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

Annex I

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

Annex I

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 978-92-76-19512-2 doi: 10.2837/19383 DR-03-20-376-EN-N

Table of Contents

1. METHODOLOGICAL NOTE 1
1.1. Catalogue of data collected 1
1.2. Data collection strategy 3
1.3. Consultation tools 5
2. LIST OF STAKEHOLDERS CONSULTED 9
2.1. Interviewees 9
2.2. Stakeholders answering the online survey 10
2.3. Stakeholders engaged in the case studies 11
2.4. Stakeholders attending the workshops 12
3. SYNOPSIS REPORT OF THE CONSULTATION ACTIVITIES 13
3.1. Objectives of the consultation 13
3.2. Results of the consultation activities 14
3.3. Feedback to stakeholders 22
4. BIBLIOGRAPHY 23
5. THE ECI DIRECTIVE 32
5.1. Description of the key provisions of the Directive 32
5.2. Workflow of activities described in the ECI Directive 34
6. EVIDENCE SUPPORTING THE IMPLEMENTATION STATE OF PLAY 36
6.1. Recent developments in national legislation 36
6.2. National CIP administrative set-up 39
7. EVIDENCE SUPPORTING THE ANALYSIS OF THE RELEVANCE 40
7.1. Relevance of definitions included in the Directive 40
7.2. Relevance of the Directive to stakeholder needs 43
7.3. Relevance of the Directive to current and future threats 45
7.4. Relevance of Directive to advances since 2008 49
8. EVIDENCE SUPPORTING THE ANALYSIS OF THE COHERENCE 54
8.1. List of pieces of legislation and policy documents analysed 54
8.2. Overview of overlaps and complementarities 55
8.3. Mapping of key aspects of relevant EU sectoral legislation 59
8.4. Analysis of key aspects of international initiatives in the context of CIP 126
8.5. Analysis EU CIP legislation besides energy and transport 129
9. EVIDENCE SUPPORTING THE ANALYSIS OF THE EFFECTIVENESS 132
9.1. Contribution of the Directive provisions in achieving the objective of establishing a procedure for the identification and designation of ECI 132
9.2. Contribution of the Directive provisions in achieving the objective of establishing a common approach to the assessment of the need to improve the protection of ECI 135
10. EVIDENCE SUPPORTING THE ANALYSIS OF THE EFFICIENCY 138
10.1. Main costs and related obligations sustained by stakeholders in relation to Directive 2008/114 138

1. METHODOLOGICAL NOTE

1.1. Catalogue of data collected

Evaluation Criteria	Evaluation questions	Desk research	Field research				
			Interviews	Online survey	Workshops	Case studies	PC
Relevance	1.1. To what extent are the definitions set out in the Directive still deemed to be suitable and fit for purpose?	x	x	x	x	x	
	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?	x	x	x	x	x	
	1.1.b To what extent does the definition of critical infrastructure provided in the Directive fit with the sectors that is applied to?	x	x	x	x		
	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?	x	x	x	x	x	x
	1.3. Is the Directive suitable to the needs/interests of the relevant industries and other stakeholders?	x	x	x	x	x	x
	1.4. To what extent does the Directive contribute to stated EU priorities?	x	x		x		
	1.5. Are there provisions contained in the Directive that might be considered obsolete?	x	x	x	x		x
	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?	x	x	x	x	x	
Coherence	2.1. To what extent the Directive is coherent and complementary to other policy interventions with similar objectives at MS level?	x	x	x	x	x	x
	2.2. To what extent the Directive is coherent and complementary to other policy interventions with similar objectives at EU and international levels?	x	x	x	x	x	x
	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?	x	x	x	x	x	x
Effectiveness	3.1. To what extent has the Directive achieved the stated objectives?	x	x	x	x	x	x
	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?	x	x	x	x	x	x

Evaluation Criteria	Evaluation questions	Desk research	Field research				
			Interviews	Online survey	Workshops	Case studies	PC
	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?	x	x	x	x	x	x
	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?	x	x	x	x	x	x
Efficiency	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?	x	x	x	x	x	x
	4.2. What factors have influenced the efficiency of the Directive? To what extent?	x	x	x	x	x	x
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?	x	x	x	x	x	x
Sustainability	6. Are the effects already achieved on account of the Directive likely to be long-lasting, if the Directive were repealed?	x	x	x	x	x	x

1.2. Data collection strategy

The study relied on both desk and field research.

1.2.1. Desk research

The Evaluation team performed an extensive desk research at the EU, national and international level.

At the **EU level**, the analysis focused on the overarching policy and legislative framework for the protection of CI. The Evaluation team looked therefore at EU policy and legislative documents on security and CI protection (adopted before and after the Directive) in the relevant sectors covered by the Directive (i.e. energy and transport) as well as in other relevant sectors (banking and financial infrastructure, health, space, Information and Communications Technology (ICT), drinking water supply and distribution).

At the **national level**, the analysis focused on the main national legislative measures, strategies, administrative procedures and guidelines that have contributed in transposing and implementing the provisions of the Directive at the national level. Such analysis has allowed the assessment of how and to what extent the 28 MS have implemented the Directive and, where possible, the understanding of the degree to which this led to an improvement of the protection of CI. Drawing on the evidence included in the 2012 review,[1] the Evaluation team analysed in-depth national implementation measures reported by MS to the EC and reported in the EUR-Lex portal, and extended the scope of the analysis with the aim to fill existing gaps and update the overview with recent changes occurred after 2012. Specifically, additional regulations and guidelines were analysed (for instance, specifying the contents of OSPs), as well as any updates, revisions to existing measures and new measures directly impacting the national ECIP framework that were made since 2012.

Relevant information is systematised in the *implementation tables* included in Annex II according to a list of the key dimensions of analysis defined based on the Team's understanding of Directive 2008/114 and its provisions. Sources consulted are duly referenced in correspondence with each information recorded in the tables. To validate the analysis of national implementation and fill the remaining gaps, the implementation tables were shared with the national Points of Contact (PoCs). PoCs from 24 Member States[2] provided a feedback and information collected from the desk research has been integrated and triangulated with it. When coming from the PoCs, information is reported in the implementation table with a different colour code (blue) and with indication of the PoC among the sources.

At the **international level**, the analysis focused on international standards and initiatives related to the protection of CI, as identified by the research team or suggested by stakeholders interviewed. A list of the analysed documentation is presented in Section 4.

1.2.2. Field research

Stakeholders have been consulted through a combination of instruments, managed either by the Evaluation team or the Commission, and addressing either the EU or the MS level.

At the EU level: 37 **interviews** with representatives from EC DGs and Agencies, academia and think tanks, and European associations of CI owners/operators; and a **public consultation** (PC) launched by the EC and targeting the general public and a vast array of stakeholders with few and quite general questions on the perceived level of security of CI, the type of security threats and possible areas for improvement.

At the MS level: an **online survey** to PoCs and other national competent authorities and CI owners/operators aiming at collecting 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; four **case studies** that aimed at collecting first-hand information on implementation practices, obstacles and enablers in four MS (FR, ES, DK, SK) and that consisted of six interviews per MS

[1] 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".

[2] AT, BE, BG, CZ, DE, DK, EE, ES, FI, FR, EL, HR, HU, IT, LU, LV, MT, NL, PL, PT, RO, SE, SI, SK.

with the PoC, other national competent authorities and CI owners/operators. An additional **consultation with the PoCs** was carried out in February-March 2019 in order to validate the findings contained in the Final report for review.

In order to mitigate some of the limitations encountered in the study, in addition to what was originally planned, additional field research has been undertaken through **a round of validation and integration of the implementation tables**. PoCs were asked to validate the content of the tables, fill in any gaps, and resolve any conflicts between the information gathered through the desk and the field research.

1.2.3. Stakeholders involved

Overall, the study involved **147 stakeholders**[3] belonging to different categories, each one targeted through specific data collection tools, as shown in Table 1.

Table 1 – Stakeholders involved, related consultation tool and type of information retrieved

Stakeholder category	# of stakeholders[4]	Online survey[5]	Interviews	Workshop	Case study	PC	Type of information retrieved
EU level							
EC DGs, EU Institutions and EU Agencies	18		x	x			• **State of the debate on CIP;** • **Relevant EU policy context, legislation and initiatives in the field of CIP;** • **The organisation of the work aimed at implementing the Directive at EU level;** • **Expectations on the current evaluation;** • **Examples of good practices and recommendations;** • **Potential additional sources of information.**
Academia and think tanks	10		x			x	• **Current and emerging security threats in relation to CI;** • **Good practices implemented within and outside Europe to ensure protection of CI;** • **Relevant international policies or frameworks to be considered in the analysis of the coherence of the Directive;** • **Views on specific evaluation questions;** • **Examples of good practices and recommendations;** • **Potential additional sources of information.**
CI owners /operators at European level	11		x	x		x	• **Current and emerging security threats in relation to CI;** • **Relevance of the rules and processes included in the Directive for the energy and transport related CI;** • **Key developments in the protection of CI;** • **Views on specific evaluation questions;** • **Good practices in the protection of CI.**
MS level							
PoCs	24	x		x	x		• **Information on the implementation of the Directive at the national level and on their CIP policy;** • **Evolution in the protection of CI since the transposition of the Directive;**
Other competent authorities	26	x			x	x	

[3] This number accounts only for stakeholders involved directly by the Evaluation team and does not include the respondents to the PC.

[4] These numbers do not account for stakeholders that often took part to the interview together with the Evaluation team's primary contact.

[5] National stakeholders answering the survey were contacted by the PoCs.

Stakeholder category	# of stakeholders[4]	Online survey[5]	Interviews	Workshop	Case study	PC	Type of information retrieved
CI owners/ operators	58	x		x	x	x	• **Relevance of the provisions and clarity of the definitions;** • **EU added value and sustainability of achieved results;** • **Suggestions for improvement.** **For case studies** • **The organisation of the work aimed at implementing the Directive;** • **Reasons for not implementing certain provisions;** • **Key results achieved since the transposition of the Directive;** • **Main obstacles in the implementation of the Directive and possible enablers;** • **National-specific features having affected the implementation of the Directive.**

In terms of **geographical distribution**, almost all Member States have been covered through the different collection tools (at least by one representative from one of the three targeted national categories of stakeholders). The only countries that were not covered at CY, IE, LT and UK[6] (see Table 2).

Table 2 - Number of stakeholders engaged through the on-line survey, workshops and case studies

Country	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU
PoCs	1	1	1		1	1	1	1	1	1	1	1	1	1
Other competent authorities	2		1		2		3	1	3	3		2		
CI owners/operators	5	2	2		2	2	2	1	5	3	1	2		
Total	*8*	*3*	*4*		*5*	*3*	*6*	*3*	*9*	*7*	*2*	*5*	*1*	*1*
Country	**IE**	**IT**	**LT**	**LU**	**LV**	**MT**	**NL**	**PL**	**PT**	**RO**	**SE**	**SI**	**SK**	**UK**
PoCs		1		1	1	1	1	1	1	1	1	1	1	
Other competent authorities		2						2			2	1	2	
CI owners/operators		1				1		13	6	3			8	
Total		*4*		*1*	*1*	*2*	*1*	*16*	*7*	*4*	*3*	*2*	*11*	

Source: Authors' elaboration

1.3. Consultation tools

1.3.1.1. Online Survey

The online survey aimed at collecting comprehensive and specific information on procedures and rules applied at national level to implement the Directive and better understand the relationship with other relevant measures in the field of the protection of CI. It helped in filling in information gaps on the national implementation, and to collect high level insights from an extensive number of stakeholders on the main aspects covered by the study.

The online survey **targeted**: national PoCs; other competent authorities; and CI owners/operators in the field of energy and transport.

As for the PoCs, the EC provided the Evaluation team with a list of contacts (i.e. more than one contact per MS). In order to encourage a unique and coordinated response from the different

[6] CY and IE did not take part to the consultations conducted for the previous study - Booz & Company (2012), 'Study to support the preparation of the review of the Council Directive 2008/114/EC', Final Report.

stakeholders identified as PoC for the same MS, the Evaluation team sent one invitation per MS[7] and asked for a unique response whenever possible.

As for the other categories of stakeholders, the EC asked the PoCs to spread the survey among relevant contacts at the national level. As a consequence of this decision, the Evaluation team had little if any insight as to which entities at national level received access to information about the survey.

The Evaluation team designed the survey questionnaire around four main **sections**:

1. *Personal information*, to provide general information and personal details;
2. *Framework of protection of national Critical Infrastructures (NCIs)*, to provide information on current rules applicable to the protection of CI at national level and their evolution;
3. *Evaluation of Directive 2008/114* – the main section of the survey – to gather information on the main aspects covered by study: relevance, effectiveness, efficiency, coherence, sustainability and EU added value of the Directive. Questions included in this section aimed, *inter alia*, at investigating the concrete implementation of the Directive, the results achieved, the problems encountered and the interaction of this piece of legislation with other sectoral regulations; and
4. *Suggestions for improvement*, to provide inputs for the improvement of ECI protection.

The questions were customised depending on the three specific categories of stakeholders, thus creating three different questionnaires.

The survey was launched on 12 October using EY's on-line survey tool, eSurvey©, with the initial goal of keeping it open for three weeks. Two email reminders (on 19 and 26 October) were sent by the Evaluation team. The EC also supported the Evaluation team in the follow-up with national PoCs to increase the rate of response. Given the limited number of responses, and in agreement with the EC, the deadline for submissions was postponed on 2 November by 1 week (until 9 November). Table 3 provides an overview of the response rates for each category.

Table 3 – Overview of the survey

	PoCs	Other national authorities	CI owners/operators
Number of respondents	23	17	47[8]
Coverage of MS	**23**[9]	**10**[10]	**15**[11]

The survey questions aimed at gathering descriptive information concerning implementing practices at the national level. They were also leveraged to integrate the implementation tables and then analysed horizontally vis-à-vis implementation aspects. Feedback from stakeholders answering the survey is included in the report only where this was particularly relevant and easy to extract.

From an operational standpoint, all three surveys were initially sent to PoCs, with a request to fill in the survey intended for them and to forward the email with the links to surveys for other relevant national authorities and CI operators to the relevant contacts. As such, while it can be stated that the response rate of the survey sent to PoCs was 82% (23/28 responses), response rates for the other two surveys cannot be known, as they depend on the number of times the respective surveys were forwarded.

1.3.1.2. Interviews

37 interviews with stakeholders at EU level were performed, and specifically:

- 10 with representatives from *academia and think tanks,* mainly to investigate current and future needs and challenges, as well as the main policy developments in the CIP field vis-à-vis the objectives of the current Directive;
- 18 (including three scoping interviews performed during the preparatory phase) with representatives from *EC Directorates General (DGs), EU Institutions and EU Agencies*,

[7] When different ministries were identified as PoCs, the email was sent to the Ministry of Interior and all the other contacts were in copy.
[8] 31 in the energy sector, 12 in the transport sector, and 4 no sector specified.
[9] AT, BE, BG, CZ, DE, DK, EE, EL, ES, FI, FR, HR, HU, IT, LU, MT, NL, PL, PT, RO, SE, SI, SK.
[10] AT (2), BG, CZ (2), EE, EL (3), IT (2), PL (2), SE (2), SI, SK.
[11] AT (4), BG (2), CZ, DE, EE, EL (5), ES, FI, FR, IT, MT, PL (13), PT (5), RO (3), SK (7).

mainly to understand the current state of the debate on CIP in different sectors, and investigate the degree of coherence and complementarity between EU interventions in the CIP field; and

- Nine with representatives from *European associations of CI owners/operators,* mainly in the energy and transport sectors, to understand the results achieved by the Directive in the specific sector and the EU added value of the EU intervention.

The interviewees were selected in agreement with the Commission. Section 2.1 includes the list of stakeholders that were interviewed.

Interviews were performed mainly by telephone (except for two scoping interviews that were performed in-person on the same day as the Kick-off meeting).

1.3.1.3. Workshops

DG HOME together with EY held **two consultative workshops of one day each**. Both were held in Brussels. The first on 13 November involved Member States and related PoCs, while the second, on 14 November, involved CI owners/operators and other industry stakeholders.

Each workshop included:

- **Plenary sessions** for the discussion of the study interim findings and the results of the survey;
- **Break-out sessions** in smaller groups to examine in depth certain key aspects of the implementation of the ECI Directive according to a sectoral perspective. The workshop with MS included three thematic break-out sessions: power plant, gas pipeline, railway. The workshop with CI owners/operators included two thematic break-out sessions: energy and transport.

However, it should be noted that, despite the initial sectoral scope, the discussions held during the break-out sessions did not always relate exclusively to the identified sector, and information gathered could be extended to other sectors. This might be attributed to the limited sectoral specialisation of many PoCs.

1.3.1.4. Case studies

The aim of the case studies was to analyse in depth key issues linked to the implementation (or lack of implementation) of the Directive by gathering information through interviews with key stakeholders, analysing relevant documents and integrating information collected through other tools used in this evaluation. The information collected through case studies was used for the purposes of the overall evaluation study, considering case studies as representative of possible approaches to the most relevant issues related to the implementation of the Directive.

More specifically, the case studies aimed at:

- Better understanding the **organisational assets, division of responsibilities and approaches** in the CIP framework and implementation of the Directive at national level, thus providing a higher level of detail in the analysis;
- Better illustrating, in practical terms, the **implication and impacts** of actions related to the introduction and implementation of the Directive at the national level, which served to identify any causal links between the intervention and related actions and results/impacts;
- Better understanding the **contribution of other factors and developments** (e.g. actions at MS level, developments within the relevant sectors, other international mechanisms) to the results/impacts that can attributed to Directive; and
- Identifying **successful practices and approaches** that served as a basis for the definition of the recommendations.

The case studies covered 4 Member States, namely DK, FR, SK and ES, through 22 interviews with representatives from PoCs, other ministries and CI owners/operators. These countries were selected considering, among other things, the degree of CIP development prior to the introduction of the Directive, the dependence on CI located in other MS, the MS's exposure to risks, and geographical representation.

Where relevant, the main findings stemming from the analysis of the case studies have been included in the main report.

1.3.1.5. Public Consultation

The Commission launched on 19 November a Public Consultation open to anyone interested in providing input on the implementation of the Directive. It lasted 12 weeks, concluding on 11 February.

As of 11 February, 69 responses had been submitted to the Commission by respondents[12] representing national authorities, associations of CI owners/operators and other categories of stakeholders.[13] Additionally, two ad-hoc responses were received by means of position papers and emails. A synopsis report of the PC has been drafted and the feedback from stakeholders has been analysed and, when appropriate, included in the main report.

[12] In terms of geographical coverage, respondents were distributed in this way: 12 from AT, 8 BE, 1 BG, 7 CZ, 8 DE, 2 DK, 2 EE, 1 EL, 7 ES, 2 FR, 1 IE, 9 IT, 1 LU, 2 LV, 1 PL, 2 RO, 1 SK, 1 UK and 1 from Turkey.

[13] Answers to the public consultation included: 8 Academics/research institutions, 31 businesses, 14 EU citizens, 2 NGOs, 9 Public authorities and 4 non-specified.

2. LIST OF STAKEHOLDERS CONSULTED

2.1. Interviewees

Category of stakeholder	Institution
CI Owners/Operators	Confederation of European Security Services (COESS)
CI Owners/Operators	European Organisation for Security (EOS)
CI Owners/Operators	European Network of Transmission System Operators for Gas (ENTSOG)
CI Owners/Operators	Airports International Council (ACI)
CI Owners/Operators	Community of European Railways (CER)
CI Owners/Operators	Gas Infrastructure Europe (GIE)
CI Owners/Operators	European Sea Ports Organisation (ESPO)
CI Owners/Operators	Total[14]
CI Owners/Operators	Polskie Sieci Elektroenergetyczne S.A.[15]
EC DGs, EU Institutions and EU Agencies	EC – DG HOME
EC DGs, EU Institutions and EU Agencies	EC – DG HOME
EC DGs, EU Institutions and EU Agencies	EC – DG HOME
EC DGs, EU Institutions and EU Agencies	ENISA
EC DGs, EU Institutions and EU Agencies	JRC
EC DGs, EU Institutions and EU Agencies	EC (Cabinet of Commissioner Julian King)
EC DGs, EU Institutions and EU Agencies	EC - DG ECHO
EC DGs, EU Institutions and EU Agencies	EC - DG ENER
EC DGs, EU Institutions and EU Agencies	EC - DG GROW
EC DGs, EU Institutions and EU Agencies	EC - DG FISMA
EC DGs, EU Institutions and EU Agencies	EC - DG MOVE
EC DGs, EU Institutions and EU Agencies	EEAS
EC DGs, EU Institutions and EU Agencies	JRC
EC DGs, EU Institutions and EU Agencies	DG GROW
EC DGs, EU Institutions and EU Agencies	DG SANTE
EC DGs, EU Institutions and EU Agencies	DG CONNECT
EC DGs, EU Institutions and EU Agencies	DG HOME
EC DGs, EU Institutions and EU Agencies	EUROPOL
Academia and Think tanks	Leiden University Crisis Research Centre, Department of Public Administration

[14] Company member of CONCAWE, through which the contact was obtained.
[15] Company member of ENTSO-E, through which the contact was obtained.

Category of stakeholder	Institution
Academia and Think tanks	Norwegian Water Resources and Energy Directorate
Academia and Think tanks	Universidad Politécnica de Madrid, Department of Civil Engineering – Construction, Infrastructure and Transportation
Academia and Think tanks	Lund University Centre for Risk Assessment and Management (LUCRAM), Division of Risk Management and Societal Safety
Academia and Think tanks	Laboratory for the Analysis and Protection of Critical Infrastructures, ENEA
Academia and Think tanks	Universität der Bundeswehr München
Academia and Think tanks	Stockholm Universit, Department of Economic History
Academia and Think tanks	University of Warwick
Academia and Think tanks	Fraunhofer Institute for Intelligent Analysis and Information Systems
Academia and Think tanks	Delft University

2.2. Stakeholders answering the online survey[16]

Category of stakeholder	MS	Institution
PoC	AT	Federal Chancellery
PoC	BE	National Crisis Center
PoC	BG	DG Fire Safety and Civil Protection – Ministry of Interior
PoC	CZ	Directorate General of Fire Rescue Service – Ministry of Interior
PoC	DE	Federal Ministry of Interior, Building and Community
PoC	DK	Emergency Management Agency
PoC	EE	Ministry of Interior
PoC	EL	Ministry of Citizen Protection
PoC	ES	National Centre for Infrastructure Protection and Cybersecurity
PoC	FI	Ministry of Interior
PoC	FR	Secrétariat général de la défense et la sécurité nationale
PoC	HR	National Protection and Rescue
PoC	HU	National Directorate General for Disaster Management
PoC	IT	Presidency of the Council of Ministers
PoC	LU	Haut-Commissariat à la protection nationale – Ministère d'Etat
PoC	MT	Critical Infrastructure Protection Directorate
PoC	NL	Ministry of Justice and Security
PoC	PL	Government Centre of Security
PoC	PT	National Authority for Civil Protection and the Cabinet of the Secretary General for the Internal Security System
PoC	RO	National Centre for Coordination of Critical Infrastructure Protection – Ministry of Interior
PoC	SE	Civil Contingencies Agency
PoC	SI	Ministry of Defence
PoC	SK	Ministry of Interior
Other ministries	AT	Ministry of Defence
Other ministries	AT	Department of Civil Protection and Disaster Relief - Tyrolean Regional Government
Other ministries	BG	Safety, Technical Supervision and Crisis Management Directorate – Ministry of Transport
Other ministries	CZ	Ministry of Industry and Trade
Other ministries	CZ	Ministry of Transport
Other ministries	EE	Ministry of Economic Affairs and Communications
Other ministries	EL	Ministry of Environment and Energy
Other ministries	EL	Ministry of Environment and Energy

[16] National CI owners/operators organisations are not disclosed for confidentiality reasons.

Category of stakeholder	MS	Institution
Other ministries	EL	Ministry of Infrastructure and Transport
Other ministries	IT	Ministry of Transport and Infrastructure
Other ministries	IT	Ministry of Economic Development
Other ministries	PL	Ministry of Maritime Economy and Inland Navigation
Other ministries	PL	Ministry of Energy
Other ministries	SE	Energy Agency
Other ministries	SE	Transport Administration
Other ministries	SI	Ministry of Infrastructure
Other ministries	SK	Ministry of Economy
CI owners/operators	AT	Three energy operators and one transport operator
CI owners/operators	BG	Two energy operators
CI owners/operators	CZ	One energy operator and one transport operator
CI owners/operators	DE	One energy operator
CI owners/operators	EE	One energy operator
CI owners/operators	EL	Three energy operators and two transport operators
CI owners/operators	ES	One energy operator
CI owners/operators	FI	One energy operator
CI owners/operators	FR	One transport operator
CI owners/operators	IT	One transport operator
CI owners/operators	MT	One transport operator
CI owners/operators	PL	Six energy operators, four transport operators and three operators in other sectors
CI owners/operators	PT	Three energy operators and two transport operators
CI owners/operators	RO	Three energy operators
CI owners/operators	SK	Five energy operators and two operators in other sectors

2.3. Stakeholders engaged in the case studies[17]

MS	Category of stakeholder	Institution
DK	PoC	Emergency Management Agency
DK	Other ministries	Center for Cybersikkerhed
DK	Other ministries	Transport, Construction and Housing Authority
DK	Other ministries	Energy Agency
DK	CI owners/operators	Energy operator
DK	CI owners/operators	Transport operator
ES	PoC	National Center for the Protection of Infrastructures and Cybersecurity
ES	Other ministries	Secretaría de Estado de Infraestructuras, Transporte y Vivienda, Unidad de Emergencias y Coordinación y Gestión de Crisis
ES	Other ministries	Departamento de Seguridad Nacional
ES	Other ministries	Ministerio para la Transición Ecológica
ES	CI owners/operators	Energy operator
ES	CI owners/operators	Transport operator
FR	PoC	Secrétariat Général de la Défense et de la Sécurité Nationale
FR	Other ministries	Ministère de la Transition écologique et solidaire
FR	Other ministries	Ministère de l'Intérieur
FR	CI owners/operators	Energy operator
FR	CI owners/operators	Transport operator
SK	PoC	Department of Civil Protection and Crisis Planning
SK	Other ministries	Ministry of Economy
SK	Other ministries	Ministry of Health
SK	CI owners/operators	Energy operator

[17] National CI owners/operator organisations are not disclosed for confidentiality reasons.

