciated by stakeholders. In respecting subsidiarity, the Directive provides the legal basis for an EU intervention that both acknowledges the MS' primacy on CIP and creates a space for European action targeting infrastructures that, where vulnerable, risk cross-border disruptions.

Seen in this light, this recommendation entails revising the Directive in ways that clarify key terms and provisions, while at the same time ensuring that national CIP stakeholders retain enough freedom so as to permit adjustments to national practices and to avoid unnecessary burden. Any such discussion on a revised Directive would benefit from focused examination of the more detailed NIS Directive.

1.1 Better articulate the "E" factor of ECI and specify their minimum requirements

In order both to more clearly define the European nature (the "E" factor) of CI that might be subject to the Directive and to provide improved guidance to MS engaged in such processes, the EC may consider modifying the definition of ECI in the following ways:

- Inclusion of a reference to infrastructures that are located in several MS and whose functioning depends on the initiative of all MS concerned (e.g. Galileo, Eurocontrol and the electricity and gas transmission networks);
- Inclusion of infrastructures that are not physically located in a given MS, but whose disruption or destruction may affect one or more MS;
- Introduction of minimum thresholds for certain sectoral and cross-cutting criteria that would qualify a given CI as being an ECI; and
- A more detailed description of the meaning of "cross-sector dependencies".

The amendments listed above, and especially the minimum thresholds and the definition of cross-sector dependencies, could be developed by the EC with the support of national experts (engaged, for instance, via ERNCIP or an ad hoc group of experts designated by MS) along with the JRC. This process could start with a mapping of the various criteria and related thresholds currently being used in the different national CIP frameworks. This would allow the EC to design relevant binding requirements; uptake by MS would be facilitated due to the fact that revised definitions and criteria would be based on existing practice at MS level. However, as this study has shown repeatedly, such criteria/thresholds can be sensitive information in certain MS that is often classified. For this reason, any such effort involving the MS should be conducted with an adequate level of confidentiality.

If taken together with the proposed actions concerning methodologies to perform risk analysis (recommended action 1.3) and cross-sector dependencies (recommended action 1.4), this could help in reducing the extent of differences in how different MS interpret the ECI Directive's definitions and procedures. This action should also ensure a better accounting of interdependencies and provide clearer indications as to CI that merit an ECI designation.

1.2 Refine the definition of 'protection' so as to include/account for the concept of resilience and its current use in relevant sectoral legislation

Considering the distinctive elements of the Directive and the EU added value it brought to MS, it is recommended that the EC clarify the Directive's scope of action by both refining the definition of 'protection' and more clearly explaining the relationship between 'protection' and 'resilience'. Drawing on the outcome of the discussions that DG HOME should hold with other DGs (see recommended action 7.1), there would be value in the EC clarifying the need for MS and CI owners/operators to consider measures implemented in compliance with sectoral legislation where an overlap cannot be avoided, this in order to avoid duplication of efforts or inconsistencies.

1.3 Set minimum elements to be covered when performing the risk analysis, and review the JRC risk assessment guidelines

The EC may consider setting minimum elements that need to be considered when carrying out the risk analysis, while at the same time leaving MS and operators with the freedom to develop specific methodologies best suited to their specific contexts. Such is the case in other EU sectoral legislation. The EC may consider first conducting a comparative analysis of the content and structure of existing sectoral risk analyses/methodologies. The EC could investigate the various risk analysis practices that have been implemented in compliance with EU sectoral legislation, but especially where there is demonstrated overlap between this legislation and the ECI Directive. Based on this preliminary mapping, the EC could then discuss the issue with European associations of CI owners/operators, the aim being to generate a comprehensive overview of what typically falls within the scope of the risk analysis exercise. This effort on the part of the EC should provide enough detail in order to identify the essential minimum elements as part of the risk analysis involving ECI.

As with the other actions included as part of this recommendation, it is important for the actual adoption of these minimum elements that MS are involved in the design from the outset so as to ensure that the measures are considered relevant for and applicable to the different national frameworks.

In order to further support MS and operators, the JRC might also consider revising the current guidelines on risk assessment methodologies for CIP, which many CIP stakeholders consulted as part of this Evaluation found did not meet their needs. Any new iteration of these guidelines might include a range of different approaches among which the MS can choose to use "off-the-shelf", in adapted form, or simply as a source of inspiration.