SK	CI owners/operators	Transport operator

2.4. Stakeholders attending the workshops[18]

Category of stakeholder	MS	Institution
PoC	AT	Federal Chancellery
PoC	BE	National Crisis Center
PoC	BG	DG Fire Safety and Civil Protection – Ministry of Interior
PoC	CZ	Directorate General of Fire Rescue Service – Ministry of Interior
PoC	DE	Federal Ministry of Interior, Building and Community
PoC	DK	Emergency Management Agency
PoC	EE	Ministry of Interior
PoC	EL	Ministry of Citizen Protection
PoC	ES	National Centre for Infrastructure Protection and Cybersecurity
PoC	FI	Ministry of Interior
PoC	FR	Secrétariat général de la défense et la sécurité nationale
PoC	HR	National Protection and Rescue
PoC	HU	National Directorate General for Disaster Management
PoC	IT	Presidency of the Council of Ministers
PoC	LU	Haut-Commissariat à la protection nationale – Ministère d'Etat
PoC	LV	Ministry of interior
PoC	MT	Critical Infrastructure Protection Directorate
PoC	NL	Ministry of Justice and Security
PoC	PL	Government Centre of Security
PoC	PT	National Authority for Civil Protection and the Cabinet of the Secretary General for the Internal Security System
PoC	RO	National Centre for Coordination of Critical Infrastructure Protection – Ministry of Interior
PoC	SE	Civil Contingencies Agency
PoC	SI	Ministry of Defence
PoC	SK	Ministry of Interior
CI owners/operators	AT	Energy operator
CI owners/operators	AT	Energy operator
CI owners/operators	BE	European Sea Ports Organisation
CI owners/operators	BE	Community of European Railway and Infrastructure Companies
CI owners/operators	BE	UNIFE
CI owners/operators	BE	SMEunited
CI owners/operators	BE	Operator in another sector
CI owners/operators	BE	Operator in another sector
CI owners/operators	DE	Transport operator
CI owners/operators	EL	Transport operator
CI owners/operators	ES	Energy operator
CI owners/operators	ES	Energy operator
CI owners/operators	MT	Transport operator
CI owners/operators	PL	Energy operator
CI owners/operators	PT	Energy operator
CI owners/operators	RO	Energy operator

[18] National CI owners/operators organisations are not disclosed for confidentiality reasons.

3. SYNOPSIS REPORT OF THE CONSULTATION ACTIVITIES

3.1. Objectives of the consultation

A series of consultations, both with key stakeholders and the public at large, were carried out in conjunction with the evaluation of the implementation of Council Directive 2008/114 on the identification and designation of European critical infrastructures (ECI) in the transport and energy sectors and the assessment of the need to improve their protection (hereafter referred to as either "the Directive" or "Directive 2008/114"). The consultations and the corresponding study will assist the European Commission (EC) in preparing a Staff Working Document presenting the findings of the evaluation and providing recommendations for the improvement of the EU framework for Critical Infrastructure Protection (CIP).

The evaluation leveraged, as a starting point of the analysis, the 2012 review of the European Programme for Critical Infrastructure Protection (EPCIP), the study into the potential impacts of options amending the Directive, and the 2017 Comprehensive Assessment of EU Security Policy. The outcomes of the evaluation may be used to inform future policy work within the CIP field.

A range of stakeholders operating at both EU and MS/national level was consulted using a combination of different consultation tools. The stakeholders can be organised into a number of general categories described in the Table below.

Table 4 – Categories of stakeholders involved

Stakeholder category	
EU level	General public
	EC DGs, other EU Institutions, and EU agencies
	Academia and think tanks
	CI Owners /operators at European level
MS level	PoCs
	Other competent authorities
	CI owners / operators

3.1.1. Consultation methods and tools

MS National Points of Contact (PoC) responsible for CIP were involved throughout the course of the study. The PoCs were asked to validate key desk research concerning the way in which the Directive had been deployed and transposed in their respective MS (which was summarised in an Implementation Table for each MS), provided invaluable input for the four case studies featured in the research (on DK, ES, FR and SK) and participated in a stakeholder workshop in Brussels in November 2018.

Consultation of the general public was carried out through a **Public Consultation in all EU official languages**. This was published on a consultation website hosted on the European Commission's website (ec.europa.eu). The consultation ran for three months, from 19 November 2018 to 11 February 2019.

The Public Consultation was supplemented by **two one-day stakeholder workshops** organised by the Commission, the first on 13 November with MS and related PoCs, and the second on 14 November with CI owners/operators and other industry stakeholders. Each workshop included:

- **Plenary sessions** for the discussion of the study interim findings and the results of the **survey;** and
- **Break-out sessions** in smaller groups to examine in depth some key aspects of the implementation of the ECI Directive according to a sectoral perspective. Specifically, the workshop with MS included three break-out sessions: power plant, gas pipeline, railways. The workshop with CI owners/operators included two break-out sessions: energy and transport.

Moreover, 30 individual **interviews** were conducted with key stakeholders (EU officials, practitioners and members of academia). These included 15 EU officials, eight members of

academia/think tanks and seven CI operators. Moreover, to support triangulation activities and perform MS-level deep dives, an additional 24 interviews were conducted during the course of four national case studies (DK, ES, FR, SK). For each MS selected for the case studies, six interviews were performed: one with the PoC, three with responsible authorities/regulators of the transport and energy sector, and two with network operators in each sector.

The interviewees were selected in agreement with the Commission and were conducted, for the most part, by phone. The interviews were used to confirm the findings of the desk research as well as to delve into greater detail on specific aspects and gap. For instance, interviews with PoCs and competent national authorities were focused on the ECI identification, designation and negotiation process foreseen in the Directive, with a view to perform an analysis that went beyond the assessment of the formal transposition and understand how the Directive is implemented at an operational level. Interviews with members of academia, meanwhile, helped in gaining an understanding of the regulatory scaffolding surrounding the Directive, as well as perceived limitations and areas of improvement. Finally, the involvement of operators allowed the Evaluation team to gain a "field" perspective on the issue. This allowed the team to see how the Directive impacted the work of actors that are the directly involved with the protection of CI in the transport and energy sectors, looking at both areas where the Directive provided clear added value (for instance, by fostering co-operation among the public and private sector in some MS) and areas where the is room for improvement (such as the need to ensure that there is real harmonisation in CI protection procedures across MS).

Finally, a **survey** was deployed using the contractor's survey tool. The survey targeted PoCs, other relevant ministries and national authorities and CI operators. In total, 87 responses were received, 23 from PoCs, 17 from authorities from other Ministries and 47 from CI owners and operators.

In all cases, quantitative data was systematised and assessed in Excel tables, generating corresponding charts and tables to illustrate the main findings that could be gleaned from the analysis activities. Overall, the analysis performed by the Evaluation team included – and was duly informed by - all the information obtained from field research activities.

3.2. Results of the consultation activities

3.2.1. Online survey

The study at hand involved the launching of three surveys, all of which were launched on 12 October 2018 and completed on 9 November 2018. The different surveys targeted PoCs (23 responses), relevant national authorities/ministries (17 responses), and CI operators (47 responses). The results of the surveys are presented below according to the evaluation's main of analysis. From an operational standpoint, all three surveys were initially sent to PoCs, with a request to fill in the survey intended for them and to forward the email with the links to surveys for other relevant national authorities and CI operators to the relevant contacts. As such, while it can be stated that the response rate of the survey sent to PoCs was 82% (23 / 28 responses), response rates for the other two surveys cannot be known, as they depend on the number of times the respective surveys were forwarded.

3.2.1.1. Relevance

Looking at specific threats (such as bombings, cyberattacks, infiltrations and natural disasters), only 40% of PoCs consider the provisions contained in the Directive appropriate to protect CI to a high or very high extent, with another 40% mentioning that it is appropriate to a low extent. Representatives of other Ministries were more uncertain, with 22% mentioning a low relevance of the Directive, 23% mentioning a high/very high relevance and the majority indicating a moderate relevance or lack of sufficient knowledge. On the hand, operators tended to be more sceptical, with 55% mentioning a low relevance in terms of protection against specific threats.

Looking at the definitions contained in the Directive, stakeholders were asked to evaluate their relevance given the requirements of each MS to protect CI in light of current and emerging

threats. Around 40% of PoCs mentioned a low relevance in this area, compared to a quarter of representatives from other ministries and of network operators.

Overall, the survey provides clear supporting evidence that the relevance of the Directive should be improved, especially with regards to the point of view of network operators and especially in terms of protection against specific threats.

3.2.1.2. Effectiveness

Responses from stakeholders indicate that there is evidence that the level of overall protection of ECI in the transport and energy sectors has increased in MS since the introduction of the Directive. This was indicated by around 50% of PoCs, two thirds of representatives from other ministries and three quarters of network operators, which is on the whole quite a convincing majority. Similar responses were recorded concerning the perceived increase in co-operation fostered by the Directive. A large majority of PoCs (90%) also mentioned an increase in co-operation with competent authorities in other MS after the introduction of the Directive, a testament to the effective implementation of the ECIP contact point arrangement. Moreover, three quarters of PoCs also mentioned that the frequency of exchanges of best practices and experiences increased when compared to the situation before the entry into force of the Directive.

Overall, the results of the survey support the conclusions that the Directive was effectively transposed in MS, while the overall effectiveness in fostering a common approach across MS is not clear.

3.2.1.3. Efficiency

A large majority (over 70%) of network operators and of PoCs mentioned that the procedures and requirements introduced by the Directive entailed additional costs (as compared with the situation prior to the existence of the Directive), though there is no consensus among PoCs as to the magnitude of such costs (estimated to be anywhere between 2% and 20% by the majority of respondents). On the other hand, operators viewed the Directive as being much more efficient compared to the opinion of PoCs, with 50% indicating that additional costs are lower than 1%. It is likely that the additional costs reported by PoCs have more to do administrative burden and reporting requirements rather than specific protection measures.

Generally speaking, the Directive does not appear to have caused significant costs to the stakeholders closest to its implementation, namely network operators. On the other hand, there is no consensus amongst PoCs, likely since CIP is managed quite differently across MS, which entails different implementation costs.

3.2.1.4. Coherence

There is scant evidence of regulatory overlap between the Directive and legislation at the national level: 60% of PoC responded that there was no overlap at all or only to a small degree. This however, runs partially counter to the view of network operators, of which 50% mentioned a high degree of overlap. PoCs were more concerned with overlap with EU legislation, with 60% of them reporting a moderate to high overlap (mostly mentioning the NIS Directive). Open responses show that both Directives ask from the MS to identify CI, where the Directive asks for the European CI whereas the NIS Directive identifies national ones. This could imply that different national authorities might have to implement two different Directives with similar scope, and this creates risk of duplications.

3.2.1.5. Added value and sustainability

The majority of network operators (70%) indicate that the repeal of the Directive would have a negative impact on the level of protection of ECI, while a smaller share of PoCs are of the same opinion (40%), with about 15% not knowing the effects of a potential repeal. Concerning the specific added value of the Directive, PoCs mentioned the fact that the Directive facilitated the development and exchange of good practices, guidelines and standards in the CIP field, the fact that it created common terms of reference for the protection of CI in the EU and that it supported

the emergence of a European forum for CIP-related issues. Operators on the other hand placed greater emphasis on the fact that the Directive supported the framing of national policy, measures and initiatives, thereby fostering the creation of a harmonised framework and approach, and that it created common terms of reference for the protection of CI in the EU.

3.2.1. Interviews

Stakeholders from **academia** tended to stress the fact that there are significant differences in how individual MS apply the provisions of the Directive, with particular reference to the specific definitions, as well as on the fact that the scope of applicability of the Directive (namely on energy and transport sectors) might be too limiting. Moreover, academics mentioned that the Directive also possesses some important and interesting elements. For instance, it refers to vital societal functions, focusing on the function offered by the CI rather than simply the "technicalities" of the infrastructure.

Stakeholders from **DGs, EU Institutions and EU Agencies** provided a more structured and institutional feedback. In general, these stakeholders stressed that there is a need to focus on new threats, particularly those represented by cyberattacks. In this sense, stakeholders mentioned that the use of Galileo services represents a particular threat which spills over to other CI. Stakeholders also focused on information-sharing issues, which requires trust that is developed over time. The problem of sharing information is also present at the national level, between different authorities and you need to make sure info is shared.

Representatives from CI associations broadly agreed with the points above, stressing that there is no uniform approach to security and CIP at the national level. This, together with the increased interconnection of the CI, make the system less secure and makes the Directive and similar exercises good initiatives in principle which however are difficult to apply in practice. Moreover, CI associations stressed that the high number of actors involved at both national and EU level creates confusions and slows down the decision-making process.

3.2.2. Workshops

3.2.2.1. Views on the Implementation of the Directive

The following processes were discussed during the workshops:

- **The process of identifying and designating ECI**: Generally speaking, stakeholders agreed that there is significant heterogeneity in the approaches followed at national level by competent authorities to identify ECI, and this appears to be linked to heterogeneous levels of maturity and institutionalisation of the national CIP frameworks. Specifically, notable differences have been reported by PoCs in relation to the interpretation of CI, and to the degree of involvement of operators in the process; and,
- **Co-operation between authorities and operators:** CI owners/operators reported two opposite approaches to co-operation with authorities, one in which *co-operation is centred around authorities* (centre-led, such as in Spain), and one in which *co-operation is pushed mainly by operators* (decentralised) with limited involvement of public authorities (this is the case in Austria and Portugal).

3.2.2.2. Relevance of the Directive

The Directive is considered to be an important first step towards the protection of CI; however, stakeholders agreed on the need to update it to consider the recent policy and security developments (i.e. NIS, cyberthreat, increased terrorist activities, increased interdependence). Moreover, stakeholders discussed the nature of the "common approach" adopted in the Directive, adding that more clarity is needed to determine if the Directive is to be seen as an operational tool or more as a sort of strategic guidance for MS. In the latter case, MS mentioned that a common approach is indeed pivotal, but that harmonisation in terms of procedures might be superfluous, as procedures are designed on the administrative context of a MS and on the security structures, and thus differ by MS. PoCs mentioned that outputs should be the focus, rather than the "nuts and bolts" of CIP that PoCs might not even aware of because they are technical and sectoral issues.

In terms of **definitions** provided by the Directive, stakeholders mentioned that there is no one-size-fits-all approach in defining CI and no homogeneous interpretation of protection. Moreover, operators mentioned that the focus of the Directive on protection of assets is not entirely relevant to the energy sector, since the energy system has a built-in redundancy so that even if an asset of the system is damaged, the service can nonetheless be delivered.

Stakeholders did not reach any conclusive vision on additional **sectors** that might be relevant to include in potential future revisions of the Directive.

3.2.2.3. Effectiveness

Generally speaking, there was a generalised difficulty to **distinguish the effects** that are directly attributable to the Directive from those related to other national and EU initiatives. There was agreement on the limited effects of the Directive on the protection of CI. Some MS reported to have already high levels of security for NCIs prior to the Directive, and others point at the current heterogeneity in the methodologies for risk assessment as the main limitation that currently affects the achievement of a higher level of protection, thus calling for an EU intervention in this regard. Operators agreed on the need to have more methodological guidance (with rail transport sector as a notable exception). In some MS, the Directive was fundamental, as it represented a starting point for CIP in MS (e.g. BE, ES and MT).

Nonetheless, MS acknowledged the positive contribution of the Directive to foster an **increase in the level of awareness** and expertise in CIP. There was overall agreement on the usefulness of having a CIP PoC in all MS.

MS reported various **difficulties in the implementation of the Directive** and identification and designation of ECI. These include, for instance, the handling of classified information, the limited added value of the provisions of the Directive compared to the existing national measures, and heterogeneous relevance of threats to the MS.

3.2.2.4. Efficiency

For the most part, stakeholders found it difficult to distinguish between costs related to the protection of NCIs from costs related to the protection of ECI (even in a hypothetical scenario). Operators raised the issue of limited funding. While the Directive in 2008 allowed operators to invest in security, it lacks enough details and requirements to "justify" current requests for funding in a context on limited national resources.

3.2.2.5. Coherence

The coherence with other legislation was not raised as an issue by operators and PoCs (with the notable exception of the NIS Directive and the rail transport sector). While acknowledging the existence of several sectoral measures, no inconsistencies were identified. Nonetheless, stakeholders mentioned that implementing the Directive was challenging as it links to several other pieces of legislation (e.g. in Galileo) and several DGs to interact with. During the workshops, the fact that the NIS Directive introduced a shift from an object-oriented approach to a service-oriented approach, with MS also going in this direction.

One point that was raised concerned the fact that the ECI Directive has a focus on protection, whereas **service resilience** should also be in focus. The concepts of essential services and resilience are more mature concepts, which embed and go beyond protection and individual assets, to look for systems and the assets that are part thereof.

3.2.2.6. EU added value

There was agreement on the current limited added value of the Directive compared to existing national initiatives. While the EU added value of this piece of legislation is acknowledged at the time when it was firstly introduced, its current EU added value is questioned. Stakeholders underscored that the EU added value of EU action on CIP derives mainly from the EPCIP programme rather than from the Directive. Nonetheless, the creation of CIP PoCs would have not been possible without the Directive and this is one of its greatest achievements.

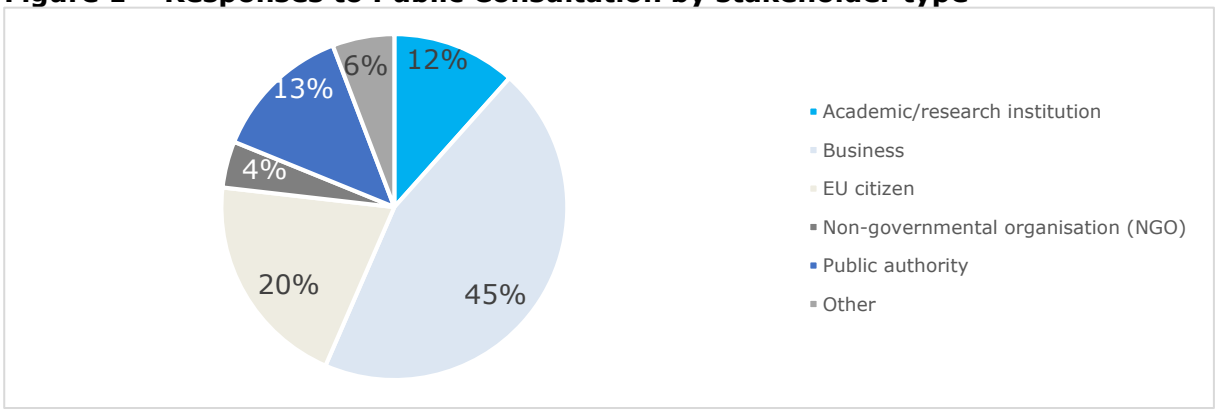
3.2.2.7. Sustainability

There was convergence among workshop participants on the need to update the Directive, which was still viewed as being a necessary instrument, which is now integrated in the national CIP systems of MS.

3.2.3. Public Consultation

A Public Consultation was carried out via the European Commission's website between 19 November 2018 and 11 February 2019 concerning the evaluation of the 2008 European Critical Infrastructure Protection Directive. Overall, 69 responses were received from stakeholders in 19 countries, including EU MS[19] and third countries.[20] Almost half of responses (45%) came from business representatives, followed by individual EU citizens (20%), public authorities (13%) and academia (12%). The overall results are presented in Figure 1.

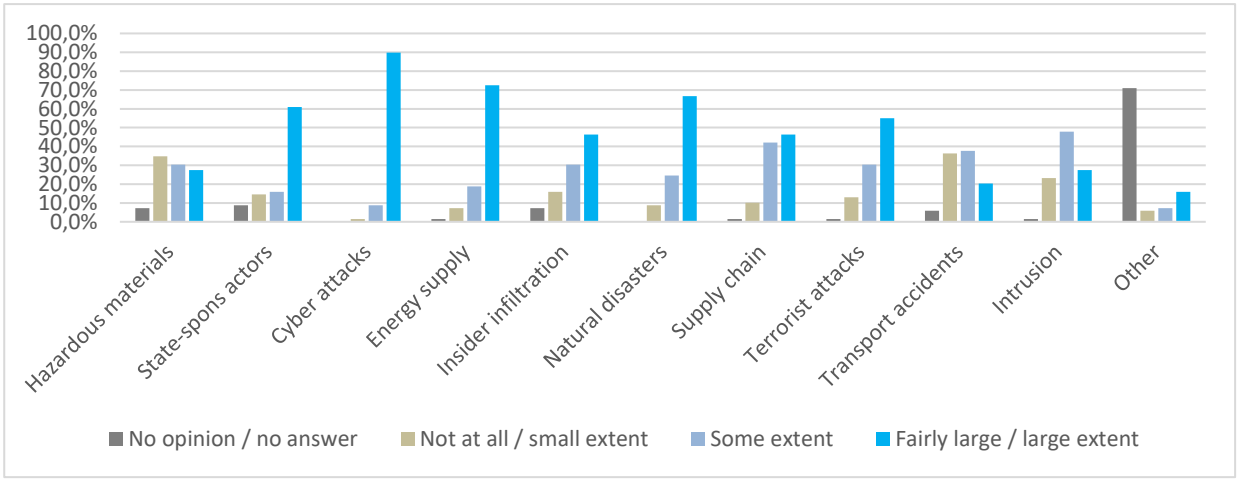
Figure 1 – Responses to Public Consultation by stakeholder type



Moreover, two additional contributions were received by means of specific position papers, as outlined below.

Respondents identified **cyber-attacks and energy supply risks** as the areas posing the most serious threats to CI in the EU, followed closely by natural disasters, attacks from state sponsored actors and terrorist attacks, as illustrated in the Figure 2. Interestingly, transport-related incidents (which along with energy, is one of the two sectors of application of the Directive) were not viewed as particularly serious threats compared to other types of incidents.

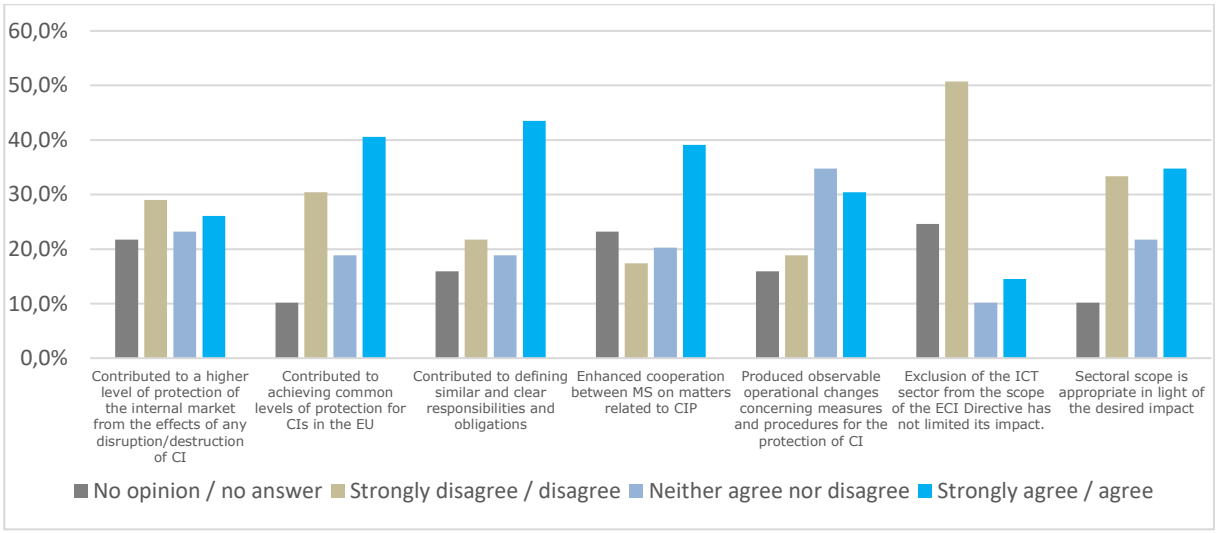
Figure 2 – Incident types posing a serious threat to CI in the EU



[19] AT, BE, BG, CZ, DE, DK, EI, EL, ES, ET, FR, IT, LV, LU, PL, RO, SK, UK.
[20] Turkey.

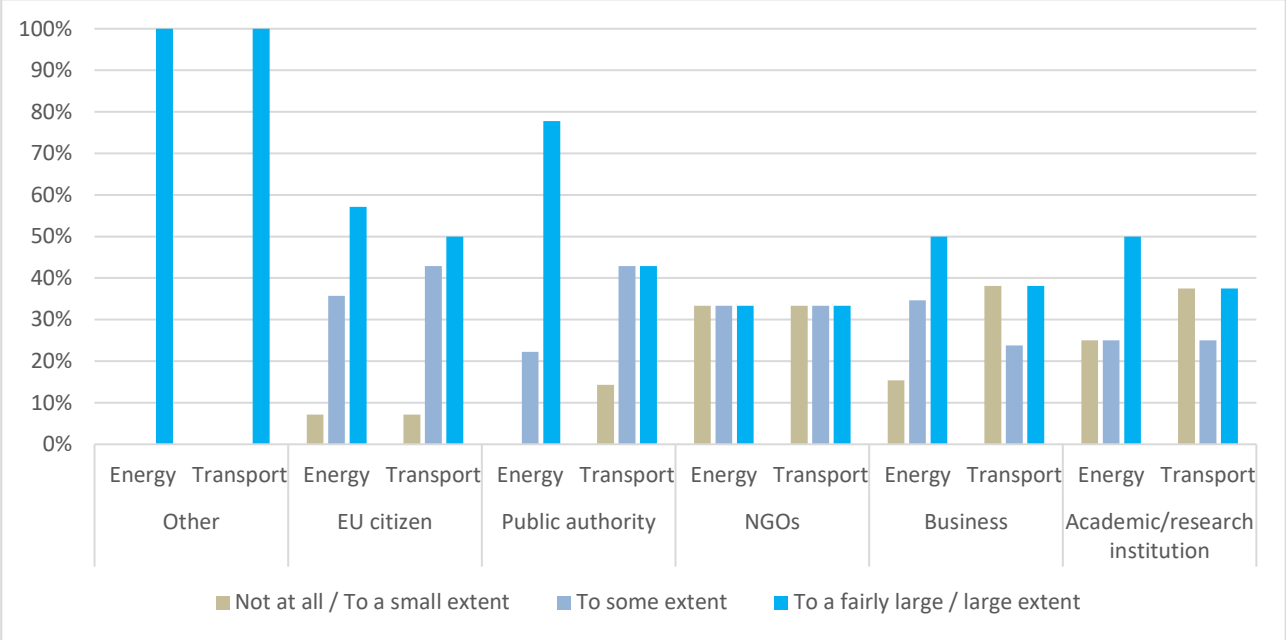
Concerning specific opinions on the effects of the ECI Directive, stakeholders mostly saw the Directive as a way of achieving clear responsibilities and obligations vis-à-vis responsible actors in the CIP sector and as a tool to enhance co-operation amongst MS, also through operational changes to the way CI are protected. On the other hand, respondents considered the exclusion of the ICT sector as a hindrance to the effective deployment of the Directive, while there was uncertainty as to whether the sectoral scope of the Directive is appropriate considering the desired impacts. Moreover, responses from stakeholders indicate there is lack of consensus as to whether the Directive achieved its protection objectives, namely achieving a higher level of protection of CI across MS.

Figure 3 – Effects of the ECI Directive



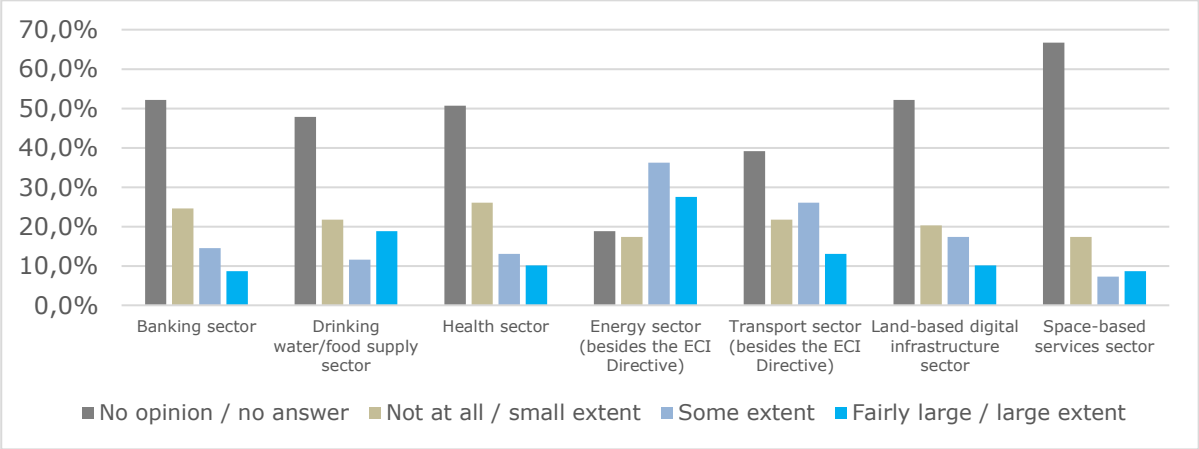
With regards to the ongoing relevance of the ECI Directive, respondents were asked to what extent the provisions of the ECI Directive are still relevant and needed to ensure a common level of protection of CI across the EU, with regard to both the transport and energy sectors. The responses exemplify the different perceptions of stakeholders: while EU citizens tended to consider the Directive to be relevant in both the energy and transport sector, this was not the case for public authorities, which considered the Directive to be more relevant for the energy sector (with almost 80% agreeing to a fairly large or large extent) compared to the transport sector. This view appears to be robust with regard to industry stakeholders, with a higher share of businesses reporting a lower perceived relevance in the transport sector (with close to 40% of responding business stakeholders mentioning that in their view the Directive is not at all relevant or relevant only to a small extent), as well as among academic / research institutions. Finally, NGOs tended to have a more balanced view of the relevance of the directive across both sectors.

Figure 4 – Continued relevance of the ECI Directive



Moreover, with regards to the coherence of the Directive with other sectoral legislation, results from the consultation show that the majority of respondents did not have strong opinions on the subject one way or the other. Generally speaking, stakeholders see the greatest level of coherence with other legislation in the energy sector, while lower degree of coherence are perceived with the banking, healthcare, drinking water/food supply, space and land-based digital infrastructure sectors. Even in the case of the transport sector, more stakeholders responded that the Directive is not coherent with other sectoral legislation compared to those that responded that there is at least some coherence.

Figure 5 – Coherence of the ECI Directive



Finally, there is evidence that a number of respondents provided feedback within the context of organised campaigns launched as a result of the public consultations. As a case in point, three organisations from Austria underscored, using the same terms, the complementarity between the ECI Directive and APCIP (the Austrian cyber-security strategy). Moreover, three German companies mentioned that there are many regulations in Germany that correspond with the level of protection as set out in the ECI; and that no additional action for the water (or energy) sector is needed. Finally, a business association in Belgium and a business in Italy both reported that, in their view the ECI Directive was not applied by the vast majority of MS and, as far as the transport sector is concerned, only a handful of few transport infrastructures have been designated and identified according to the ECI Directive.

3.2.3.1. Other contributions received (position papers or emails)

Two interested parties submitted separate position papers, which revealed 1) that MS some hold that the scope of application of the Directive should be limited to ECI and the extension of the Directive to national infrastructure is not warranted 2) that other stakeholders in the CIP sector (associations and organisations) hold a contrasting view to that of MS, wishing to go further in the integration and harmonisation of CIP.

Concerning the scope of the Directive, the position paper received from a MS stated that leaving the protection of national infrastructures in the competence of the MS would ensure the necessary flexibility, and that the MS-level competence would allow the development of requirements and protection measures, taking into account the specific characteristics of the infrastructure and the region and the needs of the country. In the case of national infrastructures, the guidelines of EPCIP would suffice.

On the other hand, the position paper received from a CIP association mentioned that the current text of the directive fails to take into consideration a common level of CIP across the EU when it comes to topics like: natural disasters (earthquakes, fires, floods, etc.); cyber-attacks and cyber-enabled attacks; supply chain disruptions; terrorist attacks; accident involving hazardous materials; unlawful intrusions (including drones); as well as hybrid threats, and that therefore, in any follow-up on the Directive, the EU should take into account the need to harmonise the protection of critical infrastructures across these possible threats.

The MS further mentioned that it does not does not consider it necessary to increase the stringency of the currently applicable Directive requirements, as the protection and service continuity of the energy and transport sector infrastructure is already regulated in sufficient detail. Moreover, in the opinion of the MS, the protection and continuity of electronic communications services requires further regulation, but outside the Directive currently under consultation. This is due to the fact that, in the view of the MS, it is difficult to independently establish additional standards/requirements on the continuity of communications services in crisis situations, mainly because of the fact that in the case of communications services — similarly to other services the obligation of the Member States to ensure the free movement of services has to be taken into account. Ensuring the continuity of communications services in crises requires the application of more stringent standards/requirements and therefore the establishment of restrictions on the providers of communications services. The Member States' differing approaches to ensuring communications services in crisis situations may thus obstruct the harmonisation of the communications services market and the free movement of services. Attention should also be paid to ensuring the cross-border continuity of communications services, as this is important from the viewpoint of the functioning of the European Union internal market. In the light of this, it was considered important to develop common principles for ensuring communications services in crisis situations.

The position paper of the association is in partial agreement with that of the MS on this point, as in its view the current text of the Directive focuses on CI the disruption or destruction of which would have significant cross-border impact. The Directive thus requests MS to perform an assessment aimed at the identification and designation of the ECI. To this end, MS must go through a cooperative designation process of identifying potential ECI. In the view of the association, this approach has shown not to be the optimal route to ensure an EU-wide level of protection, as the identification process has proved to be slow while the increasing interconnection and interdependence among infrastructures requires a more integrated approach across Europe. In order to fill this gap, the association recommends the definition of a set of common EU criteria to evaluate the status of an ECI, independently from a single MS evaluation.

Finally, the association promoted in its paper the idea to constitute an EU Critical Infrastructure Competence Centre connected to a network of MS Critical Infrastructure Competence Centres. This could be achieved, in the view of the association, by taking stock and inspiration from what has been already proposed in the cybersecurity domain, by establishing National Competence Centres connected through a coordinating European Competence Centre. In this way, MS would be assured that their national interests are properly catered for through the National Competence Centre, whilst taking full advantage of a properly pan-European knowledge sharing system.

3.2.4. Involvement of National Points of Contact in validating desk research

The Evaluation team sent MS PoCs the analysis performed at the national level, concerning the main legislative measures, strategies, administrative procedures and guidelines that have contributed in transposing and implementing the provisions of the Directive. This analysis made it possible to assess how and to what extent the 28 MS implemented the Directive and, where possible, the understanding of the degree to which this led to an improvement of the protection of CI. This analysis featured the in-depth research of national implementation measures reported by MS to the EC and reported in the EUR-Lex portal; moreover, the Evaluation team also extended the scope of the analysis to include recent normative changes affecting the implementation of the Directive in the 28 MS, with the aim of filling in existing gaps and updating the overview with recent changes that occurred after 2012. Specifically, additional regulations and guidelines were analysed (for instance, specifying the contents of OSPs), as well as any updates, revisions to existing measures and new measures directly impacting the national ECIP framework that were made since 2012.

Relevant information was systematised in the draft implementation tables. In order to validate the analysis of national implementation and fill the remaining gaps, the implementation tables were shared with PoCs. PoCs from 25 MS provided feedback on the tables. As some information gaps and grey areas on national implementing practices still existed, the analysis also relied on a number of short supplementary interviews with the relevant PoCs.

3.3. Feedback to stakeholders

The consultation processes provided a wide range of views regarding the implementation of the Directive in terms of what has worked well and what has not worked so well, seen through the eyes of these stakeholders. The meetings with the stakeholders provided an opportunity to promote the engagement of the national authorities, thus enhancing the chances of a good response rate.

The overall objective of this initiative was to evaluate the implementation of Council Directive 2008/114 on the identification and designation of ECI and the assessment of the need to improve their protection. It will assist the EC in preparing a Staff Working Document presenting the results of the evaluation, and suggest recommendations for the improvement of the EU framework for CIP. The preponderance of evidence collected throughout this study indicates that there is a need to update the Directive, making it more streamlined and more system-focused rather than asset-focused (in the spirit of the NIS Directive), while also including a focus on resilience, going beyond mere protection. The consultations with stakeholders clearly indicate that the option to update and review the Directive is preferable to other solutions, including repealing the Directive and replacing it solely with regional co-operation or "soft law" approaches.

4. BIBLIOGRAPHY[21]

Abele-Wigert, I., & Dunn, M. (2006). An inventory of 20 national and 6 international critical information infrastructure protection policies. *International CIIP Handbook*, *1*.

Albrechtsen, E. (2002). *A generic comparison of industrial safety and information security*. Norwegian University of Science and Technology, Trondheim.

Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, *8*, 53–66.

Angori, E., Baldoni, R., Dekel, E., Dingsor, A., & Lucchetti, M. (2012). The Financial Critical Infrastructure and the Value of Information Sharing. Springer, Berlin, Heidelberg.

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.

Bell, L. (2018). Europe is the world's biggest target for DDoS attacks, F5 Networks claims. *ITPRO*.

Black Hat. (2017). The 2017 Black Hat Europe Attendee Survey - The Cyberthreat in Europe. Black Hat.

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". European Commission.

Bossong, R. (2014). The European Programme for the protection of critical infrastructures – meta-governing a new security problem? *European Security*, *23*(2), 210–226.

Bouchon, S., Di Mauro, C., Logtmeijer, C., Nordvik, J. P., Pride, R., Schupp, B., & Thornton, M. (2018). 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. JRC.

Casalicchio, E., & Galli, E. (2008). Metrics for Quantifying Interdependencies. In *Critical Infrastructure Protection II* (ICCIP, Vol. 290, pp. 215–227). Springer.

Castellon, N., & Frinking, E. (2015). Securing Critical Infrastructures in the Netherlands: Towards a National Testbed. The Hague Security Delta.

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.

Chiappetta, A., & Cuozzo, G. (n.d.). Critical infrastructure protection: Beyond the hybrid port and airport firmware security cybersecurity applications on transport. 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems.

CoESS. (2016). Critical infrastructure security and protection: the public-private opportunity. CoESS.

Copeland, B. J. (2019). Artificial intelligence. In *Encyclopedia Britannica*. Encyclopædia Britannica, inc.

CORDIS. (2018). A pan European framework for strengthening Critical Infrastructure resilience to climate change. Horizon 2020.

[21] National legislation considered for the study is listed in Annex II in the implementation tables.

Council of the European Union. (1998). *Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption*. Official Journal of the European Union.

Council of the European Union. (2004). EU Solidarity Programme on the consequences of terrorist threats and attacks. 15480/04, Brussels.

Council of the European Union. (2005). The European Union Counter-Terrorism Strategy. 14469/4/05, Brussels.

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.

Council of the European Union. (2009). *Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products*. Official Journal of the European Union.

Council of the European Union. (2014). *Council Decision 2014/496/CFSP of 22 July 2014 on aspects of the deployment, operation and use of the European Global Navigation Satellite System affecting the security of the European Union and repealing Joint Action 2004/552/CFSP*. Official Journal of the European Union.

Council of the European Union. (2015). Draft Council Conclusions on the Renewed European Union Internal Security Strategy. 2015-2020, Brussels.

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.

Croce, P., Formichi, P., Landi, F., Mercogliano, P., Bucchignani, E., Dosio, A., & Dimova, S. (2018). The snow load in Europe and the climate change. *Climate Risk Management*, *20*, 138–154.

Drozdiak, N. (2018, October 16). Fear of Russian Meddling Hangs Over Next Year's EU Elections. *Bloomberg*.

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

ESPI Workshop. (2018). Shared challenges, varying angles; developing a common understanding of cyber threats and tools for space operations. ESPI.

European Commission. (2004). Communication on Critical Infrastructure Protection in the fight against terrorism. COM(2004) 702 final, Brussels.

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

European Commission. (2006). 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. COM(2006) 787 final, Brussels SEC(2006) 1654.

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

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.

European Commission. (2006). The European Programme for Critical Infrastructure Protection (EPCIP). MEMO/06/477, Brussels.

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 Commission. (2012). Commission Staff Working Document on the review of the European Programme for Critical Infrastructure Protection (EPCIP). SWD(2012) 190 final, Brussels.

European Commission. (2012). Commission Staff Working Document on Transport Security. SWD(2012) 143 final, Brussels.

European Commission. (2013). *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.

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. (2013). Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure. SWD(2013) 318 final, Brussels.

European Commission. (2014). Annex – The urbanisation of Europe and the World. Publications Office of the European Union, Luxembourg.

European Commission. (2014). Communication from the Commission to the European Parliament and the Council - European Energy Security Strategy. COM(2014) 330 final, Brussels.

European Commission. (2015). Commission Directive (EU) 2015/1787 of 6 October 2015 amending Annexes II and III to Council Directive 98/83/EC on the quality of water intended for human consumption. Official Journal of the European Union.

European Commission. (2015). Commission Implementing Regulation (EU) 1998/2015 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security. Official Journal of the European Union.

European Commission. (2015). Commission Implementing Regulation (EU) 2015/1136 of 13 July 2015 amending Implementing Regulation (EU) No 402/2013 on the common safety method for risk evaluation and assessment. Official Journal of the European Union.

European Commission. (2015). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank - A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy. COM(2015) 80 final, Brussels.

European Commission. (2015). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions An Aviation Strategy for Europe. COM/2015/0598 final, Brussels.

European Commission. (2016). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Space Strategy for Europe. COM(2016) 705 final, Brussels.

European Commission. (2016). Next Generation Internet initiative. European Commission.

European Commission. (2016). Proposal for a Regulation of the European Parliament and of the Council on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC. COM(2016) 862 final Brussels.

European Commission. (2016). Proposal for a Regulation of the European Parliament and of the Council on the internal market for electricity. COM(2016) 861 final, Brussels.

European Commission. (2016). Joint Framework on countering hybrid threats a European Union response. Joint Communication to the European Parliament and the Council, JOIN(2016) 18 final.

European Commission. (2017). Commission Staff Working Document Comprehensive Assessment of EU Security Policy. SWD(2017) 278 final Brussels.

European Commission. (2017). Communication Ninth progress report towards an effective and genuine Security Union. SWD(2017) 278 final.

European Commission. (2017). Eleventh progress report towards an effective and genuine Security Union, Communication from the Commission to the European Parliament, the European Council and the Council. COM(2017) 608 final Brussels.

European Commission. (2017). Strengthening EU Disaster Management: rescEU Solidarity with Responsibility Solidarity with Responsibility. COM/2017/0773 final, Brussels.

European Commission. (2018). Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks regulation. COM(2017) 610 final Brussels.

European Commission. (2018). Annex to the Communication from the Commission to the European Parliament, the European Council and the Council. Fifteenth Progress Report towards an effective and genuine Security union. COM(2018) 470 final Brussels.

European Commission. (2018). Commission Delegated Regulation (EU) 2018/762 of 8 March 2018 establishing common safety methods on safety management system requirements pursuant to Directive (EU) 2016/798 of the European Parliament and of the Council and repealing Commission Regulations (EU) No 1158/2010 and (EU) No 1169/2010. Official Journal of the European Union.

European Commission. (2018). Commission Staff Working Document on the ex post evaluation of the 'Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks' 2007-2013 Programme (CIPS). SWD(2018) 331 final, Brussels.

European Commission. (2018). Communication from the Commission to the European Parliament, the European Council and the Council. Fifteenth Progress Report towards an effective and genuine Security union. COM(2018) 470 final Brussels.

European Commission. (2018). Geopolitical Outlook for Europe; confrontation vs co-operation. EPSC Brief.

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.

European Commission. (2018). Evaluation of the EU Strategy on adaptation to climate change, Accompanying the document Report from the Commission to the European Parliament and the Council on the implementation of the EU Strategy on adaptation to climate change. Commission Staff Working Document, SWD(2018) 461 final.

European Commission. (2018). JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL: Increasing resilience and bolstering capabilities to address hybrid threats. JOIN(2018) 16 final.

European Commission and High Representative of the Union for Foreign Affairs and Security Policy. (2016). Joint Communication to the European Parliament and the Council Joint Framework on countering hybrid threats a European Union response. JOIN(2016) 18 final, Brussels.

European Council. (2009). The Stockholm Programme — An open and secure Europe serving and protecting citizens (2010-2014). 17024/09, Brussels.

European Environment Agency. (2017). Disasters in Europe: more frequent and causing more damage. European Environment Agency.

European Parliament. (2012). European Parliament Resolution of 12 June 2012 on Critical Information Infrastructure Protection: towards global cyber-security. P7_TA(2012)0237, Strasbourg.

European Parliament. (2018). Hearing The Security of Critical Infrastructures and Public Spaces. List of presentations presented at The Security of Critical Infrastructures and Public Spaces, Brussels.

European Parliament and Council of the European Union. (2004). Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security. Official Journal of the European Union.

European Parliament and Council of the European Union. (2005). Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security. Official Journal of the European Union.

European Parliament and Council of the European Union. (2007). Note on NATO's role in Critical Infrastructure Protection. Publications Office of the European Union, Luxembourg.

European Parliament and Council of the European Union. (2008). Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002. Official Journal of the European Union.

European Parliament and Council of the European Union. (2009). Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II). Official Journal of the European Union.

European Parliament and Council of the European Union. (2012). Directive 2012/18/EU of the European Parliament and the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances and repealing Council Directive 96/82/EC (known as Seveso III). Official Journal of the European Union.

European Parliament and Council of the European Union. (2013). Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC. Official Journal of the European Union.

European Parliament and Council of the European Union. (2013). Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism. Official Journal of the European Union.

European Parliament and Council of the European Union. (2013). Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC. Official Journal of the European Union.

European Parliament and Council of the European Union. (2013). Regulation (EU) No 462/2013 - see Regulation (EC) No 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit rating agencies - consolidated version. Official Journal of the European Union.

European Parliament and Council of the European Union. (2013). Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012. Official Journal of the European Union.

European Parliament and Council of the European Union. (2013). Regulation (EU) No 1285/2013 of the European Parliament and of the Council of 11 December 2013 on the implementation and exploitation of European satellite navigation systems and repealing Council Regulation (EC) No 876/2002 and Regulation (EC) No 683/2008 of the European Parliament and of the Council (Galileo Regulation). Official Journal of the European Union.

European Parliament and Council of the European Union. (2014). Decision No 541/2014/EU of the European Parliament and of the Council of 16 April 2014 establishing a Framework for Space Surveillance and Tracking Support. Official Journal of the European Union.

European Parliament and Council of the European Union. (2014). Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU. Official Journal of the European Union.

European Parliament and Council of the European Union. (2014). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). Official Journal of the European Union.

European Parliament and Council of the European Union. (2014). Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012. Official Journal of the European Union.

European Parliament and Council of the European Union. (2014). Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU). Official Journal of the European Union.

European Parliament and Council of the European Union. (2015). Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. Official Journal of the European Union.

European Parliament and Council of the European Union. (2016). Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016 on railway safety. Official Journal of the European Union.

European Parliament and Council of the European Union. (2017). Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010 (Gas Supply Directive). Official Journal of the European Union.

European Parliament and Council of the European Union. (2018). Proposal for a Directive of the European Parliament and of the Council on the quality of water intended for human consumption (recast). COM(2017) 753 final Brussels.

European Union. (2016). A Global Strategy for the European Union's Foreign And Security Policy, European Union Global Strategy. Publications Office of the European Union, Luxembourg.

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.

Europol. (2015). Exploring tomorrow's organised crime. Europol.

Europol. (2017). Internet Organised Crime Threat Assessment. IOCTA.

Europol. (2017). Terrorism Situation and Trend Report. Europol.

Forzieria, G., Bianchi, A., Silva, F., Marin Herrera, M., Leblois, A., & Lavalle, C. (2018). Escalating impacts of climate extremes on critical infrastructures in Europe. *Global Environmental Change*, *48*, 97–107.

Fritzon, Å., Ljungkvist, K., Boin, A., & Rhinard, M. (2007). Protecting Europe's Critical Infrastructures: Problems and Prospects. *Journal of Contingencies and Crisis Management*, *15*(1), 30–41.

Giannopoulos, G., & Schimmer, M. (2011). Memorandum on the results of the sixth Workshop on the Implementation and Application of the Directive. JRC.

Giroux, J., & Melkunaite, L. (2013). Information Sharing for Critical Energy Infrastructure Protection: Finding value & overcoming challenges. *Energy Security Forum*, (8), 20–22.

Goldammer, J. G. (2017, August 8). Fires in Europe Fuelled by Urbanisation and Climate Change. UNISDR.

Governing Council of the European central Bank. (2014). *Regulation of the European Central Bank (EU) No 795/2014 of 3 July 2014 on oversight requirements for systemically important payment systems (ECB/2014/28)*. Official Journal of the European Union.

Hämmerli, B., & Renda, A. (2010). Protecting Critical Infrastructure in the EU - CEPS Task Force Report. CEPS.

Jahier, K. (2014). *Presentation on Critical infrastructure protection within NATO*.

Johansson, G. (2018, October 25). Cyber-attacks one of the biggest threats to the world in 2018 says WEF. *SC Magazine*.

Johnson, C. W. (n.d.). Understanding Failures in International Safety-Critical Infrastructures: A Comparison of European and North American Power Failures. University of Glasgow.

JRC. (2012). Presentation of Christian Krassnig at the 1st international Workshop on Regional Critical infrastructures Protection Programmes. Publications Office of the European Union, Luxembourg.

Karagiannis, G. M., Turkesezer, Z. I., Alfieri, L., Feyen, L., & Krausmann, E. (2017). Climate change and critical infrastructure – floods. JRC.

Kobie, N. (2015). What is the internet of things?

Lazari, A. (2014). *European Critical Infrastructure Protection*. Springer.

Lazari, A., & Simoncini, M. (2016). Critical infrastructure protection beyond compliance - Analysis of national variations in the implementation of Directive 114/08/EC. *Global Jurist*, *16*(3), 267–289.

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.

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.

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

Moteff, J., & Parfomak, P. (2004). Critical Infrastructure and Key Assets: Definition and Identification - CRS Report for Congress. Congressional Research Service.

Nepal, R., & Jamasb, T. (2013). Security of European electricity systems: Conceptualizing the assessment criteria and core indicators. *International Journal of Critical Infrastructure Protection*, *6*(3–4), 182–196.