1.4 Develop criteria and methodologies to be used during the identification process so as to assess 'cross sector dependencies'

Building on recommended action 1.1 (on 'cross-sector dependencies'), this action aims to provide the MS with tools with which to in fact identify and assess existing interdependencies. Specifically, the EC and the JRC could develop an illustrative framework that would serve as a non-binding approach guiding MS during the identification process, and which would adequately consider and assess the presence of cross-sector (and sub-sector) dependencies. Existing risk assessment procedures addressing threats to assets and systems, but also at societal level, could be considered as a starting point in developing such a framework. Existing practices adopted by MS that already account for this dimension when performing the risk assessment could also be considered as a starting point for further elaboration. These practices could be collected within the consultation activities foreseen under recommended action 1.1.

1.5 Set minimum criteria for the identification process

Building on the work already performed by the JRC, the EC may consider expanding the description of the procedure for the identification of potential ECI. Specifically, the EC could provide additional detail concerning the criteria to be used in each step, but also in setting minimum criteria to be considered while acknowledging that no one-size-fits-all solution exists. In other words, room should be left for the MS to adapt and adjust as appropriate.

In order to do so (and in a similar vein as the approach described under the recommended action 1.1), the EC may choose to consult MS experts (either via ERNCIP or in the context of an ad hoc group of experts designated by MS) in order to understand the criteria currently being used at the national level. This would allow the EC to gain a more complete overview, to identify commonalities, and to identify aspects that could be further refined.

1.6 Provide guidelines so as to assess the 'availability of alternatives'

The EC could consider providing guidelines on criteria and related thresholds that MS should consider when assessing the availability/non-availability of alternatives. In order to develop these guidelines, the EC should engage with MS experts through targeted workshops. Examples of aspects to guide the discussion at the workshop include consideration of whether the alternatives should be in the same sub-sector; which geographic locations are in/out of scope (e.g. third countries); or whether there is time- or resource-related thresholds beyond which an option cannot be considered an 'alternative'.

1.7 Specify in more detail the minimum content that OSPs should include

The EC might consider introducing more details about the minimum content of the OSP. This action is related to recommended action 1.3.

In order to accomplish this, the EC could consult CI owners/operators so as to better understand the content (usually classified) of the security plans that are adopted by operators operating in different sectors in different MS. Based on the output of this consultation, and with the support of the JRC, the EC could identify commonalities and gaps with the ultimate aim of designing a common minimum structure/content for OSPs.

The OSP structure should make clear the need to consider measures that simultaneously serve to comply with any other relevant sectoral legislation affecting the same CI. Additional details that could be provided in the revised guidance on OSP development could include the actors that should associated with the drafting process, and the imperative that it be developed in co-operation with the relevant competent authorities and other CI operator stakeholders (thereby accounting for known interdependencies).

1.8 Develop a competency framework for the SLO function

It is recommended that the EC develop a common framework detailing the key competences that all SLOs should have. This could include a common core description of the SLO role, a set of SLO responsibilities/objectives, and a list of mandatory and desired qualifications for all SLO candidates.

As a starting point in developing any such framework, the EC could draw on evidence both from this Evaluation and from the 2014 EC-funded study on the topic of SLOs. The EC could then convene a series of workshops with the JRC and European associations of sectoral CI owners/operators with the aim of agreeing on a set of core SLO competences. The output of these workshops would be a formalised framework for key SLO competences. Such a framework would serve to improve the operationalisation of the SLO provision among CI owners/operators and to increase harmonisation insofar as there would be a "European vision" as to what SLOs should have in terms of background, competences and roles/responsibilities. This framework would also clarify the distinctive features of the SLO when compared to other roles that might already exist at the national level (e.g. Chief Security Officer).

The EC may also wish to consider establishing a requirement to embed this framework into SLO recruitment processes across MS. To encourage uptake of the new competency framework, the EC could hold a set of targeted briefings with PoCs and CI owners/operators across MS and deliver training sessions for SLOs (see recommended action 1.9) once the framework is ready for operationalisation.

1.9 Organise training sessions for security officers in relation to ECI and NCI

Following the development of a SLO competency framework (recommended action 1.8), there would be merit in the EC and the JRC organising and delivering training sessions that focus on the role and tasks of the SLO in relation to ECI and NCI. To ensure that the confidentiality of identified ECI is protected, these trainings would be made available to security officers responsible for both ECI and NCI.