Newman, L. H. (2018, December 2). Now cryptojacking threatens critical infrastructure, too. *Wired*.

Nieuwenhuijs, A., Luiijf, E., & Klaver, M. (2008). Modeling Dependencies In Critical Infrastructures. In *Critical Infrastructure Protection II* (ICCIP, Vol. 290, pp. 205–213). Springer.

OSCE. (2013). Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace. OSCE.

Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety*, *121*, 43–60.

Park, D., Summers, J., & Walstrom, M. (2017). Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks. The Henry M. Jackson School of International Studies.

Peter, G. (2017, March 20). Critical infrastructures under daily attack. Horizon - The EU Research & Innovation Magazine.

Pezard, S., Radin, A., Szayna, T., & Larrabee, F. (2017). European Relations with Russia: Threat Perceptions, Responses, and Strategies in the Wake of the Ukrainian Crisis. RAND Corporation.

Poustourli, A., Ward, D., Zachariadis, A., & Schimmer, M. (2015). An overview of European Union and United States critical infrastructure protection policies. In *12th International Conference "Standardization, Protypes and Quality: A means of Balkan Countries' Collaboration"* (pp. 549–557). Kocaeli University Foundation.

Pursiainen, C. (2018). Critical infrastructure resilience: A Nordic model in the making? *International Journal of Disaster Risk Reduction*, *27*, 632–641.

Rahman, H. A., Armstrong, M., Marti, J., & Srivastava, K. D. (2011). Infrastructure interdependencies simulation through matrix partitioning technique. *International Journal of Critical Infrastructures*, *7*(2), 91–116.

Ramboll. (2012). Study into the potential impacts of options amending council Directive 2008/114/EC. European Commission.

Regling, K. (2016). *The European economy after the crisis*. Singapore.

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

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2002). Identifying, understanding, and analysing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, *21*(6), 11–25.

Rubin, A. J. (2018, August 4). Scorching Summer in Europe Signals Long-Term Climate Changes. *New York Times*.

Scalangi, P. (2007). Scalangi, P.L., (2007), Moving Beyond Critical Infrastructure Protection to Disaster Resilience, Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience, CIP Program Discussion Paper Series. In *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience* (pp. 73–86). George Mason University.

Secrétariat général de la Défense et de la Sécurité nationale, & ET DE LA SECURITE NATIONALE. (2014). *Instruction Generale Interministerielle Relative a La Securite Des Activites D'importance Vitale N°6600/SGDSN/PSE/PSN du 7 janvier 2014*. Journal officiel de la République française.

Setola, R. (2014). Security Liaison Officer Project - Final Report. European Commission.

Setola, R., & Theocharidou, M. (2016). Setola, R., Luiijf, E., Theocharidou, M., (2017), 'Critical Infrastructures, Protection and Resilience', in Managing the Complexity of Critical Infrastructures, 1-18. In *Managing the Complexity of Critical Infrastructures* (Vol. 90, pp. 1–18). Cham: Springer.

Shakou, L. M. (2017, March). *Impacts of climate change on CI*. Presented at the Workshop on Critical Infrastructure Protection and Climate Change, Nicosia.

Steer Davies Gleave. (2016). Study on options for the security of European high-speed and international rail services. European Commission.

Theocharidou, M., & Giannopoulos, G. (2015). Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. Publications Office of the European Union, Luxembourg.

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.

Trend Micro. (2018). How cryptocurrency is shaping today's threat environment.

UNISDR. (2009). UNISDR Terminology on Disaster Risk Reduction. United Nations.

United Nations. (2017). Building State Prevention, Response Capacities Essential for Protecting Critical Infrastructure from Terrorist Attacks. SG/SM/18436-SC/12715.

Utah State University. (2017). A drier south: Europe's drought trends match climate change projections. EurekAlert.

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.

World Economic Forum. (2015). Deep Shift: Technology Tipping Points and Societal Impact. Global Agenda Council on the Future of Software & Society.

World Economic Forum. (2018). The Global Risks Report 2018, 13th Edition. Insight Report

5. THE ECI DIRECTIVE

5.1. Description of the key provisions of the Directive

Provision	Article	Description	Stakeholders concerned
Scope and definitions	1, 2, 3.3, 14	The purpose of the Directive is to create a horizontal EU process for identifying and designating ECI, and set out an approach for improving their protection. The Directive applies only to the energy and transport sectors (specific subsectors are laid down in Annex I), although the Directive leaves room for expanding its sectoral scope upon subsequent revision. In this regard, priority is given to the ICT sector. The Directive is addressed to 28 EU MS and is applicable to EEA countries.[22] Six definitions are laid down under this provision to define key terminology used for the purpose of the Directive, including 'CI', 'ECI', and 'protection'.	• Member States • Commission • Owners/operators
Identification of the ECI	3	The Directive requires MS to identify potential ECI through the following procedure (detailed in Annex III): (1) Application of the sectoral criteria to make an initial selection of NCIs in the scope of the Directive; (2) Application of the Directive's definition of 'CI' to the selected NCI; (3) Application of the trans-boundary element of the Directive's definition of ECI; (4) Application of cross-cutting criteria (i.e. possible casualties, economic effects, effect on the public), which specify thresholds to evaluate the impact of any disruption of the selected CI. This assessment should consider the existence of alternatives and the time of disruption/recovery. The Directive provides that thresholds must be defined on a case-by-case basis bilaterally or multilaterally by the MS concerned by the potential ECI. MS are also under the obligation to inform the Commission yearly on the number of infrastructures per sector for which discussion on thresholds were held. The Commission may step in the identification process either upon request of a MS or on its own initiative to draw attention on potential ECI. Moreover, the Commission may facilitate the application of the identification procedure by providing the MS with specific guidelines.[23] The MS and the Commission must continue the process of identifying potential ECI on an ongoing basis.	• Member States • Commission
Designation of the ECI	4	The Directive provides for EU countries to go through a cooperative designation process for potential ECI located on their territory. Each MS shall inform other MS that may be significantly affected by a potential ECI about its identification, and engage with them in bilateral/multilateral discussions aimed	• Member States • Commission • Owners/operators

[22] By the Decision of the EEA Joint Committee No 101/2012 of April 30, 2012.
[23] The JRC has developed the "Non-binding guidelines for the application of the Council Directive on the identification of European Critical Infrastructure and the assessment of the need to improve their Protection". The Guidelines were published on November 11, 2008, few days before the adoption of the Directive.

Provision	Article	Description	Stakeholders concerned
		at reaching an agreement on the designation of the CI as ECI. In this regard, the final decision ('acceptance') rests with the MS on whose territory the ECI is located. The latter MS is also under the obligation to inform both the Commission (annually, on the number of designated ECI and the number of MS that may be significantly affected) and the owner/operators of the designated ECI. The Commission acts as a facilitator. It may participate in MS' discussions but shall not have access to information allowing for the identification of the CI under discussion. Moreover, it may facilitate the dialogue between MS, in particular case where a MS believes that it may be significantly affected by the disruption of a CI located on the territory of another MS which has not been identified as potential ECI.	
Operator security plans (OSPs)	5	Each MS is required to verify that an Operator Security Plan (OSP) is in place for each ECI. The purpose of the OSP, whose minimum content is laid down in Annex II, is to identify the critical assets of the ECI, as well as the existing security solutions for protecting them. If an OSP in not in place, the MS must ensure that such plan is developed by the owner/operator and reviewed regularly within one year following the designation of the ECI (otherwise, in exceptional circumstance, an extension can be agreed and notified to the Commission). In case the MS finds that an OSP or equivalent already exist for each designated ECI and updated regularly, no further implementation measure shall be taken.	• Member States • Commission • Owners/operators
Security Liaison Officers (SLOs)	6	Each MS is required to ensure that a Security Liaison Officer is designated for each ECI. The officer serves as the contact point between the owner/operator of the ECI and the national authority concerned. If a Security Liaison Officer does not exit, the MS must ensure that such officer is identified by the owner/operator. In case the MS finds that a Security Liaison Officer or equivalent already exist for each designated ECI, no further implementation measure shall be taken.	• Member States • Owners/operators
Reporting	7	The Directive requires MS to carry out threat assessments in relation to ECI within 1 year following the designation of CI. Moreover, they must report general data to the Commission on the types of risks, threats and vulnerabilities per ECI sector in which an ECI has been designated every 2 years. Based on the outcome of these exercises, the Commission and the MS shall assess whether further protection measures shall be taken on occasion of the review (to begin on 12 January 2012).	• Member States • Commission
Commission support for ECI	8	The Commission is required to support, through the relevant MS authority, the owners/operators of designated ECI by sharing available best practices and methodologies as well as support training and the information exchange on new technical developments related to CI protection.	• Member States • Commission • Owners/operators
ECIP contact points	10	Each MS must appoint a ECIP contact point to coordinate ECIP-related issues within the MS, with other MS and with the Commission.	• Member States

5.2. Workflow of activities described in the ECI Directive

The Directive provides a workflow of activities structured according to three phases: the identification of the ECI (phase 1); the designation of the ECI (phase 2); and the protection of the ECI (phase 3), as shown in Figure 6.

Generally speaking, the process provided by the Directive involves three types of actors: **MS** (i.e. the relevant CIP authorities responsible for implementing the Directive at MS level); **the EC**; and **owners/operators of ECI**.

For the sake of simplification, the flowchart below presents the ECI process in the context of bilateral negotiations between MS, although the Directive allows for multilateral discussions as well. Therefore, Member State 1 corresponds to the 'hosting state', i.e. the MS on whose territory the potential ECI is located and which has to take the final decision on its designation as ECI, while Member State 2 refers to the MS that would be significantly affected by the disruption or destruction of the potential ECI.

Moreover, it should be kept in mind that the process depicted below is a recurring one, as the Directive calls both the Commission and the MS to continue the process of identifying potential ECI on an ongoing basis (Article 3), and stipulates that the process of identifying and designating ECI should be reviewed on a regular basis (Article 4), possibly also removing the CI from the ECI list. Similarly, owners/operators of ECI shall review the OSPs regularly (Article 5).

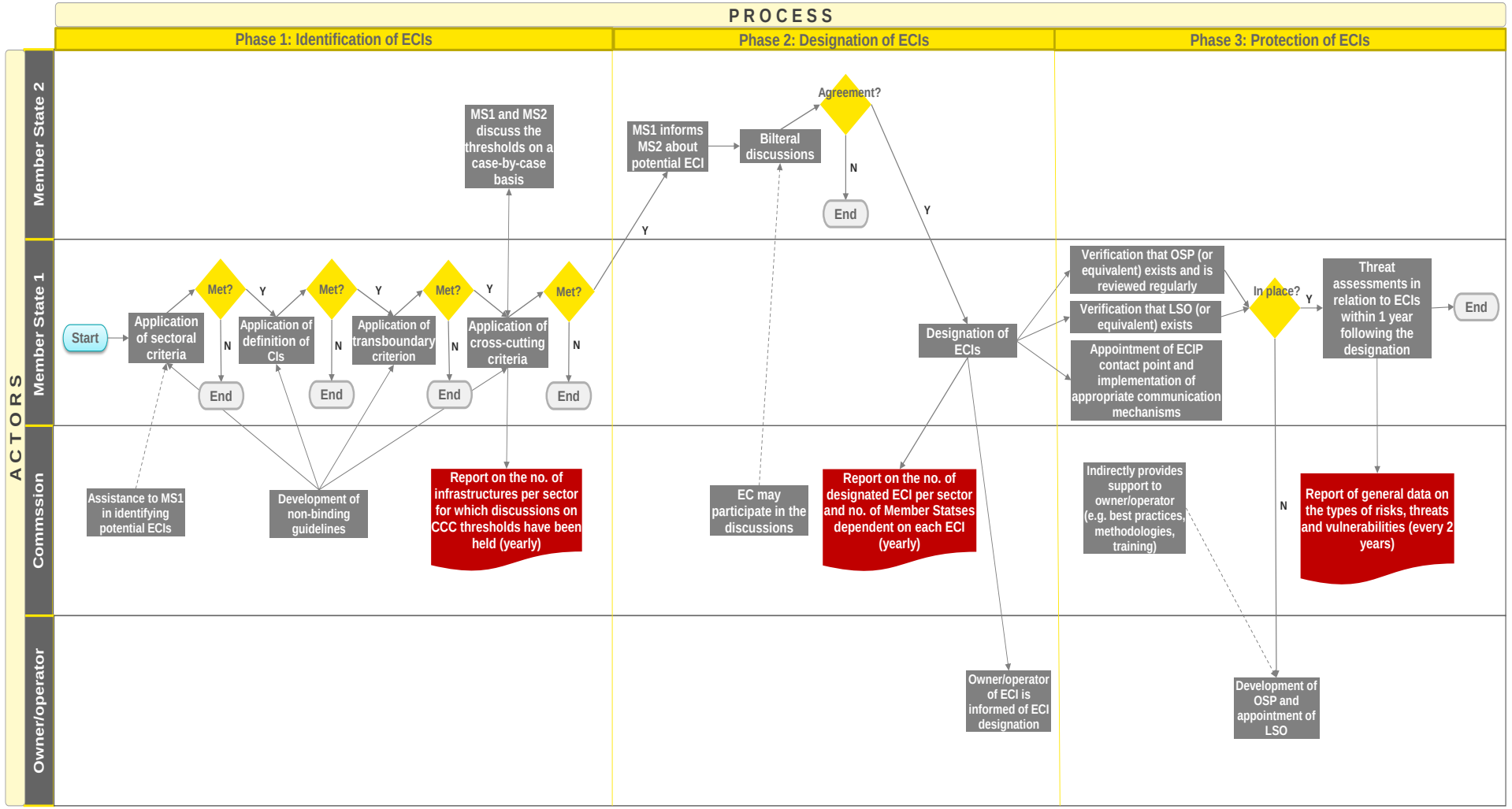
During the *identification phase*, **Member State 1** carries out the four-step procedure for the identification of ECI laid down in Annex III of the Directive. If a potential ECI fails to meet the requirements of any of the sequential steps, it shall be regarded as non-ECI and the identification procedure shall be terminated. To apply the procedure, Member State 1 shall also start a collaboration with **Member State 2** to determine the thresholds for the cross-cutting criteria. Member State 1 reports to the **Commission** on the number of infrastructure per sector for which discussions on the thresholds have been held on yearly basis. The Commission may support Member State 1 in identifying potential ECI, either on its own initiative or upon request, and acts as a facilitator by developing non-binding guidelines for the implementation of the identification procedure.

During the *designation phase*, **Member State 1** notifies to **Member State 2** the identification of a potential ECI on its territory and starts bilateral discussions on the actual designation. The **Commission** may be involved in such discussion, although without access to information allowing for the identification of the potential ECI. In case Member State 1 and Member State 2 reach an agreement, the infrastructure under discussion is designated as ECI by the MS on whose territory it is located. Member State 1 shall report about the ECI designation to the Commission (on an annual basis) and shall inform the **owner/operator** of the CI concerned.

In the *protection phase*, **Member State 1** verifies that the **owner/operator** has already put in place both an OSP (or equivalent) to be reviewed regularly, and a SLO (or equivalent). If this is not the case, Member State 1 must ensure that the owner/operator of the ECI prepares an OSP and appoints a SLO. Moreover, to ease coordination and information exchange on ECI-related issues, Member State 1 appoints an ECIP contact point and establishes appropriate communication mechanisms. To ensure a high level of protection, Member State 1 conducts threat assessments in relation to the ECI within 1 year following its designation and reports general data to the **Commission** on the types of risks, threats and vulnerabilities every 2 years. Moreover, through Member State 1, the Commission indirectly supports the owner/operator providing access to best practices and methodologies as well as training and exchange of information on new technical developments in the CI protection field.

The Team are aware that other relevant categories of stakeholders (namely **academia and think tanks**, and the **general public**) might be relevant to the evaluation of the Directive insofar as they can provide valuable insights to assess the relevance of the current scope and definition of the Directive and its impacts on security. These stakeholders will be targeted by specific consultation activities to factor their views and opinions into the evaluation exercise, as requested by the Technical Specifications. However, since these stakeholders are not directly involved in implementing activities, and in order to achieve a better rationalisation of the ECI process designed by the Directive, they are not included in the flowchart below.

Figure 6 - Workflow of activities in the ECI process established by Directive 2008/114/EC



Source: author's elaboration

6. EVIDENCE SUPPORTING THE IMPLEMENTATION STATE OF PLAY

6.1. Recent developments in national legislation

National transposition legislation has, for the most part, remained the same since the study conducted in 2012, with very few MS performing changes since then.

France is one key MS that has provided clarifications to the transposition legislation in the 2012-2018 period. The legal framework concerning the transposition of the Directive in France is quite unique, as the MS considered that no formal transposition of the Directive was needed, judging that its national legislative framework on CIP already adequately addressed the points raised by the Directive.[24] Indeed, France saw no need to formally transpose the Directive given the fact that it considered its Defense Code and Instruction no. 6600 SGDN/PSE/PPS of September 26, 2008 as already sufficiently comprehensive.[25] The French legislation, for instance, already called for drawing up Operator Security Plans (*Plan de sécurité d'opérateur*), established the presence of Security Liaison Officers and already had set up mechanisms for the identification of CI.[26] However, the legislation was updated in 2014, directly referencing the Directive and providing greater clarity and additional details on the obligations of the MS and of critical infrastructure operators, on practical aspects of the ECI identification process and on the negotiation process with other MS for the designation of ECI, in which for instance it is clarified that the Directive does not impose any particular rules or methods for this, so the bilateral/multilateral agreement can simply take the form of an informal exchange of letters between the governments of the respective MS, and thus does not require prolonged and complex formal ratification processes.[27]

Besides France, other MS that updated their transposition legislation include Estonia, Romania, Bulgaria and Spain.

Estonia also produced legislative innovation in recent years. The implementation of the Directive was originally performed through amendments to the existing national CIP framework.[28] Recently, in July 2017, Estonia promulgated a new "Emergency Act", amending provisions relevant to the implementation of the Directive, such as the performance of sectoral risk analyses.[29]

Romania recently revised legislation relevant to the national transposition of the Directive. In previous research it was shown that Romania had leveraged the Directive to support the development of a comprehensive CIP law, and also cited the Directive as a stimulus for the development of a CIP-focused centre, namely the Centre for Coordination of Critical Infrastructure Protection within the Ministry of Administration; this was established with Emergency Ordinance no. 98 of 03/11/2010 on the identification, designation and protection of critical infrastructures.[30] Significant modifications to the Ordinance were performed in 2015 and 2018:

- Law 344/2015, published in the Official Monitor no. 970 on December 28th, 2015; and,
- Law 225/2018, published in the Official Monitor no. 677 on August 3rd, 2018.

These updates to the national legislation on CIP also impacted ECI-related provisions. For example, Law 344/2015 specifies that the designation of ECI is based on a simple "written

[24] Lazari, A. (2014). European Critical Infrastructure Protection. Springer.
[25] Code de la défense, version consolidée. Instruction Générale Interministérielle Relative à La Sécurité Des Activités D'importance Vitale, N°6600/SGDN/PSE/PPS du 26 septembre 2008.
[26] Ibid.
[27] Instruction Générale Interministérielle Relative à La Sécurité Des Activités D'importance Vitale, N°6600/SGDSN/PSE/PSN du 7 janvier 2014, section 7 (Les Infrastructures Critiques Européennes).
[28] Based on the "Emergency Act", passed 15 June 2009.
[29] "Emergency Act", in force since 01 July 2017, Article 4.
[30] 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".

consent" of the competent authorities in Romania and the impacted MS, rather than through a formal agreement as was originally written in the transposition legislation. This was due to the fact that the term "agreement" often has a more complex meaning in national legislation, which was making the designation process more bureaucratic.[31] The issue concerning the form of the agreement with another MS, as mentioned above, was also indirectly addressed by French legislation, in the spirit of fostering simplification in this area.

Law 225/2018, on the other hand, expanded on the concept of Critical Infrastructure Protection, describing it as a unitary set of processes and activities organised and conducted to ensure the functionality, continuity of services and integrity of national CI and ECI to discourage, diminish and neutralise threats, risks and vulnerabilities.[32] The Law also provided additional details on the definition, role and function of Security Liaison Officers and OSP,[33] on the OSP in particular, the 2018 Law clarifies that responsible public authorities in different sectors shall ensure, within one year of the designation of an infrastructure as a CI/ ECI, that there is a PSO or equivalent.[34]

Bulgaria amended its national transposition legislation (originally adopted in 2011, namely the "Disaster Protection Act" - SG 80/11, in force from 14/10/2011) in February 2013.[35] As was the case with Romania, changes here mostly involved and sought to clarify specific aspects of the transposing legislation, concerning chiefly the performance of threat assessments.

Spain also introduced new legislation impacting the ECI through *Real Decreto* 12/2018, promulgated on 7 September 2018, concerning the security of networks and information systems. This law is closely linked to Directive 2016/1148/EU (known also as the "NIS Directive"); however, it is clarified that its scope of application includes the CI sectors (which are identified in previous legislation transposing Directive 2008/114). Crucially, the new legislation clarifies that an "operator" shall be identified as an operator of essential services if an incident suffered by the operator is likely to have significant disruptive effects on the provision of the service, considering at least the following factors:

- In relation to the importance of the service provided:
    - The availability of alternatives to maintain a sufficient level of provision of the essential service; and
    - The assessment of the impact of an incident on the provision of the service, evaluating the extent or geographical areas that could be affected by the incident; the dependence of other strategic sectors on the essential service offered by the entity and the impact, in terms of degree and duration, of the incident on economic and social activities or on public safety.
- In relation to the clients of the operator:
    - The number of users who place their trust in the services provided by the entity; and
    - Its market shares.

Spain therefore made an effort to integrate the transposition of the NIS Directive into its existing CI/ECI framework; the transposition was also an opportunity to further specify certain aspects of the transposition legislation on ECI, which remains in force to this day.

Moreover, **Croatia** transposed the Directive in view of its accession to the EU. In this case, a National Law on Critical Infrastructures was promulgated in 2013, which implemented the

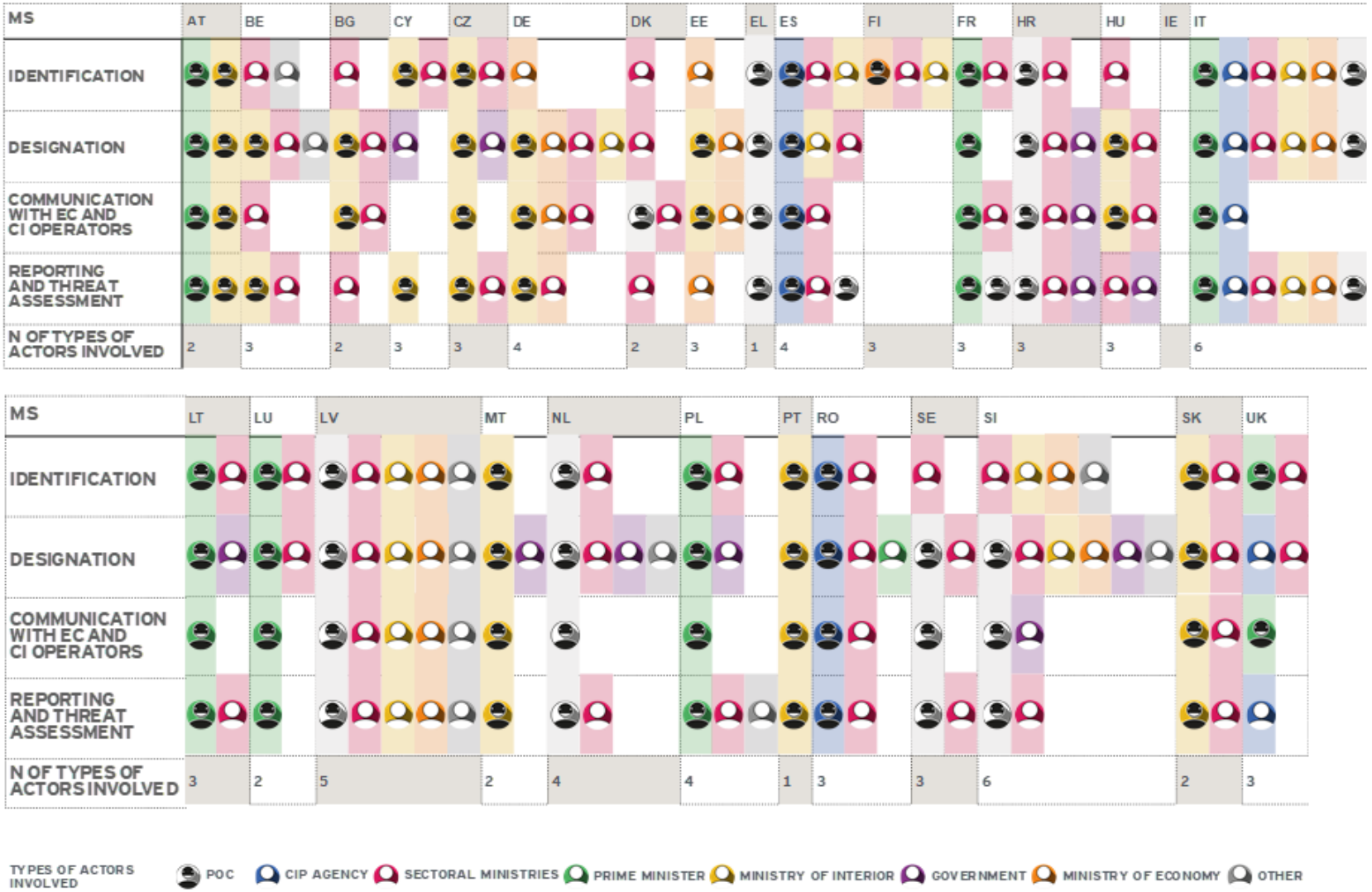
[31] Law 225/2018, published in the Official Monitor no. 677 on August 3rd 2018, as well as further contextual elaboration by the Romanian POC on the Implementation Table.
[32] Law 225/2018, published in the Official Monitor no. 677, article 3.
[33] Ibid.
[34] Law 225/2018, published in the Official Monitor no. 677, article 11.
[35] Decree No 38 of 18 February 2013 for the adoption of the Regulation on the Procedure for the Establishment and Designation of European Critical Infrastructures in the Republic of Bulgaria and the Measures for their Protection.

Directive into national law and which also provides for a process of regulation and oversight for both national and European CI.[36] Through this law, a critical infrastructure security and resilience system was consolidated in the MS. Moreover, two key legislative measures were subsequently implemented pursuant to the National Law on Critical Infrastructures:

- The first is the Decision on designation the sectors from which the central state administrative bodies identify national critical infrastructure and lists of the order of the sectors of critical infrastructures (Decision on Designation). A total of eleven sectors have been determined from which ministries (the central administrative bodies) can identify the national CI. These are: Energy, Communications and IT technology, Transport, Public health, Water management, Food, Finance, Production, storage and transport of hazardous materials, Government sector, National monuments, and Science and education;[37] and,
- The second document, titled the Rules on the methodology for drafting business risk analysis of critical infrastructure, determines the guidelines, criteria and measurements for CI identification and risk analysis management.[38]

[36] National law on Critical Infrastructures n. 56/2013.
[37] Decision on Designation the Sectors from which the Central State Administrative Bodies Identify National Critical Infrastructure and Lists of the Order of the Sectors of Critical Infrastructures), in Official Gazette, No 108/2013.
[38] Rules on the Methodology for Drafting Business Risk Analysis of Critical Infrastructure), in Official Gazette, No 128/2013.

6.2. National CIP administrative set-up[39]



[39] In DE and EE, the Ministry of Economy is the authority in charge for the sectors in scope.

7. EVIDENCE SUPPORTING THE ANALYSIS OF THE RELEVANCE

7.1. Relevance of definitions included in the Directive

Term	Stakeholder views on the relevance of the definition	Other considerations on the relevance of the definition	Overall assessment
Critical infrastructure (CI)[40]	• Six interviewees consider the definition of CI to be appropriate.[41] Overall, a small majority (51%) of survey respondents from other ministries and CI operators agree to a high and very high extent that the CI definition is helpful to the process of identifying CI. Just under half (44%) of PoC respondents agree with the same statement, with the majority (52%) agreeing to a moderate or low extent.[42] • A number of caveats are also highlighted by study stakeholders (below). • The definition of CI is considered broad and lacking in clarity in some areas.[43] In particular, 'vital functions' could be more clearly defined.[44] Nonetheless, the broad nature of the CI definition allows for tailoring to national environments when transposing the Directive as part of national legislation.[45]	• Within the wider definition of CI, the Directive does not define certain specialised terms. In not offering clear definitions, this could result in differences of interpretation of the terms between MS, particularly when translated into different national languages.[50] • The CI definition provided in the Directive has led to the identification of many new national CI and has been linked in the reviewed literature to improved awareness of threats and vulnerabilities relating to CI.[51]	The definition of CI is **moderately – though not entirely – appropriate**, with areas for improvement identified, particularly in relation to providing specific guidance for MS on what is 'critical' and defining specialised terms more clearly, namely 'assets' and 'systems'.

[40] An asset, system or part thereof located in MS which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a MS as a result of the failure to maintain those functions. (*Source: Article 2 (a)*)
[41] Interview: 2 CI owners/operators, 1 Academia and think tanks and 3 EC DGs and Agencies.
[42] Survey: 74% (N=17) of PoCs, 69% (N=11) of Other ministries, 81% (N=35) of CI owners/operators agree to a moderate/high/very high extent that definitions included in the Directive are helpful to the process of identifying CI.
[43] Interview: 1 Academia and think tanks and 1 CI owner/operator.
[44] Interview: 1 Academia and think tanks.
[45] Case study: 1 MS.
[50] 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".
[51] Giannopoulos, G., & Schimmer, M. (2011). Memorandum on the results of the sixth Workshop on the Implementation and Application of the Directive. JRC.

Term	Stakeholder views on the relevance of the definition	Other considerations on the relevance of the definition	Overall assessment
	• The definition of CI does not include an explanation of the terms 'services', 'assets' or 'systems'.[46] • Further guidance on what is deemed to be 'critical' would be helpful to MS.[47] • The definition omits 'supra-national' CI which are linked to more than one MS (e.g. financial sector).[48] • The definition does not consider third countries, however their CI might be related to EU security.[49]		
European critical infrastructure (ECI)[52]	• One interviewee considers the definition of ECI to be appropriate.[53] Additionally, a small majority (57%) of respondents across PoC, other ministries, and CI operators agree to a high and very high extent that the definitions included in the Directive are helpful to the process of identifying ECI.[54] • Nonetheless, several caveats are highlighted by interviewees (below). • The distinction between European and non-European is outdated in the light of increased connectedness.[55]	• The ECI definition does not account for the increased interconnectedness of CI across MS and third countries, focusing instead on 'CI located in MS.' However, CI failure in third countries can affect the vital societal functions of MS (e.g. the 2003 power supply blackout in Italy due to an incident in Switzerland).[57] • Very few ECI have been identified by MS and the literature reviewed	The definition of ECI is **moderately – though not entirely appropriate**, due to its focus only on CI located in MS, with areas for improvement identified particularly in relation to increased interconnectedness.

[46] Workshop: PoCs; Case study: 1 MS.
[47] Interview: 1 CI owner/operator and 4 EC DGs and Agencies.
[48] Interview: 2 EC DGs and agencies.
[49] Interview: 2 EC DGs and agencies.
[52] 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.
[53] Interview: 1 academia and think tanks.
[54] Survey: 87% (N=20) of PoCs, 83% (N=14) of Other Ministries, 87% (N=35) of CI owners/operators agree to a moderate/high/very high extent that definitions included in the Directive are helpful to the process of identifying ECI.
[55] Interview: 1 EC DGs and Agencies.
[57] European Commission. (2018). Communication from the Commission to the European Parliament, the European Council and the Council. Fifteenth Progress Report towards an effective and genuine Security union. COM(2018) 470 final Brussels. Johnson, C. W. (n.d.). Understanding Failures in International Safety-Critical Infrastructures: A Comparison of European and North American Power Failures. University of Glasgow.

Term	Stakeholder views on the relevance of the definition	Other considerations on the relevance of the definition	Overall assessment
	• The definition lacks a perspective on networks and interdependencies.[56]	suggests that the cross-cutting criteria used to help define ECI lacks clarity.[58]	
Risk analysis[59]	• The definition also lacks clear details on the practical steps involved in conducting this type of assessment.[60]	• Analysis of the Directive text indicates a lack of practical detail on what the risk analysis should include.	The definition of 'risk analysis' is **not entirely appropriate**, lacking clear detail on the practical steps involved in the assessment.
Sensitive CIP-related information[61]	• Applicable information not provided in stakeholder engagement.	• Applicable information not provided in desk research.	There is **not enough data** available to assess the relevance of the definition
Protection[62]	• Two interviewees consider that the 'protection' definition does not include clear operational detail (e.g. a crisis management plan).[63] • According to three interviewees, the lack of focus on 'resilience' as part of 'protection' reduces the usefulness of the definition.[64] • According to workshop participants, 'resilience' is a more mature concept than 'protection', as it captures interdependencies between CI.[65]	• Efforts to secure CI have prioritised 'protection' – as reflected in the Directive – but there has been a shift 'from protection towards resilience' in recent years.[66]	The definition of 'protection' is **not entirely appropriate**, as it does not include a focus on resilience.
Owners/ operators of ECI[67]	• The Directive defines owners/operators of ECI, but does not focus on CI owners/operators - which two interviewees consider equally as	• Applicable information not provided in desk research.	This definition is **not entirely appropriate**, as it lacks a focus on CI owners/operators.

[56] Interview: 4 EC DGs and Agencies; Workshop: CI owners/operators and PoCs.
[58] Lazari, A. (2014). European Critical Infrastructure Protection. Springer.
[59] Consideration of relevant threat scenarios, in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure.
[60] Workshop: CI owners/operators.
[61] Facts about critical infrastructure, which if disclosed could be used to plan and act with a view to causing disruption or destruction of critical infrastructure installations.
[62] All activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability.
[63] Interview: 2 EC DGs and agencies and 2 CI owners/operators.
[64] Interview: 3 EC DGs and agencies.
[65] Workshop: POCs.
[66] Setola, R., & Theocharidou, M. (2016). Setola, R., Luijf, E., Theocharidou, M., (2017), 'Critical Infrastructures, Protection and Resilience', in Managing the Complexity of Critical Infrastructures, 1-18. In *Managing the Complexity of Critical Infrastructures* (Vol. 90, pp. 1–18). Cham: Springer.
[67] Those entities responsible for investments in, and/or day-to-day operation of a particular asset, system or part thereof designated as an ECI under the Directive.

Term	Stakeholder views on the relevance of the definition	Other considerations on the relevance of the definition	Overall assessment
	important to CIP due to increased interconnectedness of systems.[68]		

7.2. Relevance of the Directive to stakeholder needs

Stakeholder category	Needs	Relevance of Directive 114 to stakeholder needs
MS	• Ensuring that CIP is included in MS national agendas.[69] • Ensuring that a broad range of interconnected sectors across Europe are supported by the Directive.[70]	**Partially relevant:** • Most national authorities consider the Directive relevant to CI protection,[71] especially in its provisions on the OSP, the SLO, and the creation of CIP PoCs. • The Directive helps ensure that CIP is included in MS agendas. It does this by providing a definition of CI (Article 2a), and stipulating that the process for ECI identification and designation pursuant to Article 3 should be repeated on a regular basis (Article 4, Section 6). • However, the definition of CI does not consider third countries, despite the potential relevance of their CI to EU security.[72] Moreover, the bilateral/multilateral meeting format (Article 4, Section 2) is not perceived by MS to provide the best framework for discussing CIP.[73] • Although the Green Paper (2006) identified 9 CI sectors, the Directive only focuses on energy and transport. This limited sectoral focus is not sufficient to consider possible domino effects that involve vital CI such as healthcare and government.
EC	• Providing MS and CI operators/owners with an overarching framework for CIP	**Partially relevant**: • Even though it is not possible to assess the extent to which there is currently a common level of protection of CI across MS[76], differences

[68] Interview:2 EC DGs and agencies.
[69] 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".
[70] Lazari, A. (2014). European Critical Infrastructure Protection. Springer.
[71] Survey: on average, 76% of PoCs and 90% of Other ministries find the provisions relevant for CI protection from a moderate, to a high or very high extent.
[72] Survey: 1 PoC. Interview: 1 EC DGs and Agencies; Case study: 1 MS.
[73] Giannopoulos, G., & Schimmer, M. (2011). Memorandum on the results of the sixth Workshop on the Implementation and Application of the Directive. JRC.
[76] PC: 45% (N=28) of respondents agree and strongly agree with the fact 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.

Stakeholder category	Needs	Relevance of Directive 114 to stakeholder needs
	offering the same level of protection across MS. • Maintenance of a well-functioning internal market, which depended on an integrated approach to transnational CI.[74] • Protecting ECI and pan-European assets in a way that is responsive to changes in the threat landscape and wider contextual changes.[75]	remain between MS in terms of definitions, perception of risks (and hence criteria and thresholds to assess the significance of the impact) and details of requirements (e.g. on the OSP and SLO). This is likely associated with different levels of protection of CI and ECI across MS. • The Directive has partially addressed the need of clarifying rights and obligations for stakeholders, as it has defined the CIP PoCs, the SLO and the obligations for national authorities to carrying out a threat assessment and for ECI operators to develop an OSP. However, there are national variations across MS as to the way in which these rights and obligations understood and applied. • The Directive only focuses on CI located in MS, and therefore pan-European assets fall out of its scope, despite the importance EPCIP has placed on protecting these. Further, the Directive has not been updated since 2008, and it is not fully adapted to developments that have occurred since its publication, although it does retain sufficient flexibility due to the general way in which the Directive is written.
CI owners/ operator (energy and transport sectors)	• Safeguarding security of energy supply (e.g. gas/electricity),[77] quality of water for human consumption,[78] and transport security.[79] • Remaining agile to changing threats/wider contextual developments.[80]	**Partially relevant**: • The Directive provides an overarching framework for CIP – thus supporting CI owners'/operators' efforts to safeguard transport and energy security at a fairly high level.[82] • In general, CI owners/operators answering the survey find the provisions in the Directive relevant to the protection of CI, with some sectoral differences.[83]

[74] European Commission. (2013). Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure. SWD(2013) 318 final, Brussels.
[75] European Commission. (2017). Communication Ninth progress report towards an effective and genuine Security Union. SWD(2017) 278 final PART 1/2.
[77] EUR-Lex (2006), Directive 2005/89/EC of the European Parliament and of the Council of 18 January 2006 concerning measures to safeguard security of electricity supply and infrastructure investment (Text with EEA relevance), OJ L 33, 4.2.2006, p. 22–27.
[78] EUR-Lex (1998), Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption, OJ L 330, 5.12.1998, p. 32–54.
[79] EUR-Lex (2017), Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010 (Text with EEA relevance), OJ L 280, 28.10.2017, p. 1–56.
[80] European Commission. (2017). Communication Ninth progress report towards an effective and genuine Security Union. SWD(2017) 278 final PART 1/2.
[82] Bossong, R. (2014). The European Programme for the protection of critical infrastructures – meta-governing a new security problem? *European Security*, *23*(2), 210–226. Interview: 3 EC DGs and Agencies.
[83] Survey: on average, 83% of CI owners/operators find the provisions of the Directive relevant for CI protection from a moderate, to a high or very high extent.

Stakeholder category	Needs	Relevance of Directive 114 to stakeholder needs
	• Improving knowledge and understanding among on-the-ground law enforcement personnel of CI and CIP.[81]	• Overall, the Directive has sufficient flexibility to adapt to changes in wider context, given that definitions and procedures are described in a generalised way that can be adapted to broader contextual developments. • However, in some cases CI operators/owners consider the OSP to be an 'additional measure' that may impact their competitiveness due to the application of European legislation.[84] • The Directive does not mandate information-sharing in relation to CI among stakeholders – other than requiring MS to share information regarding ECI –which means that those in charge of protecting CI, such as police officers, may not be aware of the Directive, or of the importance of CIP.[85]

7.3. Relevance of the Directive to current and future threats

Threat	Description	Considerations on overall relevance of the Directive to threats	Overall assessment
Terrorism	While terrorist attacks continue to present a threat to CI,[86] Europol has noted a shift in Islamist terrorist attacks away from attacks on infrastructure (such as 9/11, UK 2005 attacks, Spain 2004 attacks), to 'soft targets', attempting to	The Directive identifies terrorism as a key threat for CIP, and this view is echoed by survey respondents.[88] It dates back to 20 October 2004, where the EC adopted a Communication on critical infrastructure protection in the fight against terrorism. However, when looking at the terrorist incidents in Europe between 2006 and 2017,[89] while a few attacks appear to have been aimed at the transport sector, attacks have primarily targeted businesses, followed by government, and religious figures and institutions.[90] Therefore, the limited sectoral scope does not consider the	Mixed relevance of Directive to the terrorism threat. On one hand, the overall terrorist threat to Europe is still high. However, terrorist attacks primarily tend to target sectors other than energy and transport.

[81] Case study: 1 MS; Interview:1 CI owner/operator.
[84] Lazari, A. (2014). European Critical Infrastructure Protection. Springer.
[85] Interview: 1 CI owner/operator. On average, 84% of CI owners/operators in the energy sector find the provisions relevant for CI protection from a moderate, to a high or very high extent, against 80% of CI owners/operators in the transport sector.
[86] Workshop: PoCs; Interview: 1 Academia and think tanks, 3EC DGs and agencies, 4 CI owners/operators.
[88] Survey: 75% (N=15) of PoCs, 76% (N=13) of Other ministries, and 70% (N=32) of CI owners/operators respondents consider 'bombing' as a moderate/high/very high threat to CI.
[89] Based on data from the Global Terrorism Database.
[90] Global Terrorism Database (2018), Search criteria: Years (between 2006-2017), All incidents, Targets (Business; Government (General); Airports and Aircraft; Educational Institution; Food or Water Supply; Journalists & Media; Maritime; Religious Figures/Institutions; Telecommunication; Transportation; Unknown; Utilities), Attacks (Hijacking; Facility/Infrastructure Attack), Region (Western Europe; Eastern Europe).

Threat	Description	Considerations on overall relevance of the Directive to threats	Overall assessment
	kill and wound as many people as possible.[87]	broader threat from terrorism, which affects a much wider range of sectors and CI.	
Natural hazards (including earthquakes, volcanic eruptions, flooding)[91]	Extreme weather events, in part due to climate change, could bring about increasing damage to CI in Europe.[92] The impact of climate change would be felt across sectors, but could be particularly harmful to energy and transport, due to the direct impact of environmental changes on these infrastructures.[93] Certain natural hazards, such as flooding, are also deemed to be a threat to CI.[94]	The Directive highlights that "natural disasters […] should be considered in the critical infrastructure protection process".[95] Research shows that Europe is currently experiencing damage from a range of natural climatic events, with natural disasters set to increase in the coming years, with damages likely tripling by the 2020s.[96] According to this research, applicable industries (including heavy industries, and water/waste treatment systems), the transport sector, and the energy sector will be most affected.[97] Therefore, the sectoral scope appears to be appropriate for this specific threat. However, it has been noted by the European Environment Agency that natural disasters are becoming more frequent and causing more damage, and in this light, the 'twice-per-year' reporting structure on risks, threats, and vulnerabilities (Article 7) is unlikely to be responsive enough with regards to the fast-paced climatic changes.	Mixed relevance of Directive to the threat from natural hazards. On one hand, the transport and energy sectors are particularly vulnerable to the effects of natural events. However, the twice-per-year reporting structure is not suited to rapidly evolving climate change.

[87] Europol. (2017). Terrorism Situation and Trend Report.
[91] European Commission. (2017). Eleventh progress report towards an effective and genuine Security Union, Communication from the Commission to the European Parliament, the European Council and the Council. COM(2017) 608 final Brussels.
[92] Interview: 2 EC DGs and Agencies, 2 Academia and think tanks.
[93] Forzieri, G., Bianchi, A., Silva, F., Marin Herrera, M., Leblois, A., & Lavalle, C. (2018). Escalating impacts of climate extremes on critical infrastructures in Europe. *Global Environmental Change*, *48*, 97–107.
[94] Survey: regarding the extent to which earthquakes, volcanic eruptions, and flooding would represent a threat to CI, on average 55% of respondents (on average 68% of PoCs; 65% of Other ministries; 46% of CI owners/operators) agreed that flooding was a threat to a high/very high extent. In comparison, the majority of respondents across all three groups (on average 82%) agreed that volcanic eruptions posed a low to no threat to CI. Answers were more mixed regarding earthquakes, with 28% (N=5) of PoCs respondents considering the threat from earthquakes to be of a high and very high extent, compared to 59% (N=10) of Other ministries respondents and 42% (N=19) of CI owners/operators.
[95] Official Journal 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, L345/75, Section 3 p. 1.
[96] European Environment Agency. (2017). Disasters in Europe: more frequent and causing more damage.
[97] Forzieria, G., Bianchi, A., Silva, F., Marin Herrera, M., Leblois, A., & Lavalle, C. (2018). Escalating impacts of climate extremes on critical infrastructures in Europe. *Global Environmental Change*, *48*, 97–107.

Threat	Description	Considerations on overall relevance of the Directive to threats	Overall assessment
Cyber-attacks from organised crime groups and state actors	Cyber threats have increased, particularly given the growing use of ICT in the functioning of CI.[98] Cyber-attacks from state and non-state actors are a growing issue for CI, in terms of cyber espionage as well as cyber-attacks on CI, such as the attack on Ukraine's power grid by Russia-backed hackers.[99] Attacks by state-sponsored actors have risen, and online organised crime is also a growing threat to CI.[100]	The Directive highlights that "technological threats…should be taken into account in the critical infrastructure protection process".[101] Since 2008, the threat from cyber-attacks has increased – a development that is linked to the increased interconnectedness of different systems and sectors on a global scale.[102] The latest Europol report on Internet organised crime and cyber-attacks shows that cyber threats affect a number of CI beyond energy and transport: banking, financial market and infrastructures, the health sector, the drinking water supply and distribution, and digital infrastructure.[103] Despite the limited coverage of the cyber threats, the Directive can be considered to some extent as one of the main triggers that served to increase the maturity of cyber security for oil and gas, and for CI owners/operators. Prior to the Directive, there were protections in place against physical threats such as human error, terrorism and natural disasters, but cyber security was mainly treated from an information protection perspective, rather than a holistic systems approach. Annex II of the Directive pointed out also "security of information systems". That was a trigger to also include the cyber aspect within protection.[104]	Partial relevance of Directive to the threat from cyber-attacks in relation to organised crime groups and state actors, given that these attacks target not only energy and transport, but a wide range of sectors. The contribution of the Directive to increasing the maturity of cyber security for CI owners/operators should be noted.
Insider infiltration	Insider infiltration – referring to a malicious threat to an organisation from people inside the	Insider infiltration is a type of 'man-made threat', a wider category that is mentioned in the Directive. The Directive recognises the classification restrictions around sharing identified CI with other MS (Article 9, Paragraph 1), but does not outline	Low relevance of Directive to the threat from insider infiltration, as the Directive's means of implementation

[98] Interview: 3 Academia and think tanks, 9 EC DGs and Agencies, and 6 CI operators.
[99] Park, D., Summers, J., & Walstrom, M. (2017). Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks. The Henry M. Jackson School of International Studies. Interview: 1 EC DGs and agencies; Survey: cyberattack was generally regarded as a central threat by survey respondents across all three groups, with 90% (N=20) of PoCs, 85% (N=15) of Other ministries, and 80% (N=37) of CI owners/operators agreeing that cyber is a threat to CI to a high and very high extent.
[100] Bell, L. (2018). Europe is the world's biggest target for DDoS attacks, F5 Networks claims. *ITPRO*.
[101] Official Journal 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, L345/75, Section 3 p. 1.
[102] European Commission. (2017). Commission Staff Working Document Comprehensive Assessment of EU Security Policy. SWD(2017) 278 final Brussels.
[103] Europol. (2017). Internet Organised Crime Threat Assessment.
[104] Feedback from one of the experts of the team, based on fieldwork experience in supporting CI operators in the development of security plans.

Threat	Description	Considerations on overall relevance of the Directive to threats	Overall assessment
	organisation – has grown in prevalence in the years following the introduction of the Directive.[105] It was also highlighted as a threat to CI by survey respondents.[106]	similar security vetting requirements to be performed by owners/operators of CI, such as for Security Liaison Officers (Article 6).[107]	(Article 6) do not include a focus on security vetting of Security Liaison Officers in order to address this threat.
Hybrid threats	Hybrid threats – which encompass multidimensional activities with the aim of destabilising countries - have increased in importance and are considered a major threat.[108]	Hybrid threats use various tools and tactics, including 'diplomatic, military, economic, and technological'[109] means to destabilisation, come under the Directive's 'all-hazard' approach. While it is recognised that energy supply chains and the transport sector are particularly vulnerable to hybrid threats, the cybersecurity aspect more generally has been highlighted as needing to be addressed.[110] Additionally, the importance of reinforcing resilience of CI against hybrid threats has been highlighted by the Commission, although 'resilience' itself is not a concept which is included within the Directive.[111]	Low relevance of the Directive to hybrid threats, as the Directive does not include the concept of resilience – which has been noted as essential in responding to hybrid threats – and the limited sectoral scope of the Directive does not encompass the range of sectors that could be targeted by hybrid campaigns.

[105] Interview: 1 academia and think tanks; 1 CI owner/operator and 3 EC DGs and agencies; Case study: 1 MS.
[106] Survey: 79% (N=15) of PoCs, 65% of Other ministries (N=11), and 70% (N=32) of CI owners/operators stated that insider threats are a moderate/high/very high threat to CI.
[107] Setola, R. (2014). Security Liaison Officer Project - Final Report. European Commission. Interview: 1 academia and think tanks; 1CI owner/operator and 3 EC DGs and Agencies
[108] European Commission. (2016). Joint Framework on countering hybrid threats a European Union response. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, JOIN(2016) 18 final; European Commission. (2018). JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL: Increasing resilience and bolstering capabilities to address hybrid threats. JOIN(2018) 16 final; Interview feedback: three EC DG and agencies representatives.
[109] European Commission. (2018). JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL: Increasing resilience and bolstering capabilities to address hybrid threats. JOIN(2018) 16 final.
[110] European Commission. (2018). JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL: Increasing resilience and bolstering capabilities to address hybrid threats. JOIN(2018) 16 final.
[111] European Commission. (2016). Joint Framework on countering hybrid threats a European Union response. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, JOIN(2016) 18 final.