This training would cover the SLO competences defined in the framework (recommended action 1.8) and would be designed in conjunction with European associations of CI owners/operators in the specific sectors covered by the Directive in order to ensure sectoral relevance. It would be delivered in person (rather than online) to help foster relationships between security officers, and the training would highlight the specific requirements that exclusively apply to SLOs responsible for ECI.

The organisation of these trainings mirrors similar practices implemented within EPCIP (e.g. the ERNCIP training course for professionals held in Brussels on 21-23 July 2016). Events such as these may contribute to the continued development of the existing CIP community and serve to further refine the capabilities of professionals that serve as SLOs and/or are involved in OSP drafting/implementation.

1.10 Revise the template for the biannual report by the MS to the EC on risks, threats and vulnerabilities

It is recommended that the EC revise the structure of the biannual report template in order to elicit more useful information that can be compared. To achieve this, the EC could define categories for

threat, risks and opportunities and insert additional questions as appropriate. Any such revised template could be accompanied by reporting guidance (e.g. providing examples of key indicators to be measured). These macro categories and the accompanying guidelines for MS could be developed by the EC in discussion with MS PoCs and the JRC. The categorisation could, for instance, be designed starting from the classification of threats outlined in Annex I.7.3, but with a particular focus on terrorism, natural hazards, cyber-attacks from organised crime and state actors, and insider infiltration. Reports should be shared with the Commission through channels that reflect the sensitivity of the information contained therein.

2. Assess the opportunity to extend the sectoral scope of the Directive

One action is proposed as part of this recommendation.

Issue(s) addressed	Actions	Addressees
• The current scope of the Directive limits its relevance, given increased interdependencies across sectors including ICT and space. • Synergies among the different components of the wider EU CIP legislative framework have been somewhat under-exploited. • There is potential for misalignment with norms in the space sector. • The ECI Directive overlaps with the NIS Directive insofar as network and information systems may be considered ECI.	2.1 Perform an impact assessment study in order to assess the impacts of an extension of the scope of the Directive to include additional sectors	EC

Evidence collected as part of the Evaluation supports an in-depth investigation of a possible extension of the scope of the Directive. Most national CIP frameworks already cover sectors outside the scope of the Directive (transport and energy). Moreover, technological and scientific advances have highlighted increasing cross-sectoral interdependencies, particularly in relation to ICT, as well as interlinkages between physical and cyber protection. While the Evaluation finds a general appetite amongst stakeholders to expand the sectoral scope of the Directive, it does not suggest which sectors and sub-sectors should be included in any new initiative. That being said, the **ICT and space** sectors could be considered among the first sectors to be investigated for possible inclusion, given the interdependencies that exist with other sectors and recent policy developments (NIS Directive and the proposal for a new Space Programme, respectively).

2.1 Perform an impact assessment study in order to assess the impacts of an extension of the scope of the Directive to include additional sectors

As stated in Preamble 5 of the Directive and based on the findings of this Evaluation, the EC could consider performing an impact assessment study in order to evaluate the potential impacts of extending the scope of the Directive beyond the energy and transport sectors to include additional sectors that reflect recent policy developments and the increasingly deep interdependencies that exist between CI in different sectors. The narrow scope of the Directive makes this piece of legislation partially relevant to the current security challenges and recent technological developments. Keeping the current scope might lead in future to the development of further measures that are not completely effective as they do not account for cross-sectoral interdependencies and do not adequately protect CI from certain emerging threats (e.g. hybrid threats) that span many sectors, of which transport and energy are but two.

3. Strengthen the monitoring and evaluation framework in order to support future decision-making processes

Two actions are proposed as part of this recommendation.

Issue(s) addressed	Actions	Addressees
• The EC has a limited overview on the implementation of different provisions contained in the ECI Directive.	3.1. Design output and result indicators and require MS to report on them	EC JRC MS
• The EC lacks instruments with which to follow up on the implementation of the Directive.	3.2. Provide the EC with monitoring responsibilities over the implementation of the Directive	EC MS

The Evaluation found that a framework for monitoring and evaluating (M&E) the implementation of the Directive is largely absent, and that reporting is primarily used for compliance purposes. This affects the EC's ability to monitor the application of the Directive, to correct ECI suboptimal

security measures, to understand whether and how the Directive has been implemented by MS, and to assess whether the Directive has led to an increase in the level of protection of ECI.