7.4. Relevance of Directive to advances since 2008

Category of changes	Main changes	Relevance of Directive 114 to changes
Technological/ scientific	• Technological advances have continued to progress at a rapid pace over the last 10 years, with advances in a range of science and technology areas. In particular, the expansion of the Internet of Things (IoT),[112] Artificial Intelligence (AI),[113] Next Generation Internet (NGI)[114] and autonomous systems have increased connectivity and reliance on automated systems.[115] • The growing accessibility of technology has led to greater reliance on networked resources,[116] as well as an increasing reliance on digitalised systems across sectors.[117] • These technological developments have contributed to greater vulnerability of CI to cyber threats.[118] This increases the possibility of cyber-attacks against CI, perpetrated by terrorism or organised criminals,[119] which has become increasingly digitalised and reliant on ICT. • Certain nation-states have also lost their 'technological edge' – that is, their more advanced technological capabilities compared to those of their adversaries – which include both non-state and nation-state actors – as adversary technological capabilities have improved in recent years, increasing the vulnerability of nation-states.[120]	**Partial relevance:** • The Directive is partly relevant to the technological and scientific changes taking place since 2008. • On the one hand, these changes have heightened the need for an overarching CIP framework, and survey evidence indicates that technological and scientific changes have increased the relevance of the Directive.[121] • On the other hand, the Directive is not well-adapted with regards to technological/ scientific advances due to its limited sectoral scope, which does not take into account the interconnections with other sectors, and the possible 'domino effect' of one sector's failure impacting others.

[112] Kobie, N. (2015). What is the internet of things?. IoT is the process of connecting everyday objects to the Internet so they can communicate with the users and between themselves.
[113] Copeland, B. J. (2019). Artificial intelligence. In *Encyclopedia Britannica*. AI is a computer or robot's ability to process tasks to the same level or beyond the abilities of a human.
[114] European Commission. (2016). Next Generation Internet initiative. Setola, R. (2014). Security Liaison Officer Project - Final Report. European Commission. NGI, otherwise known as the Internet of the future, is an initiative to ensure increase privacy, openness, and inclusion in an increasingly connected society.
[115] Interview: 3 EC DGs and agencies, 2 academia and think tanks and 2 CI owners/operators.
[116] Interview: 1academia and think tanks.
[117] World Economic Forum. (2015). Deep Shift: Technology Tipping Points and Societal Impact. Global Agenda Council on the Future of Software & Society.
[118] Johansson, G. (2018, October 25). Cyber-attacks one of the biggest threats to the world in 2018 says WEF. *SC Magazine*.
[119] Case study: 1 MS.
[120] Interview: 1 academia and think tanks.
[121] Survey: 37% (N=7) of PoCs, 75% (N=9) of Other ministries, and 63% (N=25) of CI owners/operators.

Category of changes	Main changes	Relevance of Directive 114 to changes
Economic	• The financial crisis of 2008 and the European sovereign debt crisis of 2010 have contributed to an underinvestment in CI in the period after 2008.[122] • New forms of currencies such as cryptocurrencies have increasingly been used by members of the general public, particularly since 2017.[123] Cryptocurrencies can make it more straightforward to carry out certain cyber-attacks.[124] Increasing use of cryptocurrencies has also led to the rise of 'cryptojacking'; that is, the unauthorised use of someone else's connected device to 'mine' cryptocurrencies. Certain CI are a target for cryptojacking, such as industrial plants, due to the high level of computing power and electricity available for cryptomining. For example, in 2018 a cryptocurrency mining malware targeted a European water utility's SCADA servers, which could have disrupted the plant's functions.[125] However, reports of CI being victim of cryptojacking are rare.	**Relevant:** • The majority of survey respondents consider that economic factors have *not* affected the relevance of the Directive.[126] • While the Directive does not currently address economic developments, such as the increased prevalence of cryptocurrencies, the Directive has sufficient flexibility for CI owners/operators to adapt to wider changes to the economic environment, given that procedures and definitions are described in a generalised way.
Social	• Europe is predominantly urban, with around three-quarters of the total EU population living in cities, towns and suburbs.[127] Urbanisation leads to a concentration of CI,[128] as well as a high burden placed on the existing CI who have to cater for a larger number of people. Therefore, the potential of impactful CI failures which can affect large numbers of people, particularly in light of the increasing interconnectivity of systems.[129] • Urbanisation, combined with other factors such as climate change, can also contribute to natural disasters such as fires which – in turn – can also adversely affect CI.[130]	**Partial relevance:** • The Directive is more relevant to certain social changes (e.g. urbanisation) than others (e.g. social changes associated with new technologies). • Given its overarching focus on CIP – which is particularly

[122] Poustourli, A., Ward, D., Zachariadis, A., & Schimmer, M. (2015). An overview of European Union and United States critical infrastructure protection policies. In *12th International Conference "Standardization, Protypes and Quality: A means of Balkan Countries' Collaboration"* (pp. 549–557). Kocaeli University Foundation. Interview: 1 EU CI owners/operators

[123] Trend Micro. (2018). How cryptocurrency is shaping today's threat environment.

[124] Survey: 1 PoC.

[125] Newman, L. H. (2018, December 2). Now cryptojacking threatens critical infrastructure, too. *Wired*.

[126] Survey:56% (N=9) of PoCs, 40% (N=4) of Other ministries, 64% (N=21) of CI owners/operators.

[127] European Commission. (2014). Annex – The urbanisation of Europe and the World. Publications Office of the European Union, Luxembourg.

[128] Survey: 1 PoC.

[129] 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: 3 EC DGs and Agencies, 2 Academia and think thanks. Survey: 1 CI owner/operator.

[130] European Commission. (2014). Annex – The urbanisation of Europe and the World. Publications Office of the European Union, Luxembourg. Goldammer, J. G. (2017,

Category of changes	Main changes	Relevance of Directive 114 to changes
	• The use of social media in Europe (and globally) has also increased substantially since 2008. While supporting more positive outcomes such as increased online social connectivity, this development also contributes to threats including online radicalisation and terrorist attacks against CI. • Social media is also linked to another development, mentioned by CI owner/operator interviewees, in relation to the ability of protesters to mobilise more quickly now than in previous years.[131]	important for cities – the Directive is well-adapted to certain social changes in Europe, including increasing urbanisation. Indeed, social factors including growing urbanisation are highlighted by survey respondents as having increased the relevance of the Directive. • However, as mentioned above, the Directive is less well-adapted to social changes associated with new technologies: the limited sectoral scope means that the Directive does not address the issue of cross-sector interdependences.
Policy/political	• CIP has increasingly become a component of MS national strategies and action plans as a result of the Directive.[132] Similarly, CIP has continued to remain high on the EU policy agenda • CI can become a critical target in the context of inter-state relationships.[133] This can be seen in the example of relations between the EU and Russia, which have become increasingly strained in recent years, with potential implications for CIP: Europe's reliance on Russian gas is seen as a concern for CIP and security in Europe by stakeholders such as CI owners/operators.[134] • Electoral systems have recently shown themselves to be vulnerable, with both US and European elections reportedly falling victim of influence operations and disinformation tactics.[135]	**Partial relevance:** • While the Directive has helped ensure that CIP is high on EU[136] and MS policy agendas and remains relevant, the procedures within the Directive are not fully adapted to policy/political change. In particular, the bilateral/ multilateral meeting format ('designation of ECI', Article 4) does not allow for third country

August 8). Fires in Europe Fueled by Urbanisation and Climate Change. UNISDR.
[131] Interview: 2 CI owners/operators; workshop: POCs.
[132] Giannopoulos, G., & Schimmer, M. (2011). Memorandum on the results of the sixth Workshop on the Implementation and Application of the Directive. JRC. Workshop: PoCs and CI owners/operators.
[133] Interview: 1 CI owners/operators.
[134] Interview: 2 CI owners/operators.
[135] Drozdiak, N. (2018, October 16). Fear of Russian Meddling Hangs Over Next Year's EU Elections. *Bloomberg*.
[136] Council of the European Union. (2015). Draft Council Conclusions on the Renewed European Union Internal Security Strategy. 2015-2020, Brussels.

Category of changes	Main changes	Relevance of Directive 114 to changes
		involvement. Similarly, the definition of ECI does not reflect the increasing connectedness of national CI across MS and third countries. This limits the relevance of the Directive in light of increasing connectedness of national CI across MS and third countries. It should be noted, however, that a small majority of survey respondents do not consider policy and political developments to have affected the relevance of the Directive.
Environmental	• Extreme climate events are predicted to become more common in the future,[137] including increased occurrence of heatwaves,[138] erratic weather such as alternating droughts and thunderstorms,[139] droughts,[140] flooding, widespread fires,[141] and snow loads.[142] Failure to tackle climate change and extreme weather events has been highlighted as a global risk by the World Economic Forum. Additionally, climate change and extreme weather events will amplify the risks to physical infrastructure and the associated economic activities and societal functions.[143] • The energy sector is particularly vulnerable to weather extremes, such as flooding or droughts,[144] although other sectors, such as the transportation sectors and marine and water management are also vulnerable.[145]	**Limited relevance:** • The Directive is partly relevant to the environmental changes taking place since 2008. • On the one hand, the majority of survey respondents indicate that environmental changes have increased the relevance of the Directive.[149]

[137] Forzieria, G., Bianchi, A., Silva, F., Marin Herrera, M., Leblois, A., & Lavalle, C. (2018). Escalating impacts of climate extremes on critical infrastructures in Europe. *Global Environmental Change*, *48*, 97–107.
[138] Rubin, A. J. (2018, August 4). Scorching Summer in Europe Signals Long-Term Climate Changes. *New York Times*.
[139] Rubin, A. J. (2018, August 4). Scorching Summer in Europe Signals Long-Term Climate Changes. *New York Times*.
[140] Utah State University. (2017). A drier south: Europe's drought trends match climate change projections. EurekAlert.
[141] Forzieria, G., Bianchi, A., Silva, F., Marin Herrera, M., Leblois, A., & Lavalle, C. (2018). Escalating impacts of climate extremes on critical infrastructures in Europe. *Global Environmental Change*, *48*, 97–107.
[142] Croce, P., Formichi, P., Landi, F., Mercogliano, P., Bucchignani, E., Dosio, A., & Dimova, S. (2018). The snow load in Europe and the climate change. *Climate Risk Management*, *20*, 138–154. Interview: 1 EU CI owners/operators.
[143] World Economic Forum. (2018). The Global Risks Report 2018, 13th Edition. Insight Report.
[144] Karagiannis, G. M., Turkesezer, Z. I., Alfieri, L., Feyen, L., & Krausmann, E. (2017). Climate change and critical infrastructure – floods. JRC.
[145] CORDIS. (2018). A pan European framework for strengthening Critical Infrastructure resilience to climate change. Horizon 2020.
[149] Survey: 55% (N=11) of PoCs, 67% (N=8) of Other ministries and 54% (N=22) of CI owners/operators. Some of the free text responses on the nature of these

Category of changes	Main changes	Relevance of Directive 114 to changes
	• Extreme weather events can be highly disruptive to CI: for example, in 2014 snow and freezing rain caused a partial collapse of Slovenia's electricity infrastructure.[146] • 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,[147] and the importance of having climate resilient infrastructure was reinforced in the 2018 Evaluation of the EU Strategy on adaptation to climate change, with particular focus on energy and transport infrastructure due to their vulnerability.[148] As highlighted in the evaluation of the EU Strategy, there is a need to ensure the climate resilience of existing and future CI, to ensure reliability of service provision and increased asset life.	• On the other hand, the Directive's provisions regarding the identification and designation of ECI appear to be not fully adapted to the changing climatic context as they offer only limited criteria (the 'cross-cutting criteria' in Article 3 (2)) with which to assess the significance of the effects of an event. Additionally, the ECI OSPs procedure for identifying, selecting and prioritising counter-measures and procedures to protect ECI (Annex II of the Directive) only focuses on security measures, as opposed to more general safety measures concerning the ECI structure itself.

threats include rising sea levels, forest fires, flooding, landslides, and storms.

[146] Shakou, L. M. (2017, March). *Impacts of climate change on CI*. Presented at the Workshop on Critical Infrastructure Protection and Climate Change, Nicosia.

[147] European Commission. 2013. EU Strategy on Adaptation to Climate Change. DG CLIMA.

[148] European Commission. 2018. Evaluation of the EU Strategy on adaptation to climate change, Accompanying the document REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of the EU Strategy on adaptation to climate change. Commission Staff Working Document, SWD(2018) 461 final.

8. EVIDENCE SUPPORTING THE ANALYSIS OF THE COHERENCE

8.1. List of pieces of legislation and policy documents analysed

8.1.1. EU sectoral legislation

ENERGY

The energy sectoral measures taken into account are:

- Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010, hereinafter Gas Supply Regulation;
- Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products, hereinafter Oil Stocks Directive; and,
- Proposal for a Regulation of the European Parliament and of the Council on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC, COM/2016/0862 final, hereinafter Risk-preparedness in the electricity sector Regulation.

TRANSPORT

Aviation:

- Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002; and,
- Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security.

Maritime:

- Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security; and
- Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security.

Rail:

- European Commission (2018), Action Plan to protect rail passengers and staff in Member States.

OTHER SECTORS

ICT:

- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

Space:

- Regulation (EU) No 1285/2013 of the European Parliament and of the Council of 11 December 2013 on the implementation and exploitation of European satellite navigation systems and repealing Council Regulation (EC) No 876/2002 and Regulation (EC) No 683/2008 of the European Parliament and of the Council;
- Council Decision 2014/496/CFSP of 22 July 2014 on aspects of the deployment, operation and use of the European Global Navigation Satellite System affecting the security of the European Union and repealing Joint Action 2004/552/CFSP;
- Decision No 541/2014/EU of the European Parliament and of the Council of 16 April 2014 establishing a Framework for Space Surveillance and Tracking Support; and,
- 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 and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013, (EU) No 377/2014 and Decision 541/2014/EU.

Financial:

- Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC; and,
- Regulation of the European Central Bank (EU) No 795/2014 of 3 July 2014 on oversight requirements for systemically important payment systems (ECB/2014/28).

Health and water:

- Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC;
- Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption; and,
- Proposal for a Directive OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the quality of water intended for human consumption (recast), COM(2017) 753 final.

Cross-sectoral:

- Directive 2012/18/EU of the European Parliament and the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances and repealing Council Directive 96/82/EC (known as Seveso III); and,
- Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism.

8.1.2. International legislation

CIP is high on the international agenda, and in 2017 the **United Nations (UN) Security Council** approved Resolution 2341[150] calling upon MS to put in place comprehensive measures for the protection of CI against terrorist attacks. Linked to this, the *Compendium of good practices* was compiled by the UN Counter-Terrorism Centre and the Counter-Terrorism Committee Executive Directorate, which presents additional case studies as examples related to the topics covered by the Resolution.

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.[151] On digital infrastructures specifically, the OECD adopted in 2015 *Recommendation on Digital Security Risk Management for economic and social prosperity* and is currently working to revise the 2008 *Recommendation on the Protection of Critical Information Infrastructures.* In addition, the OECD has organised several workshops related to CIP[152] 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 Organization (NATO)** is also involved in security and resilience of CI, especially in the energy sector.[153] The Civil Emergency Planning Committee of NATO provides expertise and capabilities, coordinates planning to support national authorities in civil emergencies to achieve higher standards of preparedness and better interoperability in crisis, and supports the exchange of experience and best practice between nations, especially in relation to energy security. It does not have a regulatory approach, but supports MS in. In 2017, it issued political guidelines, which, within crisis management, covers prevention, preparedness, response and recovery.[154]

The **International Organization for Standardization** (ISO) developed widely used standards that covers risk analysis and risk management practices and that are widely used by CI operators.[155] The ISO/IEC 27000-series, developed by ISO and the International Electrochemical Commission (IEC) presents the Information Security Management System (ISMS) (ISO/IEC 27000), the goal of which is to protect valuable information against the loss of availability, confidentiality and integrity. ISMS can be applied to CI, especially to their IT component. Other standards focus on business continuity, risk management and environmental risks. They provide their own definitions and guidelines on conducting risk analysis and risk management, which overlap with the risk analysis and risk management measures in the OSP as per the Directive. Other ISO standards are also relevant.

8.2. Overview of overlaps and complementarities

8.2.1. Energy

Elements	Assessment	Rationale
Objectives	**Overlap and complement**	The ECI Directive complements sectoral legislation objectives insofar as the protection (objective of the ECI Directive) is separate from resilience (objective of the sectoral legislation). Objectives may however overlap as the distinction between these two concepts is often not so clear-cut.

[150] UN Security Council, Resolution 2341 (2017). The resolution is not legally binding.
[151] 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)".
[152] 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.
[153] 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.
[154] Jahier, K. (2014), Presentation on Critical infrastructure protection within NATO, available On the Critical Infrastructure Protection and Resilience Europe website.
[155] Workshop: CI owners/operators.

Elements	Assessment	Rationale
Object to protect	**Overlap and complement**	Systems are covered by both the ECI Directive and the sectoral legislation. Assets are covered exclusively by the ECI Directive.
Gas and electricity		
Threat assessment/ Risk analysis	**Overlap and complement**	The threat assessment/risk analysis per sub-sector requested by the ECI Directive may overlap with the one carried out by national authorities as requested by sectoral legislation. The risk analysis to be conducted by operators and to be included in the OSP is a distinctive feature of the ECI Directive.
Risk management	**Complement**	Risk management measures to be implemented by operators and included in the OSP according to the ECI Directive complement the risk preparedness plan and the preventive plan that national authorities have to design according to sectoral legislation. However, obligations on operators are likely to derive from the implementation of the plan as well as from other CI-specific obligations. Specifically related to electricity transmission system operators (TSO), risk management obligations derive from the network code on electricity emergency and restoration. [156]
Crisis management	**Complement**	The reference to crisis management measure to be included in the OSP prepared by operators according to the ECI Directive complements with the Emergency Plans (gas supply) and Risk and Preparedness plans (electricity) that need to be developed by national authorities according to sectoral legislation. Obligations on operators are however likely to derive at the national level from the plans developed by national authorities as well as from other CI-specific obligations.[157]
Oil		
Threat assessment/ Risk analysis	**Complement**	The threat assessment per sub-sector to be conducted by national authorities and the risk analysis to be conducted by operators are distinctive features of the Directive.
Risk management	**Complement**	The ECI Directive intends risk and crisis management measures as protection measures while the sectoral legislation includes rules for stocking oil and releasing the stocks.
Crisis management		

8.2.2. Transport

Aviation

Elements	Assessment	Rationale
Objectives	**Overlap**	The ECI Directive overlaps with the objectives of the aviation legislation insofar as the protection of airports (objective of the ECI Directive) is included in the protection of civil aviation (objective of the aviation legislation).
Object to protect	**Overlap**	Airport security is covered by both the ECI Directive and the sectoral legislation.
Threat assessment/ Risk analysis	**Overlap**	The threat assessment/risk analysis requested by the ECI to national authorities and to operators in the OSP may overlap with the risk analysis requested by sectoral legislation to national authorities and operators.
Risk management	**Overlap**	Risk management measures included in the OSP may overlap with the measures required to operators that are included in the airport security programmes foreseen by sectoral legislation.
Crisis management	**Overlap**	The reference to crisis management measure to be included in the OSP prepared by operators according to the ECI Directive overlap with the airport security programmes that,

[156] Specifically related to transmission system operators, risk management obligations derive from the network code on electricity emergency and restoration.
[157] Specifically related to transmission system operators, risk management obligations derive from the network code on electricity emergency and restoration.

		even if not including specific details on crisis management measures, refer to them and leave MS to detail, in confidential documents, the required measures and responsibilities.

Maritime

Elements	Assessment	Rationale
Objectives	**Overlap**	The ECI Directive overlaps with the objectives of the maritime legislation insofar as the protection of ports (objective of the ECI Directive) is included in the security of port facilities (objective of the maritime legislation).
Object to protect	**Overlap**	Ports are covered by both the ECI Directive and the sectoral legislation.
Threat assessment/ Risk analysis	**Overlap**	The threat assessment/risk analysis per sub-sector requested by the ECI Directive to national authorities and to operators (in the OSP) may overlap with the threat assessment and risk analysis requested by the sectoral legislation.
Risk management	**Overlap**	Risk management measures included in the OSP may overlap with measures included in the security plans requested by sectoral legislation (port/port facility security plans).
Crisis management	**Overlap**	Risk management measures included in the OSP may overlap with measures included in the security plans requested by sectoral legislation (port/port facility security plans).

Rail

Elements	Assessment	Rationale
Objectives	**Overlap**	The ECI Directive overlaps with the rail security measures in addressing security challenges deriving from terrorism, and may overlap with safety legislation on other types of threats
Object to protect	**Complement**	The ECI Directive focuses on the security of the infrastructure and rail security measures on the security of people
Threat assessment/Risk analysis	**Overlap**	The threat assessment per sub-sector requested by the ECI Directive may overlap with: - the analysis and assessment of risk requested by the rail security measures to national authorities when drafting the national programme for railway security management - the risk assessment on physical assets requested to operators for the creation of the safety management system imposed by the rail safety legislation
Risk management	**Overlap**	Risk management measures included in the OSP may overlap with: - measures included in the security management plan requested to operators by the rail security measures - measures included in the safety management system imposed to operators by the rail safety legislation
Crisis management	**Overlap**	Risk management measures included in the OSP may overlap with measures included in the emergency plan requested by rail safety legislation

8.2.3. NIS Directive

Elements	Assessment	Rationale
Objectives	**Complement and overlap**	The objective of the ECI Directive (protection of ECI) overlaps with and complements the objective of the NIS Directive (security of NIS) as the concept of ECI includes and expand the concept of NIS.
Object to protect	**Complement and overlap**	The ECI Directive overlaps with the NIS Directive as, defining CI as assets or systems, ECI can also be network and information systems which are the main object of the NIS Directive. Moreover, the energy and transport sectors are in the scope of both instruments. The ECI Directive covers also

Elements	Assessment	Rationale
		other types of systems and assets, which are excluded from the NSI Directive.
Threat assessment/Risk analysis	**Overlap**	Risk analysis developed by operators and included in the OSP according to the ECI Directive may overlap with the obligations imposed by the NIS on operators to assess the security of their network and information systems. The threat assessment/risk analysis that authorities have to conduct under the ECI Directive may overlap with the requirement that the Computer security incident response teams (CSIRTs) have to provide a dynamic risk and incident analysis under the NIS.
Risk management	**Overlap**	Risk management measures to be adopted by operators and included in the OSP according to the ECI Directive can overlap with requirements on operators imposed by the NIS to take appropriate and proportionate technical and organisational measures to manage the risks and prevent incidents.
Crisis management	**Overlap**	Crisis management measures to be adopted by operators and included in the OSP according to the ECI Directive can overlap with requirements on operators imposed by the NIS to take appropriate and proportionate technical and organisational measures to minimise the impact of incidents ensuring the continuity of services.

8.3. Mapping of key aspects of relevant EU sectoral legislation

8.3.1. Energy

	ECI Directive	Gas Supply Regulation - 2017/1938	Risk-preparedness in the electricity sector Regulation (proposal of) - COM(2016) 862 final	EU Oil Stocks Directive 2009/119/EC
Legal basis	Article 308 Treaty establishing the European Community (other measures)	Article 194(2) TFEU (energy)	Article 194 TFEU (energy)	Article 100 of the Treaty establishing the European Community (implementing measures appropriate to the economic situation if severe difficulties arise in the supply of certain products)
Objectives	Provide procedures for the **identification and designation of ECI**, and common approach to the assessment of the need to improve the **protection**	**Safeguard the security of gas supply** in the EU by ensuring the proper and continuous functioning of the internal market in natural gas, by allowing for exceptional measures to be implemented when the market can no longer deliver the gas supplies required, including **solidarity measure of a last resort**, and by providing for the clear definition and attribution of responsibilities among natural gas undertakings, the MS and the Union regarding both preventive action and the reaction to concrete disruptions of gas supply	**Provide rules for the co-operation between MS** in view of preventing, preparing for and handling electricity crises in a spirit of solidarity and transparency and in full regard for the requirements of a competitive internal market for electricity.	**Secure** the EU **oil supply** by requiring governments to keep a minimum level of crude oil and/or petroleum **stocks**, setting out procedures for **releasing** these if there is a **serious shortage**
Sectors covered by security measures	**Energy:** electricity, oil, gas **Transport**: road, rail, air, inland waterways, ocean and short-sea shipping and ports	**Energy:** gas	**Energy**: electricity	**Energy:** oil
Type of threats	All-hazards approach while countering threats from terrorism as a priority	All relevant risk factors such as natural disasters, technological, commercial, social, political and other risks, which could lead to the	Variety of circumstances (e.g. extreme weather circumstances, malicious attacks including cyber-attacks, a fuel shortage)	Major disruptions of supply of crude oil or petroleum products

	ECI Directive	Gas Supply Regulation - 2017/1938	Risk-preparedness in the electricity sector Regulation (proposal of) - COM(2016) 862 final	EU Oil Stocks Directive 2009/119/EC
		materialisation of the major transnational risk[158] to the security of gas supply	affecting the risk of an **electricity crisis**	
Operations	Threat assessment, risk analysis, risk management	Threat assessment, risk analysis, risk management, crisis management	Threat assessment, risk analysis, crisis management	Risk management, crisis management
Definition of object to protect	**ECI**: CI located in MS the disruption of which would have significant impact on at least 2 MS [**CI:** asset, system or part thereof located in MS which is essential for the maintenance of vital societal functions, health, safety, security, economic and social well-being of people, and the disruption of which would have a *significant impact* in a MS as a result of the failure to maintain these functions]	**Gas supply:** sale, including resale, of natural gas, including LNG, to customers	**Electricity system / electricity supply in general** [**security of electricity supply:** the ability of an electricity system to guarantee an uninterrupted supply of electricity to consumers with a clearly defined level of performance]	**oil supply** (not defined/referenced in the Directive)
Other definitions	*Significance of impact*: based on sectoral criteria and cross-cutting criteria: casualties, economic effects, public effects; these are defined on a case-by-case basis - JRC has elaborated non-binding guidelines (sectoral criteria are classified and details of cross-cutting criteria); JRC guidelines mention that only one cross-sectoral criterion is necessary	**Security of gas supply:** both security of supply of natural gas and technical safety	**Electricity crisis:** a situation of significant electricity shortage or impossibility to deliver electricity to end-consumers, either existent or imminent	None

[158] The definition of the transnational risk is neither provided nor referenced in the Directive.

	ECI Directive	Gas Supply Regulation - 2017/1938	Risk-preparedness in the electricity sector Regulation (proposal of) - COM(2016) 862 final	EU Oil Stocks Directive 2009/119/EC
	Protection: all activities aimed at ensuring the functionality, continuity and integrity of CI in order to deter, mitigate and neutralise a threat, risk or vulnerability			
Definition of operators / owners	**Owners/operators of ECI**: entities responsible for investment in, and/or day-to-day operation of, an ECI	**Transmission system operator:** a natural or legal person who carries out the function of transmission and is responsible for operating, ensuring the maintenance of, and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transport of gas **Natural gas undertaking:** a natural or legal person carrying out at least one of the following functions: production, transmission, distribution, supply, purchase or storage of natural gas, including LNG, which is responsible for the commercial, technical and/or maintenance tasks related to those functions, but shall not include final customers	None	**Economic operators** (not defined/referenced in the Directive) **CSE (Central Stockholding Entity):** the body or service upon which powers may be conferred to act to acquire, maintain or sell oil stocks, including emergency stocks and specific stocks
Provisions on co-operation across MS/with EC	**Before the identification** of potential ECI: discussion on the thresholds of cross-cutting criteria	**Gas Coordination Group (GCG):** representatives of the MS, the Agency for the Co-operation of Energy Regulators, ENTSOG and	**MS:** - **Inform neighbouring MS** and the EC without delay **in the event of an electricity crisis situation,** provide	**MS:** - Designate **representatives** for the Coordination Group for oil and petroleum products - Help the **EC carry out reviews**

	ECI Directive	Gas Supply Regulation - 2017/1938	Risk-preparedness in the electricity sector Regulation (proposal of) - COM(2016) 862 final	EU Oil Stocks Directive 2009/119/EC
	Before the designation of ECI: bilateral discussion **ECIP contact point**: to coordinate ECI issues within MS, across Ms with EC	representative bodies of concerned industries and relevant customers, tasked with assisting the EC in all matters related security of gas supply and facilitating the coordination of measures concerning the security of gas supply **MS:** - Designate a **competent authority**, which cooperates with each other in the implementation of this Regulation - Establish **risk groups**[159] in relation to major transnational risks. Those are **the basis for enhanced regional co-operation** to increase the security of gas supply and for agreement on appropriate and effective cross-border measures of all MS concerned within the risk groups or outside the risk groups along the emergency supply corridors. - **Preventive action plan** and the **emergency plan** shall contain **regional chapter(s)**, to be **developed jointly by all MS in the risk group** before	information on the causes of the crisis, measures taken and planned to mitigate it and the possible need for assistance from other MS. **- Cooperate in a spirit of solidarity to prepare for and manage electricity crisis situations,** with a view to ensuring that electricity is delivered where it is most needed, in return for compensation. **- Cooperate with ENTSO-E and the regional operational centres** in terms of ensuring that all risks relating to security of electricity supply are assessed in accordance with the rules set out in this Regulation and in the proposed Electricity Regulation **MS & the Energy Community Contracting Parties**[160]**:** - Closely cooperate in the process of the identification of electricity **crisis scenarios** and the establishment of **risk-preparedness plans** -Energy Community Contracting Parties may	to verify their emergency preparedness and related stockholding - May **delegate** (temporarily) the tasks related to **stockholding** to **another MS** **Coordination Group for oil and petroleum products:** chaired by the and contributes to **analysing the situation** within the Community with regard to security of supply for oil and petroleum products and **facilitates** the **coordination** and **implementation** of measures in that field

[159] The list of such risk groups and their composition are set out in Annex I. The composition of the risk groups shall not prevent any other form of regional co-operation benefiting security of supply.
[160] Non-MS Contracting Parties of the Energy Community (an international organisation) are Albania, Bosnia and Herzegovina, Kosovo, Republic of Macedonia, Moldova, Montenegro, Serbia, Ukraine, Georgia.

	ECI Directive	Gas Supply Regulation - 2017/1938	Risk-preparedness in the electricity sector Regulation (proposal of) - COM(2016) 862 final	EU Oil Stocks Directive 2009/119/EC
		incorporation in the respective national plans.	participate in the Electricity Coordination Group upon invitation by the Commission with regard to all matters by which they are concerned.	
Obligations: identifications of objects to protect	**MS:** - **Identify potential ECI by applying**: sectoral criteria, definition of CI, transboundary criterion, cross-cutting criteria (whose thresholds need to be defined with second MS) - Launch of bilateral discussions for the **identification** and **designation** **- Inform the MS** involved by ECI and the operators/ owners of ECI	None	None	**MS:** - Calculate the stock levels
Obligations: setting the goals	None	None	None	None
Obligations: threat assessments	**MS:** Carry out a threat assessment per subsector if they have designated an ECI	**MS:** A non-exhaustive **list of risk factors is presented** in the Annexes IV and V, which contain the template for the common and national risk assessments, further **risk factors** should be **identified by the competent authorities of MS** during the common risk assessments and national risk assessments	**ENTSO-E:** Develop a methodology for identifying electricity crisis scenarios at regional level Develop a methodology for assessing short and long-term adequacy of the electricity system to supply current and projected demands for electricity for a ten-year period Carry out the short and long-term adequacy assessments **ENTSO-E & MS:** For the preparation of the risk preparedness plan, use the	None

	ECI Directive	Gas Supply Regulation - 2017/1938	Risk-preparedness in the electricity sector Regulation (proposal of) - COM(2016) 862 final	EU Oil Stocks Directive 2009/119/EC
			methodology to **identify the most relevant crisis scenarios**	
Obligations: risk analysis	**MS:** - Ensure that operators have developed an Operator Security Plan (OSP) or equivalent and renewed each year - ensure that a communication mechanism with SLO is in place **Operators /owners**: - Identify important assets, carry out risk analysis based on major threat scenario, vulnerability of each asset, potential impact (in the OSP)	**ENTSOG:** - In co-operation with GCG, develop a **methodology** for simulation of gag supply and infrastructure disruption scenario - Carry out a **Union-wide simulation** of gas supply and infrastructure **disruption scenarios**, including the identification and assessment of emergency gas supply corridors and the MS which can address identified risks. **GCG:** Cooperate with ENTSOG on the simulations of disruption scenarios **MS:** Regional Within each risk group listed in Annex I (a list of groups within the EU that share certain aspects of supplying gas) make a **common assessment at risk group level** of all relevant risk factors which could lead to the materialisation of the major transnational risk to the security of gas supply of the risk group, describing the system and the infrastructure standards.	**ENTSO-E:** - Develop a **methodology** for identifying electricity crisis scenarios at regional level, considering at least the following risks: (a)rare and extreme natural hazards; (b)accidental hazards going beyond N-1 security criterion 18 (c)consequential hazards such as fuel shortages (d)malicious attacks - Identify the most relevant regional crisis scenarios - Develop a methodology for assessing short and long-term adequacy of the electricity system to supply current and projected demands for electricity for a ten-year period - Carry out the short and long-term adequacy assessments **MS:** National - **Ensure that all risks relating to security of electricity supply are assessed** in accordance with the rules set out in this Regulation and Article 18 of the Electricity Regulation [proposed Electricity Regulation].	None

	ECI Directive	Gas Supply Regulation - 2017/1938	Risk-preparedness in the electricity sector Regulation (proposal of) - COM(2016) 862 final	EU Oil Stocks Directive 2009/119/EC
		National - The competent authority of each MS shall make a **national risk assessmen**t of all relevant risks affecting the security of gas supply, consistent with the common risk assessment(s) **Operators** Cooperate with the authorities and are consulted by authorities, to develop their risk assessment	**Operators** Cooperate with the authorities and are consulted by authorities, to develop their risk assessment	
Obligations: Risk management	**Operators/ owners**: identify, select and prioritise counter-measures and procedures, distinguishing between permanent and graduated security measures (in the OSP) - Establish the SLO: link between ECI owners/operators and MS authority **MS**: ensure that a OSP or equivalent is in place and Security Liaison Officers (SLO) appointed	**MS (or its competent authority):** - ensure that in the event of a disruption of the single largest gas infrastructure, the technical capacity of the remaining infrastructure will be sufficient to satisfy the calculated gas demand in accordance with the formula and taking into account currently available data and predicted trends - create a **preventive action plan**[161] (according to the **template**) containing the measures needed to remove or mitigate the risks identified, including the effects of energy efficiency and demand-side	**MS:** **- Draw up risk-preparedness plans,** after consulting stakeholders, in order to ensure maximum preparedness for electricity crisis situations and an effective management of such situations should they occur. The plans should be developed on the basis of electricity crisis scenarios identified by ENTSOE and MS, respectively, and set out the measures planned or taken to prevent and mitigate the scenarios. Moreover, they should describe the role and responsibilities of the competent authorities and the tasks and identity of the	**MS:** - Prepare **contingency plans** to be implemented in the event of a major supply disruption - Maintain total oil stocks equivalent to at least 90 days of average daily imports or 61 days of consumption — whichever is the higher - Set up **central stockholding entities** to acquire, maintain or sell stocks to comply with the directive - Allow companies and other entities that are required to hold oil stocks to delegate some of that responsibility **CSE:**

[161] The plan is to contain a detailed description of the system, a summary of the common and national risk assessments, a description of compliance with the infrastructure standard and the supply standard, preventive measures on both the regional and national level, and the mechanisms and results of consultations with stakeholders, including gas undertakings and relevant organisations representing the interests of industrial gas customers.

	ECI Directive	Gas Supply Regulation - 2017/1938	Risk-preparedness in the electricity sector Regulation (proposal of) - COM(2016) 862 final	EU Oil Stocks Directive 2009/119/EC
		measures, in the risk assessments, with regional chapters developed jointly by all MS in the risk group **<u>Transmission system operators:</u>** enable permanent physical capacity to transport gas in both directions on all interconnections between MS having the possibility of requesting an exemption from this obligation or proposing a cross-border cost allocation, depending on particular conditions of each situation **<u>Natural gas undertakings</u>:** take measures to ensure the gas supply to the protected customers of the MS in each of the 3 cases listed, related to rarely occurring high gas demand	national crisis manager or team.	- **Assist the MS** in acquiring, maintaining or selling stocks - May a**ssist the entities** required to hold oil stocks **<u>Economic operators:</u>** - Assist the MS in stockholding
Obligations: Crisis management	**<u>Operators/ owners</u>**: Identify, crisis management measures (in the OSP)	**<u>MS:</u>** Create an **emergency plan** (according to the **template**) containing the measures to be taken to remove or mitigate the impact of a disruption of gas supply *(Art. 8(2b))*, taking into consideration **co-operation** with other **MS** within **risk groups**, defining the roles and responsibilities of **natural gas undertakings**, **transmission systems operators** for electricity and	**<u>MS:</u>** - Include in the risk preparedness plans **measures to ensure that simultaneous crisis situations are properly prevented and managed.** - Cooperate in a spirit of solidarity to **prepare for and manage electricity crisis situations,** with a view to ensuring that electricity is delivered where it is most needed, in return for	**<u>MS:</u>** Implement the contingency plans, **releasing** quickly, effectively and transparently some or all of their **emergency stocks** and **specific stocks** in the event of a major supply disruption and **imposing** general or specific **restrictions on consumption** in line with the estimated shortages

	ECI Directive	Gas Supply Regulation - 2017/1938	Risk-preparedness in the electricity sector Regulation (proposal of) - COM(2016) 862 final	EU Oil Stocks Directive 2009/119/EC
		of **industrial gas customers**, built upon the **crisis levels** (early warning, alert, emergency) **<u>Transmission system operators:</u>** cooperate and exchange information using the ReCo System for Gas established by ENTSOG	compensation; and - In the event of an electricity crisis, act in full compliance with internal electricity market rules. - Describe the mechanism to inform the public about any electricity crisis. - **Carry out an ex-post evaluation of the crisis and its impacts.**	
Reporting to EC	**<u>MS:</u>** - on annual basis on: the number of infrastructure per sector for which cross-cutting criteria **discussions** were held and the number of **designated ECI** per sector and number of MS dependent - every 2 years on: summary of **threat assessment** (type of risks, threats, and vulnerabilities per ECI sector)	**<u>MS:</u>** - name of its **competent authority** and any changes thereto (that should also be made public). - **definition of protected customers**, the **annual gas consumption volumes of the protected customers** and the **percentage that those consumption volumes represen**t of the total annual final gas consumption in that MS - every 4 years on: notify to the EC the **common risk assessment** once agreed by all MS in the risk group and the **national risk assessments**	**<u>MS:</u>** - **Name and the contact details of the competent authority** in charge of carrying out tasks set out in this Regulation, once designated - After consultation with the Electricity Coordination Group, the **final risk preparedness plan should be sent to the EC,** and updated every three years, unless circumstances warrant more frequent updates - **Inform without delay in the event of an electricity crisis** situation, provide information on the causes of the crisis, measures taken and planned to mitigate it and the possible need for assistance from other MS - Inform if they have specific, serious and reliable information that an **event may occur** that is likely to	**<u>MS:</u>** - Send the data from the **up-to-date register of their emergency stocks** to the EC by 25 February **every year** **- On demand** provide the EC with the data from the **up-to-date register of specific stocks** held within their territory - Send **monthly summaries** of the **level** of the commercial **stocks** held on their territory to the EC

	ECI Directive	Gas Supply Regulation - 2017/1938	Risk-preparedness in the electricity sector Regulation (proposal of) - COM(2016) 862 final	EU Oil Stocks Directive 2009/119/EC
			result in a significant deterioration of electricity supply - **Inform about possible risks** they see in relation to the ownership of infrastructure relevant for security of supply, **and any measures taken to prevent or mitigate such risks,** with an indication of why such measures are considered necessary and proportionate **- After declaring an electricity crisis situation, provide the Electricity Coordination Group and the Commission with an evaluation report**	
Reporting (other than to the EC)		**MS:** - Report to the GCG the agreed upon **co-operation mechanism** to conduct the **common risk assessment** 11 months before the deadline for the notification of the common risk assessment and its updates. - Report regularly to the GCG on the **progress achieved on the preparation and adoption** of the **preventive action plans** and the **emergency plans**, in particular the regional chapters - Report to the GCG the agreed upon **co-operation**	**MS:** - the competent authority should **submit a draft of the risk preparedness plan to the competent authorities in the region and to the Electricity Coordination Group** for consultation - **inform the Electricity Coordination Group about possible risks** they see in relation to the ownership of infrastructure relevant for security of supply, **and any measures taken to prevent or mitigate such risks,** with an indication of why such measures are considered necessary and proportionate.	None

	ECI Directive	Gas Supply Regulation - 2017/1938	Risk-preparedness in the electricity sector Regulation (proposal of) - COM(2016) 862 final	EU Oil Stocks Directive 2009/119/EC
		mechanism for the **preparation** of the **preventive action plan** and the **emergency plan**, including the exchange of draft plans 16 months before the deadline for agreement of those plans and the updates of those plans.	- **after declaring an electricity crisis situation, provide the Electricity Coordination Group with an evaluation report** - make public risk preparedness plan	
Sanctions		**MS:** **shall lay down the rules on penalties** applicable to infringements by natural gas undertakings of paragraph 6 or 7 of this Article (natural gas undertakings should notify to the competent authority concerned certain details of gas supply contracts) and shall take all measures necessary to ensure that they are implemented. The **penalties provided for shall be effective, proportionate and dissuasive**. *(Art. 14(10))*	None	**MS:** - lay down the **rules on penalties** applicable to infringements of the national provisions adopted pursuant to this Directive and shall take such measures as may be necessary to ensure that they are applied. Such penalties shall be **effective, proportionate and dissuasive**. *(Art. 21)*
Other		-	Relation to the NIS Directive and ECI Directive as stated in this Regulation: "The proposed Regulation **complements the NIS Directive** by ensuring that cyber-incidents are properly identified as a risk and that measures taken to deal with them are properly reflected in the risk preparedness plans. The proposed Regulation **complements also Council Directive 2008/114/EC 10**,	The Annexes contain very detailed rules for calculating the crude oil equivalents of petroleum products and of inland consumption, as well as the level of stocks held. It is noted that the MS have to ensure that sensitive data are protected and have to abstain from mentioning the names of the owners of the stocks concerned

	ECI Directive	Gas Supply Regulation - 2017/1938	Risk-preparedness in the electricity sector Regulation (proposal of) - COM(2016) 862 final	EU Oil Stocks Directive 2009/119/EC
			which established a common procedure for identifying European critical infrastructures ('ECI') such as e.g. infrastructures and facilities for generation and transmission and for protecting them against terrorist attacks and other physical risks. The proposed Regulation focuses more broadly on how to secure the resilience of the electricity system as a whole and how to manage crisis situations when they occur."	

8.3.1.1. Focus on risk analysis/threat assessment, risk management and crisis management

	Sectoral legislation	ECI Directive
RISK ANALYSIS/THREAT ASSESSMENT		
Obligation	1. EU level: EU-wide risk assessment for *gas*, short and long-term adequacy assessment for *electricity* 2. Regional level: common risk assessment at risk group level for *gas*, regional crisis scenarios for *electricity* 3. National level: national risk assessment for *gas*, security of supply assessment for *electricity*	1. ECI subsector: threat assessment 2. Individual ECI: risk analysis in the OSP
Responsible body	1. Operators' association (ENTSOG) in co-operation with MS authorities (Gas Coordination Group) for *gas*; Operators' association (ENTSO-E) for *electricity* 2. MS in risk groups (*gas*); Operators' association in consultation with the MS authorities (Electricity Coordination Group) (*electricity*); 3. MS in co-operation with operators (*gas*, *electricity*)	1. MS authorities 2. ECI operators
Content	1. Identification and assessment of emergency gas supply corridors, Union-wide simulation of gas supply and infrastructure disruption scenarios (*gas*); overall adequacy of the electricity system to supply current and projected demands for electricity for a ten-year period (*electricity*) 2. Description of the system, infrastructure standards, identification of risks, risk analysis (simulation of risk scenarios) for the region *(gas);* regional electricity crisis scenarios *(electricity)*	1. Threat assessment including types of risks, threats and vulnerabilities encountered per ECI sector 2. Identification of important assets, risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact (in OSP)

	Sectoral legislation	ECI Directive
	3. Description of the system, infrastructure standards, identification of risks, risk analysis (simulation of risk scenarios) at national level (*gas*); national electricity crisis scenarios (*electricity*)	
Templates	1. None 2. Template in Annex IV to the Gas Supply Regulation (*gas*); none (*electricity*) 3. Template in Annex V to the Gas Supply Regulation (*gas*); none (*electricity*)	1. May be developed by the EC 2. None
RISK MANAGEMENT		
Obligation	1. Risk preparedness plan (*electricity*) 2. Preventive plan (*gas*)	OSP
Responsible body	1. MS in consultation with Electricity Coordination Group and MS in the same region 2. MS, along with other MS in the risk group for the regional chapters	Operators
Content	1. Summary of electricity crisis scenarios, role and responsibilities of the competent authorities, measures designed to prepare for and to prevent the risks, tasks and identity of national crisis manager or team 2. Measures needed to remove or mitigate the risks identified, including the effects of energy efficiency and demand-side measures, in the common and national risk assessments[162]	Identification, selection and prioritisation of counter-measures and procedures with a distinction between: • permanent security measures, such as technical measures (including installation of detection, access control, protection and prevention means); organisational measures (including procedures for alerts and crisis management); control and verification measures; communication; awareness raising and training; and security of information systems; • graduated security measures
Templates	Annex to the Risk Preparedness Regulation • Annex VI to the Gas Supply Regulation • Annex VII to the Gas Supply Regulation	None
CRISIS MANAGEMENT		
Obligation	1. Risk preparedness plan (*electricity*) 2. Emergency plan (*gas*)	None

[162] Specifically: results of risk assessment and summary of scenarios; definition of protected customers; measures, volumes and capacities needed to fulfil the infrastructure and gas supply standards; obligations imposed on natural gas undertakings, electricity undertakings and other relevant bodies; other preventive measures to address the risks; information on the economic impact, effectiveness and efficiency of the measures; description of the effects of the measures; description of the impact of the measures on the environment and on customers; the mechanisms to be used for co-operation with other MS; information on existing and future interconnections and infrastructure; information on all public service obligations, as per Gas Supply Regulation, Article 9.

	Sectoral legislation	ECI Directive
Responsible body	1. MS in consultation with Electricity Coordination Group and MS in the same region 2. MS, along with other MS in the risk group for the regional chapters	
Content	1. Procedures to be followed in electricity crisis situations, identification of the contribution of market-based measures in coping with electricity crisis situations, possible non-market measures to be implemented in electricity crisis situations, detailed load shedding plan, description of mechanism to inform the public about any electricity crisis; regional measures 2. Measures to be taken to remove or mitigate the impact of a disruption of gas supply, depending on crisis levels[163]	
Templates	1. Annex to the Risk Preparedness Regulation 2. Annex VII to the Gas Supply Regulation	

8.3.2. Transport

	ECI Directive	Aviation Security Regulation - 300/2008	Commission Implementing Regulation (EU) 2015/1998	Action Plan to protect rail passengers and staff in Member States	Ship and port facility security Regulation - 725/2004	Port Security Directive - 2005/65
Legal basis	Art. 308 Treaty establishing the European Community (other measures)	Article 80 (2)Treaty establishing the European Community (transport)	Article 80 (2)Treaty establishing the European Community (transport)	NA	Article 80(2) Treaty establishing the European Community, (transport)	Article 80(2) Treaty establishing the European Community, (transport)
Objectives	Provide procedures for the **identification and designation of**	Provide **common rules** and **common basic standards**[164] **and**	Provide detailed measures for **the implementation of the common**	**Prevent and respond to possible terrorist attacks targeting**	Introduce and implement Community measures aimed at	Introduce Community measures to enhance **port security** in the face of threats of

[163] Specifically: role and responsibilities of natural gas undertakings, transmission system operators for electricity and of industrial gas customers including relevant electricity producers; role and responsibilities of the competent authorities and of the other bodies; measures and actions to be taken to mitigate the potential impact of a disruption of gas supply on district heating and the supply of electricity generated from gas, detailed procedures and measures to be followed; definition of crisis manager; identification of the contribution of market-based and non-market based measures; description of mechanisms to cooperate with other MS; reporting obligations imposed on natural gas undertakings and, where appropriate, electricity undertakings; technical or legal arrangements in place to prevent undue gas consumption, technical, legal and financial arrangements in place to apply the solidarity obligations; estimation of the gas volumes that could be consumed by solidarity protected customers; predefined actions to make gas available in the event of an emergency; as per Gas Supply Regulation, Article 10.

[164] Concerning mainly risk management and laid down in the Annex, covering: airport security, demarcated areas of airports, aircraft security, passengers and cabin baggage, hold baggage, cargo and mail, air carrier mail and air carrier materials, in-flight supplies, airport supplies, in-flight security measures, staff recruitment and training and security equipment. MS may use alternative security measures (duly justified and following an amending decision).