3.1 Design output and result indicators and require MS to report on them

The absence of an M&E framework limits the EC's ability to identify gaps in implementation at the MS level, but also to assess to which extent the objectives of the Directive have actually been achieved. To address this weakness, the EC could design a set of indicators/descriptors for use in measuring the immediate outputs and the long-term results of the Directive. Drawing on the intervention logic designed for this study and accounting for the difficulties encountered in systematically collecting implementation-related information, indicators such as these might be used to collect information concerning:

- The number of MS that launched the identification process, the MS that were engaged in these discussions, and the outcomes of these discussions (identification of ECI);
- The number of MS that entered into the designation process, and the outcomes of this process (designation of ECI);
- The background and main features of designated SLOs;
- The number of existing OSPs and the frequency with which they are updated;
- The nature of MS involvement in relevant EU-funded research projects on CIP; and
- The number and frequency of consultation activities between/among MS (besides those related to the ECI identification and designation process).

The template for reporting could be developed by the EC in consultation with the JRC. This could include a set of clearly articulated questions and indicators in order to encourage standardised responses across MS. The reporting could be completed by national PoCs and submitted to the EC on an annual basis. In light of the reluctance of MS to report information on sensitive matters relating to national security, taking part in this exercise must be seen as worthwhile/beneficial to the MS. One possibility might be for the EC to provide the MS with a summary of the outcomes of each annual reporting cycle. The information provided by the MS could also be used both in designing the SLO competency framework and customising the content of the training sessions proposed as part of recommended actions 1.8 and 1.9, respectively.

3.2 Provide the EC with monitoring responsibilities over the implementation of the Directive

The EC might be given monitoring responsibilities in relation to the implementation of the Directive. These new monitoring responsibilities should respect the confidentiality of certain categories of information. The treatment of specific categories of information should be formally agreed upon by the EC and MS. Given monitoring responsibilities, the EC would have the possibility to follow up on cases of non-compliance, not least by providing additional support/guidance as appropriate.

4. Re-balance roles and responsibilities assigned to the various stakeholders involved in the identification and designation of ECI

Two actions are proposed.

Issue(s) addressed	Actions	Addressees
• The bilateral and/or multilateral meeting format for designating ECI is not conducive to private sector involvement or to a networked approach. • The Directive does not reflect the existence of PPPs and focuses only on MS as the main actors involved in the identification and designation processes.	4.1. Clarify that MS may involve private sector representatives in the identification and designation of ECI	EC MS CI operators
• The identification and designation process relies too heavily on the initiative of individual MS. • The reporting requirement did not generate EU-wide knowledge on CIP threats and risks. Rather, it is used mainly for compliance purposes and therefore of limited EU added value. • Presence of a CIP framework prior to the adoption of the Directive and a lack of appetite at MS level have reduced the uptake of the Directive.	4.2. Require the EC to perform an EU-level threat assessment and, on this basis, suggest potential ECI to MS	EC MS

Issue(s) addressed	Actions	Addressees
• National biannual reports to the EC on risks, threats and vulnerabilities are of limited utility in assessing the need for additional protection measures.		

The Evaluation identified some issues concerning the role and responsibilities of stakeholders involved in the implementation of the activities foreseen by the ECI Directive which might affect its overall relevance and EU added value. Specifically, there is limited involvement of the private sector both in the identification process and in the subsequent discussions on designation. Furthermore, the OSP drafting process is often centralised, meaning there is limited involvement from the relevant security-related actors. Moreover, the MS where CI infrastructure (candidate ECI) is located has significant influence over the identification process. When taken together with the finding that the Directive's provisions are of limited value in light of pre-existing protection requirements at national level, there are indications that the "host" MS may be disincentivised to launch the identification process (insofar as it may not necessarily result in any higher level of protection for in-country CI).

4.1 Clarify that MS may involve private sector representatives in the identification and designation of ECI

It is recommended that the EC clarify that MS can involve private sector representatives both in the identification of ECI and during the discussions on possible designation. Deeper engagement with the private sector may lead to improved information-sharing between operators and competent national authorities and, over the longer term, to more robust CIP policy accounting for a combination of relevant stakeholder perspectives. This action envisions MS retaining the right to decide whether and how (e.g. bilateral/multilateral meetings, working groups, conferences) to involve private sector representatives.

4.2 Require the EC to perform an EU-level threat assessment and, on this basis, suggest potential ECI to MS

Building on recommendation 3, which supports improved M&E of the Directive, it is recommended that the EC perform an EU-level threat assessment in the sectors and sub-sectors within the scope of the Directive in order to identify potential ECI, which can then be suggested to MS for possible designation (this role for the EC is already foreseen in Article 3 of the Directive) and suggest to MS measures, if any, to improve their protection. MS that ultimately decide not to designate CI as ECI should provide the EC with a detailed assessment that could be used by the EC in order to improve the identification process over time. As this appears as an additional requirement to MS, it is important that the threat assessment performed at EU level adds to what MS already know based on their own intelligence.

In this view, it should be noted that similar such analyses are conducted by EU institutions in other areas (e.g. Europol's *Serious and Organised Crime Threat Assessment*; EC working documents[362]) and by CI owners/operators on a sectoral basis. In light of this fact, the EC should liaise with other actors involved in threat analysis activities in order to collect and consolidate information relevant in the context of the EU-level CI threat assessment and integrate this information with the data on risks, threats and vulnerabilities reported by MS every two years.

5. Address the key differences in national CIP frameworks that affect the identification of ECI

In implementing this recommendation, four actions are proposed.

Issue(s) addressed	Actions	Addressees
• Different national authorities have different attitudes towards co-operation. This affects the identification process.	5.1. Map existing sectoral networks, working groups, and expert groups engaged in CIP-related issues	EC CI operators
• The lack of a sectoral view on the part of PoCs limits the exchange of information between MS and the fostering of mutual trust.	5.2. Revise the format of CIP PoC meetings in order to enable exchanges between sectoral authorities and experts	EC MS

[362] For instance: EC (2017). 'Commission Staff Working Document: Overview of Natural and Man-made Disaster Risks the European Union may face'. Brussels, 23.5.2017: SWD(2017) 176 final.

Issue(s) addressed	Actions	Addressees
• The different interpretations of CI by MS might challenge the existence of a common starting point for the identification process.	5.3. Define 'asset', 'system' and 'vital societal functions'	EC
• National governance arrangements lack clarity.	5.4. Map roles and responsibilities in the various national CIP frameworks	EC

The Evaluation highlighted the appetite of some stakeholders (both PoCs and CI owners/operators) to focus on the protection of NCI in addition to ECI. Differences at the national level might indeed negatively affect the effective implementation of the identification and designation of ECI described in the Directive. Since this study was squarely focused on ECI, no systematic analysis of existing CIP measures at the national level has been conducted. That being said, there is evidence to suggest some key differences among national CIP frameworks that might have affected the implementation of the Directive. For instance, different attitudes on the part of national competent authorities towards co-operation affected the exchange of information during the identification and designation process. Meanwhile, the different types of administrative arrangements at MS level made it difficult in some cases to identify which institutions were in fact responsible for this process. Finally, different MS interpreted the CI definition in ways that were not necessarily aligned. This meant that two MS could approach the proverbial table as part of the identification and designation process with different understandings as to what CI is. For these reasons, the EC is recommended to take measures that might lay the groundwork for a more common interpretation of the Directive's provision, while at the same time respecting national competence in this area.

5.1 Map existing sectoral networks, working groups, and expert groups engaged in CIP-related issues

Besides the CIP PoCs, a number of sectoral networks, working groups and expert groups (such as ERNCIP and the Thematic Network on Critical Infrastructure Protection (TNCEIP)) dealing with issues related to CIP exist. However, not all relevant CIP stakeholders consulted over the course of the study were familiar with these constellations and their work. In light of this fact, the EC may consider mapping the main EU-level networks and groups, the scope of their activities, objectives and members. Such a list could be drawn up by DG HOME together with other relevant DGs (DG MOVE, DG ENER and DG CNECT) and European associations of sectoral CI owners/operators. Sharing this list with the CIP PoCs and national stakeholders may serve to trigger increased co-operation, additional exchange of information and even some streamlining of efforts.

In case this mapping exercise points at substantial overlaps (in terms of objectives and participants) between the CIP PoC meetings and other networks or working group, the opportunity to merge the groups could also be explored.

5.2 Revise the format of CIP PoC meetings in order to enable exchanges between sectoral authorities and experts

The EC might consider revising the format of the CIP PoCs meetings in order to create opportunities for sectoral authorities and experts to participate and exchange information as appropriate. However, such meetings should not replace the regular CIP PoCs meetings, which according to the evidence collected are widely appreciated. Rather, these could be annual events held in addition to the regular meetings of the CIP PoCs. The CIWIN platform could be used as a complement to these meetings, where it is able to provide an online forum for MS and CI owners/operators to discuss, launch ad hoc queries, exchange good practice, etc.

5.3 Define 'asset', 'system' and 'vital societal functions'

The EC may consider clarifying some key terms that are currently subject to different interpretations. These include:

- 'Asset', the meaning of which can change upon translation;
- 'System', which might refer to a network/grid, a group of assets or services, and/or a group of cross-sectoral assets; and,
- 'Vital societal functions', which may be confused with 'essential services' as defined in the NIS Directive.

5.4 Map roles and responsibilities in the various national CIP frameworks

In order to facilitate co-operation both between and within MS, there would be value in the production of a document mapping the roles and responsibilities of the different authorities part to the various national CIP frameworks. Drawing on what has already been developed within this study (Annex I.6.2), the EC could provide short descriptions of the administrative arrangements in each MS and provide the relevant contact information for key authorities. This information could then be distributed to the PoCs.

6. Strengthen the link between the requirements of the ECI Directive and the available sources of funding at the EU level

Two actions are proposed in order to implement this recommendation.

Issue(s) addressed	Actions	Addressees
• Limited awareness of the available sources of funding to support the implementation of the Directive. In addition, available sources of funding are not visible enough.	6.1. Prepare a document explaining available funding opportunities relating to CIP	EC MS
• Results of EU-funded projects are not systematically communicated within the CIP community.	6.2. Introduce a requirement for the EC to proactively contribute to and monitor research activities relating to CIP	EC MS CI operators

Even though the Evaluation was not conclusive on the importance of the costs incurred as a result of the implementation of the Directive's provisions, additional EU funding would be appreciated by stakeholders, including CI owners/operators. Existing opportunities appear to be poorly advertised, while the results of EU-funded projects are not systematically communicated to the MS. As such, there is room for the EC to play a role in facilitating access to these funds and in more effectively communicating the results of projects.

This recommendation is expected to counterbalance the introduction of new requirements for the protection of ECI described under recommendations 1 and 3, respectively.

6.1. Prepare a document explaining available funding opportunities related to CIP

The EC might consider drafting a brochure describing the various funding programs and the relevant calls (such as ISF and H2020 Secure Societies programme). The main target audiences would be CI owners/operators and MS competent authorities. Such a brochure might describe the types of projects that could be funded, the criteria for eligibility for each project type, the timeframe, etc. This product could be disseminated via the CIP PoCs, who would be responsible for distributing it widely at national level. Even though the existing funding programmes are not primarily intended for designated ECI owners/operators, the brochure could highlight specific projects/activities/programmes of particular relevance for this audience.

6.2. Introduce a requirement for the EC to proactively contribute to and monitor research activities related to CIP

It is also suggested that the EC contribute to and monitor research activities relating to CIP. This would allow the EC to identify stakeholder needs through its regular contacts with the CIP PoCs and other stakeholders. These needs would then serve as a basis in designing annual work programmes for H2020 funds and other funds. Doing so would serve to more effectively align the needs of CIP stakeholders, including ECI operators, with EU-funded research in this area. In practical terms, the EC could periodically survey the needs of the MS (via PoCs and CI owners/operators, for instance). Having this role, the EC would also be responsible for monitoring the results of relevant projects and disseminating them to the MS in order to ease their uptake around Europe. This activity would further expand what the EC is already doing, though not systematically and with a more limited scope.

7. Streamline the EU CIP legislative framework and trigger synergies at the national level

This recommendation is accompanied by two proposed actions.

Issue(s) addressed	Actions	Addressees
• There are a number of overlaps between the ECI Directive and sectoral legislation in the transport and energy sectors. • Directive provisions on risk analysis and risk management for operators overlap with similar measures in the aviation, maritime, rail safety legislation and rail security measures, and to lower extent with the NIS Directive • Directive provisions on threat assessment/risk analysis for national authorities overlap with similar obligations in the energy, aviation, maritime, rail security legislation and to lower extent in the NIS Directive • Synergies between different legislative sources in the energy and transport have been under-exploited, looking in particular at-risk analysis and risk management. • The ECI Directive overlaps with the NIS Directive insofar as network and information systems can be considered ECI	7.1. Organise sectoral meetings with the DGs responsible for the relevant sectoral legislation in the transport and energy sectors to further assess the existing overlaps	EC
	7.2. Share national good practices of integration of overlapping requirements	EC MS

The Evaluation highlighted room for improving the overall coherence of the EU CIP legislative framework by pointing at a number of overlaps of the ECI Directive with sectoral legislation. Since requirements in the EU legislation are quite general, understanding to which extent these overlaps represent a duplication or rather mutually reinforce each other requires an additional step of analysis which needs to also examine how the EU legislation has been implemented on the field. Even though stakeholders at the national level do not raise significant difficulties in making the different requirements coexist, there is room for the EC to streamline the overarching legislative framework in view of future decision-making processes. This would eventually either simplify the current framework or trigger more synergies when requirements stemming from sectoral legislation do not duplicate each other. In both cases, this intervention would bring benefits at both the EU and national level. At the EU level, this would address the objectives of the Regulatory fitness and performance (REFIT) Programme, which aims to make EU law simpler and less costly through the detection of duplications and synergies. At the MS level, national authorities and CI owners/operators would benefit from the increased clarity and could further exploit opportunities of co-operation with authorities and sectors that are usually not otherwise considered.

7.1. Organise sectoral meetings with the DGs responsible for the relevant sectoral legislation in the transport and energy sectors to further assess the existing overlaps

Drawing on the list of potential overlaps identified by this study, it is recommended that the EC starts discussions with DGs responsible for the relevant pieces of legislation to further assess the nature and scale of the overlap. These discussions could take the form of sectoral meetings and could eventually result in ideas about how to simplify the legislative framework (in case of duplications), or to strengthen synergies in the implementation of similar practices (in case of complementarities). As an alternative to sectoral meetings, the EC may also consider the opportunity to perform a 'fitness check' of the CIP legislative framework and the relevant sectoral legislation. Depending on the selected timing, these meetings could also be the opportunity to assess the extent to which the ECI Directive overlaps with the NIS Directive. Drawing on the analysis of the transposition measures recently notified by MS to the EC, it is recommended to use these meetings to clarify the main sources of confusion raised by PoCs throughout this study (e.g. the content of obligations when a network and information system is designated also as ECI, the meaning of "essential service" in both the ECI Directive and the NIS Directive).

7.2. Share national good practices of integration of overlapping requirements

To complement recommended action 7.1, the EC may consider inviting PoCs to share good practices adopted at the national level to implement similar requirements (e.g. the meetings organised by the Spanish PoC with national stakeholders). In this view, PoCs may be requested to identify national practices by consulting national stakeholders and then sharing it with other MS at the CIP PoC meetings and/or through the CIWIN platform.

8. Facilitate the exchange of information and co-operation with third countries

This recommendation is accompanied by one action.

Issue(s) addressed	Actions	Addressees
• The Directive lacks consideration of MS dependencies on third countries' CI and is therefore not fully relevant to current threats	8.1 Organise ad-hoc meetings with CIP competent authorities in selected third countries to enhance co-operation	MS EC EEAS

The Evaluation found that the Directive does not address the need of some MS to coordinate with third countries on account of specific cross-boundary CI interdependencies. Despite the potential relevance of their CI to the EU's security, the definition of CI contained in the Directive does not consider third countries. Moreover, there is no provision on the exchange of information or co-operation with third countries. The recent involvement of third countries in PoC meetings and the initiatives undertaken with third countries within the context of EPCIP further confirm the increasing interest on the part of MS to liaise with third countries in order to improve EU levels of protection. This suggests an area for further EU action to support MS.

8.1 Organise ad-hoc meetings with CIP competent authorities in selected third countries to enhance co-operation

Together with MS, the EC could identify key transboundary CI where third countries are concerned and, through the support of the European External Action Service (EEAS), liaise with third countries' relevant authorities, but also facilitate meetings between them and EU MS. These targeted meetings could pave the way for enhanced co-operation and improved exchange of information on the protection of specific CI. Such meetings might initially be used to address at a high level of abstraction national CIP frameworks and the allocation of roles and responsibilities. Any exchange of confidential information on the specific content of protection measures would need to be discussed and agreed with the EC in advance.

Publications Office of the European Union