	ECI Directive	Aviation Security Regulation - 300/2008	Commission Implementing Regulation (EU) 2015/1998	Action Plan to protect rail passengers and staff in Member States	Ship and port facility security Regulation - 725/2004	Port Security Directive - 2005/65
	ECI, and common approach to the assessment of the need to improve the **protection**	**mechanisms** to monitor compliance to protect civil aviation against acts of unlawful interference that jeopardise the security of civil aviation. **Basis for a common interpretation of Annex 17 to the Chicago Convention** on International Civil Aviation.	**basic standards on aviation security**	**rail** services by creating an effective cooperative environment and **make recommendations that will help MS coordinate rail security** actions efficiently (source: ec.europa.eu, https://ec.europa.eu/transport/modes/rail/news/2018-06-12-action-plan-security-rail-passengers_en)	**enhancing the security of ships** used in international trade and domestic shipping and associated **port facilities** in the face of threats of intentional unlawful acts. Provide a basis for the **harmonised interpretation and implementation and Community monitoring** of the special measures to enhance maritime security adopted by the Diplomatic Conference of the IMO on 12 December 2002, establishing the International Ship and Port Facility Security Code (ISPS Code)	security incidents, the measures consisting of: common basic rules on port security, their implementation mechanism and compliance monitoring mechanisms. Ensure that security measures taken pursuant to Regulation (EC) No 725/2004 benefit from enhanced port security.
Sectors covered by security measures	**Energy:** electricity, oil, gas **Transport**: road, rail, air, inland waterways, ocean and short-sea shipping and ports	**Transport:** civil aviation	**Transport:** civil aviation	**Transport:** rail	**Transport:** Maritime	**Transport:** Maritime

	ECI Directive	Aviation Security Regulation - 300/2008	Commission Implementing Regulation (EU) 2015/1998	Action Plan to protect rail passengers and staff in Member States	Ship and port facility security Regulation - 725/2004	Port Security Directive - 2005/65
Type of threats	All hazards approach while countering threats from terrorism as a priority	Acts of unlawful interference with civil aircraft that jeopardise the security of civil aviation, terrorist acts	Acts of unlawful interference with civil aircraft that jeopardise the security of civil aviation	Possible terrorist attacks targeting rail services (source: ec.europa.eu, https://ec.europa.eu/transport/modes/rail/news/2018-06-12-action-plan-security-rail-passengers_en)	Threats of intentional unlawful acts such as acts of terrorism, acts of piracy or similar	Threats of security incidents, security incidents resulting from terrorism
Operations	Threat assessment, risk analysis, risk management	Risk management, crisis management	Risk analysis, risk management	threat assessment, threat management, crisis management	Threat assessment, risk analysis, risk management, crisis management	Threat assessment, risk analysis, risk management
Definition of object to protect	**ECI**: CI located in MS the disruption of which would have significant impact on at least 2 MS [**CI:** asset, system or part thereof located in MS which is essential for the maintenance of vital societal functions, health, safety, security, economic and social well-being of people, and the disruption of which would have a *significant impact* in a MS as a result of the failure to maintain these	**Civil aviation**: any air operation carried out by civil aircraft, excluding operations carried out by State aircraft referred to in Article 3 of the Chicago Convention on International Civil Aviation	Covered in Aviation Security Regulation - 300/2008	**rail passengers and staff in the EU** (source: ec.europa.eu, https://ec.europa.eu/transport/modes/rail/news/2018-06-12-action-plan-security-rail-passengers_en)	**Shipping and port facilities:** ships used in international shipping and the port facilities which serve them, ships operating domestic services within the Community and their port facilities, in particular passenger ships, on account of the number of human lives which such trade puts at risk **Port facility:** a location where the ship/port interface takes place; this includes areas such	Every **port** located in the territory of MS in which one or more port facilities covered by an approved port facility security plan pursuant to Regulation (EC) No 725/2004 is or are situated. This Directive shall not apply to military installations in ports. [**port**: any specified area of land and water, with boundaries defined by the MS in which the port is situated, containing works and equipment designed to facilitate commercial maritime transport operations]

	ECI Directive	Aviation Security Regulation - 300/2008	Commission Implementing Regulation (EU) 2015/1998	Action Plan to protect rail passengers and staff in Member States	Ship and port facility security Regulation - 725/2004	Port Security Directive - 2005/65
	functions]				as anchorages, waiting berths and approaches from seaward, as appropriate	
Other definitions	*significance of impact*: based on sectoral criteria and cross-cutting criteria: casualties, economic effects, public effects; these are defined on a case-by-case basis - JRC has elaborated non-binding guidelines (sectoral criteria are classified and details of cross-cutting criteria); JRC guidelines mention that only one cross-sectoral criterion is necessary *protection*: all activities aimed at ensuring the functionality, continuity and integrity of CI in order to deter, mitigate and neutralise a threat, risk or vulnerability	**Aviation security**: the combination of measures and human and material resources intended to safeguard civil aviation against acts of unlawful interference that jeopardise the security of civil aviation	None	None	**Maritime security**: combination of preventive measures intended to protect shipping and port facilities against threats of intentional unlawful acts **Intentional unlawful act**: a deliberate act, which, by its nature or context, could harm the vessels used for international or national maritime traffic, their passengers or their cargoes, or the port facilities connected therewith	None

	ECI Directive	Aviation Security Regulation - 300/2008	Commission Implementing Regulation (EU) 2015/1998	Action Plan to protect rail passengers and staff in Member States	Ship and port facility security Regulation - 725/2004	Port Security Directive - 2005/65
Definition of operators / owners	**Owners/operators of ECI**: entities responsible for investment in, and/or day-to-day operation of, an ECI	**Operator:** person, organisation or enterprise engaged, or offering to engage, in an air transport operation; **Air carrier:** air transport undertaking holding a valid operating licence or equivalent; **Entity:** a person, organisation or enterprise, other than an operator (all called stakeholders)	Covered in Aviation Security Regulation - 300/2008	Not covered in document	**Operators/ owners**: Referred to in SOLAS as "Company", the owner of the ship or any other organisation or person such as the manager, or the bareboat charterer, who has assumed the responsibility for operation of the ship from the owner of the ship and who on assuming such responsibility has agreed to take over all the duties and responsibilities imposed by the International Safety Management Code (itself a chapter of SOLAS)	Operators/owners not defined in document
Provisions on co-operation across MS/with EC	**Before the identification** of potential ECI: discussion on the thresholds of cross-cutting criteria **Before the designation** of ECI: bilateral	**Stakeholders' Advisory Group on Aviation Security:** composed of European representative organisations (private or public) engaged in, or directly affected by,	**Industry associations and entities under their responsibility operating quality assurance programmes:** may be approved as EU aviation security validators	**EU Rail Passenger Security Platform:** the Platform will be composed of experts from MS and will facilitate information sharing and expertise at European and	**MS communicate (means/venue not specified):** - to other MS the information required pursuant to regulation 13 (Communication of information)	**MS:** - appoint a **focal point for port security**, which may be, but does not have to be, the same focal point as the one appointed under Regulation (EC) No

	ECI Directive	Aviation Security Regulation - 300/2008	Commission Implementing Regulation (EU) 2015/1998	Action Plan to protect rail passengers and staff in Member States	Ship and port facility security Regulation - 725/2004	Port Security Directive - 2005/65
	discussion **ECIP contact point**: to coordinate ECI issues within MS, across Ms with EC	aviation security. The role of this group shall be solely to **advise the EC.** **Single authority responsible** at MS level for coordination and implementation the application of the common basic standards and co-operation with the EC regarding monitoring and improvement of the application of the security standards.	provided equivalent measures of those programmes ensure impartial and objective validation. **Recognition** shall be done in co-operation of the appropriate authorities of **at least 2 MS**. *(Annex, 11.6.4.4)* Any **competencies acquired** by a person in order to meet the requirements under Regulation (EC) No 300/2008 and its implementing acts in one MS will be recognised by other MS	national level *(Annex to COM(2018) 470 final, I.1)* **MS:** - invited to appoint a national contact point on rail security for all companies operating on the respective MS territory. *(Annex to COM(2018) 470 final, II.4)* - invited to implement a **mechanism at national level for sharing relevant information on rail security domestically and with other MS** through the EU Rail Passenger Security Platform. *(Annex to COM(2018) 470 final, II.5)*	*(Annex I, Regulation 13)*.[165] - to other MS the **contact details** of the contact officials (Government officers to whom an SSO (ship security officer), a CSO (company security officer) and a PFSO (port facility security officer) can report security concerns) - all **known facts** (as laid down in 4.41 of Part B of the ISPS Code) when a **ship is expelled** from or refused entry to a Community port. **MS and the EC cooperate:** **-** through **coordination meetings** and/or any other appropriate means, in order to define, as appropriate, a **common position**	725/2004 to serve as contact point for the EC and other MS and to facilitate, follow up and provide information on the application of the port security measures

[165] Information required includes for example names and contact details of national authority or authorities responsible for ship/port facility security, and locations covered by appropriate security plans.

	ECI Directive	Aviation Security Regulation - 300/2008	Commission Implementing Regulation (EU) 2015/1998	Action Plan to protect rail passengers and staff in Member States	Ship and port facility security Regulation - 725/2004	Port Security Directive - 2005/65
					or approach in the competent **international fora**, in order to reduce the risks of conflict between Community maritime legislation and international instruments. **<u>MS:</u>** - **designate a focal point for maritime security**, which serves as a contact point for the EC and other MS and provides help and information on the application of the maritime security measures - may conclude among themselves, each acting on its own behalf, the **bilateral or multilateral agreements** provided for in the said SOLAS regulation, may, in particular, consider such agreements in order to **promote intra-Community**	

	ECI Directive	Aviation Security Regulation - 300/2008	Commission Implementing Regulation (EU) 2015/1998	Action Plan to protect rail passengers and staff in Member States	Ship and port facility security Regulation - 725/2004	Port Security Directive - 2005/65
					short sea shipping.	
Obligations: identifications of objects to protect	**MS:** - **Identify potential ECI by applying**: sectoral criteria, definition of CI, transboundary criterion, cross-cutting criteria (whose thresholds need to be defined with second MS) - Launch of bilateral discussions for the **identification** and **designation** **- Inform the MS** involved by ECI and the operators/ owners of ECI	None	None	None	**MS:** **Determine,** on the basis of the port facility security assessments, **which port facilities are concerned**, as not all ports receive enough international traffic, which could make applying all the rules to all port facilities in certain ports disproportionate.	**MS:** **define for each port the boundaries of the port** for the purposes of this Directive, appropriately taking into account information resulting from the port security assessment.
Obligations: setting the goals	None	**MS:** - Create a **national civil aviation security programme**, that defines responsibilities for the implementation of the common basic standards for safeguarding civil aviation and describes the measures required by operators and	Covered in Aviation Security Regulation - 300/2008	**MS:** invited to adopt a **programme for rail security management at national level,** identifying responsibilities and including protection and mitigation measures based on an analysis and assessment of risk. *(Annex to COM(2018) 470 final, II.6)*	**MS:** Adopt a **national programme for the implementation of this Regulation**, which will set the minimum security arrangements for ships, ports and government agencies.	Not covered in document

	ECI Directive	Aviation Security Regulation - 300/2008	Commission Implementing Regulation (EU) 2015/1998	Action Plan to protect rail passengers and staff in Member States	Ship and port facility security Regulation - 725/2004	Port Security Directive - 2005/65
		entities for this purpose. - Create **national quality control programme** that enables the MS to check the quality of civil aviation security to monitor compliance both with this Regulation and with its national civil aviation security programme.				
Obligations: threat assessments	**MS:** Carry out a threat assessment per subsector if they have designated an ECI	None	None	**EC:** will adopt a common methodology for the **assessment of rail security risks at EU level.** *(Annex to COM(2018) 470 final, I.2)* will develop a **regular assessment** and exchange of information concerning international rail services. *(Annex to COM(2018) 470 final, I.2)*	**MS:** **-** Ensure the completion of the **port facility security assessment (PFSA)**, which is both a **threat assessment** and a subsequent analysis of risks, and can be conducted by the MS or a recognised security organisation **Operator:** - ensures, through a company security officer, that the ship **security assessment**	**MS:** Ensure that **port security assessments** are carried out for the ports covered by this Directive, and are **reviewed** at least once **every 5 years**. The port security assessment as defined in the Annex I consists of both a threat assessment and a subsequent risk analysis, based on the risk those threats pose.

	ECI Directive	Aviation Security Regulation - 300/2008	Commission Implementing Regulation (EU) 2015/1998	Action Plan to protect rail passengers and staff in Member States	Ship and port facility security Regulation - 725/2004	Port Security Directive - 2005/65
					(SSA), which is both a **threat assessment** and a subsequent analysis of risks, is carried out by persons with appropriate skills to evaluate the security of a ship	
Obligations: risk analysis	**MS:** - Ensure that operators have developed an Operator Security Plan (OSP) or equivalent and renewed each year - ensure that a communication mechanism with SLO is in place **Operators /owners**: - Identify important assets, carry out risk analysis based on major threat scenario, vulnerability of each asset, potential impact (in the OSP)	**MS:** no specific requirement but some provisions presupposes a risk assessment, i.e.: - application of more stringent measures than those laid in this Regulation - adoption of alternative security measures that provide an adequate level of protection	**MS:** - **risk assessment** to be performed in relation to some obligations, e.g. plan to embark a potentially disruptive passenger, establish the **frequency of screening** of persons other than passengers and items carried on a continuous random basis. **Stakeholders:** - **risk assessment** to be performed in relation to some obligations, e.g. the frequency and means of undertaking	Not covered in document	As above: see threat assessment	As above: see threat assessment

	ECI Directive	Aviation Security Regulation - 300/2008	Commission Implementing Regulation (EU) 2015/1998	Action Plan to protect rail passengers and staff in Member States	Ship and port facility security Regulation - 725/2004	Port Security Directive - 2005/65
			surveillance and patrols			
Obligations: Risk management	**Operators/ owners**: identify, select and prioritise counter-measures and procedures, distinguishing between permanent and graduated security measures (in the OSP) - Establish the SLO: link between ECI owners/operators and MS authority **MS**: ensure that an OSP or equivalent is in place and Security Liaison Officers (SLO) appointed	**MS:** ensure the **application of the common basic standards for safeguarding civil aviation.** **Stakeholders:** draw up, apply and maintain an **airport/air carrier security programme** that describes the methods and procedures which are to be followed to comply both with this Regulation and with the national civil aviation security programme of the MS.	**Stakeholders:** - every authority/airport operator/air carrier/entity responsible ensures **the implementation of the measures** set out in the Annex - every entity has a **person responsible for security** at its premises, serving as a contact point	**MS:** are invited to **require railway undertakings and infrastructure and station managers to adopt a security management plan** at company level, based on an analysis and assessment of risk, and proportionate to national threat levels. *(Annex to COM(2018) 470 final, II.7)*	**MS:** **-** approve of the **ship security plans or the port facility** security plans and **test** their **effectiveness** **-** provide general guidance on the measures considered appropriate to **reduce the security risk** to ships flying their flag when at sea - introduce a system of **3 security levels** for ships and port facilities - decide the extent to which they will apply the provisions of this Regulation to different categories of ships operating domestic services (other than Class A passenger ships) with the overall level of security not compromised by such a decision.	**MS:** - introduce a system of **3 security levels** for ports or parts of ports, determine the security levels in use for each port or part of a port *(Art. 8(3))* - ensure that **port security plans** are developed, maintained and updated. Port security plan shall be reviewed at least once every five years. *(Art. 7)* - Set up a system ensuring adequate and regular supervision of the **port security plans** and their implementation. **Port security authority:** implement **different security measures** in different parts of the port depending on the findings of

	ECI Directive	Aviation Security Regulation - 300/2008	Commission Implementing Regulation (EU) 2015/1998	Action Plan to protect rail passengers and staff in Member States	Ship and port facility security Regulation - 725/2004	Port Security Directive - 2005/65
					Operators: - ensure the development, maintenance, implementing and exercising of the **port facility or ship security plan**, with the development and maintenance requiring an aforementioned port facility security assessment (by port or company security officers as appointed by the owner /operator, who also serve as points of contact between the operator and the MS)	the port security assessment and in accordance with the security levels as determined by the MS **Operators/owners:** - appoint **port security officers** who fulfil the role of **point of contact** for port security related issues.
Obligations: Crisis management	**Operators/ owners**: Identify, crisis management measures (in the OSP)	**MS:** If an MS has reason to believe that the level of aviation security has been compromised through a security breach, it shall ensure that **appropriate and prompt action is taken to rectify**	**Entity responsible in accordance with national civil aviation security programme:** Impossible to say what the programme contains for each MS and with whom the responsibility	**Information to be provided to passengers in case of a security incident** is within the targeted areas for action in the context of the technical work of the platform in the form of technical guidance	**Any competent authority, which may include the company operating the ship:** having received notification of a ship security alert (meaning that is under threat or it has been	Not covered in document

	ECI Directive	Aviation Security Regulation - 300/2008	Commission Implementing Regulation (EU) 2015/1998	Action Plan to protect rail passengers and staff in Member States	Ship and port facility security Regulation - 725/2004	Port Security Directive - 2005/65
		that breach and ensure the continuing security of civil aviation. MS taking action might mean requiring the operator to have a crisis management plan and to follow it when a breach of security (and a possible following crisis situation) happens. This depends on how the Regulation was implemented by the MS in question.	lies in each particular case. Anyway, **measures shall be in place that** both deter persons from breaching security checkpoints and**, should such a breach occur, promptly enable the breach and its repercussions to be resolved and rectified.**	documents. *(Annex to COM(2018) 470 final, I.3)*	compromised), immediately notifies the State(s) (all, not only MS) in the vicinity of which the ship is presently operating **Operators** The Port facility plan includes measures to react to alerts and procedures responding to security threats or breaches of security	
Reporting to EC	**MS:** - on annual basis on: the number of infrastructure per sector for which cross-cutting criteria **discussions** were held and the number of **designated ECI** per sector and number of MS dependent - every 2 years on: summary of **threat assessment** (type of risks, threats,	**MS:** - all airports in its territory serving civil aviation other than those for which alternative security measures were adopted - possible adoption of **alternative security measures** that provide an adequate level of protection on the basis of a local risk assessment - possible adoption of **more stringent**	**MS** - inform EC when it grants permission to permit standard 2 EDS (Explosive detection systems equipment) to continue to be used after the expiry of standard 2 *(Annex, 12.4.2.4)* - inform in writing EC and other MS before its planned introduction of methods of screening using new technologies - at intervals of no	Not covered in document	**MS** - decisions regarding the extent to which they will apply the provisions of this Regulation to different categories of ships operating domestic services (other than those referred to in paragraph 2, their companies and the port facilities serving the) - the **information** required pursuant to regulation 13	**MS:** - communicate to the EC **the text of the main provisions of national law** which they adopt in the field covered by this Directive. - appoint a **focal point for port security**, which communicates to the EC **the list of ports** concerned by this Directive and shall inform it of any changes to that list. *(Art. 12)*

	ECI Directive	Aviation Security Regulation - 300/2008	Commission Implementing Regulation (EU) 2015/1998	Action Plan to protect rail passengers and staff in Member States	Ship and port facility security Regulation - 725/2004	Port Security Directive - 2005/65
	and vulnerabilities per ECI sector)	**measures** as soon as possible after their application - **measures required by a third country** if they differ from the common basic standards in respect of flights from an airport in MS to, or over, that third country	more than six months during the 18 month long evaluation period for a method of screening, the appropriate authority in MS concerned shall provide the EC with a progress report on the evaluation. *(Annex, 12.8.2, 12.8.5)* - possible categories of passengers / cabin baggage / hold baggage that, for objective reasons, shall be subject to special screening procedures or may be exempted from screening.		(Communication of information) *(Annex I, Regulation 13)* - the **contact details** of the contact officials (Government officers to whom an SSO (ship security officer), a CSO (company security officer) and a PFSO (port facility security officer) can report security concerns) **and the all known facts** (as laid down in 4.41 of Part B of the ISPS Code) when a ship is expelled from or refused entry to a Community port. - the **list of port facilities** concerned on the basis of the port facility security assessments carried out to the other and sufficient details of the measures taken. - the **alternative security arrangements**	

	ECI Directive	Aviation Security Regulation - 300/2008	Commission Implementing Regulation (EU) 2015/1998	Action Plan to protect rail passengers and staff in Member States	Ship and port facility security Regulation - 725/2004	Port Security Directive - 2005/65
					between MS and provide sufficient details of the measures to allow the EC to consider whether the agreements compromise the level of security of other ships or port facilities not covered by the agreements. - **sufficient details of the equivalent security arrangements** as provided for in regulation 12 (equivalent security arrangements) of the special measures to enhance maritime security of the SOLAS Convention when they are adopted, and the outcome of periodic reviews thereof, at the latest five years after they were adopted or last reviewed.	
Reporting (other than to the EC)		**Stakeholders:** Submit **security programmes** to	**MS** - notifies the **air carrier** in writing in	Not covered in document	**MS:** - to the **IMO,** the EC and the other	**MS:** - communicate to the **appropriate person**

	ECI Directive	Aviation Security Regulation - 300/2008	Commission Implementing Regulation (EU) 2015/1998	Action Plan to protect rail passengers and staff in Member States	Ship and port facility security Regulation - 725/2004	Port Security Directive - 2005/65
		the appropriate authority.	advance of the plan to embark a **potentially disruptive passenger** on board its aircraft **<u>Airport operator:</u>** - informs those **carriers that are affected** when an area is no longer considered to be a critical part because of a change of security status **<u>Entity:</u>** - informs the **appropriate authority** of any **changes** related to its **AEO certificate** referred to in point (b) or (c) of Article 14a(1) of Regulation (EEC) No 2454/93 ('Security and safety' or 'Customs Simplifications / security and safety' AEO certificates). *(Annex, 6.3.1.5)* - informs the **regulated agent** of the name and contact details of		MS: the information required pursuant to regulation 13 (Communication of information) of the special measures to enhance maritime security of the SOLAS Convention. *(Art. 4(4))* - provide the security level information to ships and port facilities - to other MS: **list of port facilities** concerned on the basis of the port facility security assessments carried out to the other and sufficient details of the measures taken.	or persons (all affected by the security level, e.g. masters of ships, security officers for companies, ships, ports and port facilities) the **security level in force for each port** or part of a port as well as any changes thereto. *(Art. 8(4))*

	ECI Directive	Aviation Security Regulation - 300/2008	Commission Implementing Regulation (EU) 2015/1998	Action Plan to protect rail passengers and staff in Member States	Ship and port facility security Regulation - 725/2004	Port Security Directive - 2005/65
			the **person responsible for security** at its premises			
Sanctions		**MS:** - lay down the **rules on penalties** applicable to infringements of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be **effective, proportionate and dissuasive.** *(Art.21)*	Covered in Aviation Security Regulation - 300/2008	Not covered in document	**MS:** - ensure that **effective, proportionate and dissuasive sanctions** for breaching the provisions of this Regulation are introduced.	**MS:** - ensure that **effective, proportionate and dissuasive penalties** are introduced for infringements of the national provisions adopted pursuant to this Directive, which can affect the port security authority, operators and all other entities and persons involved.
Other		**EC in coop. with MS:** - conduct unannounced **inspections**, including inspections of airports, operators and entities applying aviation security standards - inspection report shall be communicated to the appropriate authority of the MS	None	**Sources :** https://ec.europa.eu/transport/modes/rail/news/2018-06-12-action-plan-security-rail-passengers_en https://ec.europa.eu/transport/sites/transport/files/com20180470-annex.pdf	The Regulation implements the standards set in the International Ship and Port Facility Security Code (ISPS Code) which itself is an amendment to the International Convention for the Safety of Life at Sea (SOLAS)	**Relation to Ship and port facility security Regulation - 725/2004:** "On 31 March 2004 the European Parliament and the Council of the European Union adopted Regulation (EC) No 725/2004 (4) on enhancing ship and port facility security. **The maritime security measures imposed by that Regulation**

	ECI Directive	Aviation Security Regulation - 300/2008	Commission Implementing Regulation (EU) 2015/1998	Action Plan to protect rail passengers and staff in Member States	Ship and port facility security Regulation - 725/2004	Port Security Directive - 2005/65
		concerned				**constitute only part of the measures necessary to achieve an adequate level of security** throughout maritime-linked transport chains. That Regulation is limited in scope to security measures on board vessels and the immediate ship/port interface. "MS shall ensure that port security measures introduced by this Directive are closely coordinated with measures taken pursuant to Regulation (EC) No 725/2004."

8.3.3. NIS Directive

	ECI Directive	NIS Directive
Legal basis	Article 308 Treaty establishing the European Community (other measures)	Article 114 TFEU - approximation of laws, in common rules on competition, taxation and approximation of laws
Objectives	Provide procedures for the **identification and designation of ECI**, and common approach to the assessment of the need to improve the **protection**	Measures with a view to achieving a high common level of **security of network and information systems** within the Union so as to improve the functioning of the internal market
Sectors covered by security measures	**Energy:** electricity, oil, gas **Transport**: road, rail, air, inland waterways, ocean and short-sea shipping and ports	**Energy**: electricity, oil, gas **Transport**: road, rail, air, water **Banking; financial market** infrastructures; **health** sector:

	ECI Directive	NIS Directive
		health care settings; drinking **water** supply and distribution; **digital** infrastructures
Type of threats	All-hazards approach while countering threats from terrorism as a priority	Any type of threat (cyber and physical) insofar as it affects the NIS[166]
Operations	Threat assessment, risk analysis, risk management	Threat assessment, risk analysis, risk management, crisis management
Definition of object to protect (e.g. CI)	**ECI**: CI located in MS the disruption of which would have significant impact on at least 2 MS [**CI:** asset, system or part thereof located in MS which is essential for the maintenance of vital societal functions, health, safety, security, economic and social well-being of people, and the disruption of which would have a *significant impact* in a MS as a result of the failure to maintain these functions]	**Essential services:** 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 [***network and information system***: i) transmission systems and, where applicable, switching or routing equipment and other resources as per Directive E 2002/21/EC, 2(a); ii) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; iii) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance]
Operational elements of definition	***significance of impact***: based on sectoral criteria and cross-cutting criteria: casualties, economic effects, public effects; these are defined on a case-by-case basis - JRC has elaborated non-binding guidelines (sectoral criteria are classified and details of cross-cutting criteria); JRC guidelines mention that only one cross-sectoral criterion is necessary ***protection***: all activities aimed at ensuring the functionality, continuity and integrity of CI in order to deter, mitigate and neutralise a threat, risk or vulnerability	***significant disruptive effect***: based on cross-sectoral factors: - number of users relying on the service; - dependency of other relevant sectors; - impact that incidents could have in terms degree and duration, on economic and societal activities or public safety; - market share of the entity; - geographical spread of the area that could be affected by the incident; - importance of entity for maintaining sufficient level of the service taking into account alternative means for the provision of service - where appropriate, sector-specific factors should be taken into account ***security*** thereof: the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems]

[166] Interview: 1 EC DGs and Agencies.

	ECI Directive	NIS Directive
Definition of operators /owners	**Owners/operators of ECI**: entities responsible for investment in, and/or day-to-day operation of, an ECI	**Operator of essential services:** public or private entity i) that provides a service which is essential for the maintenance of critical societal and/or economic activities; ii) the provision of the service depends on network and information system; iii) an incident would have significant disruptive effects on the provision of the service of a type referred to in Annex II, which meets the criteria laid down in Article 5(2) **Digital service provider:** legal person providing a digital service (online marketplace, search engine, cloud computing) normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services (Article 1(1) of Directive (EU) 2015/1535)
Provisions on co-operation across MS/with EC	**Before the identification** of potential ECI: discussion on the thresholds of cross-cutting criteria **Before the designation** of ECI: bilateral discussion **ECIP contact point**: to coordinate ECI issues within MS, across Ms with EC	**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 2+ MS **Co-operation Group**: composed of MS, EC (secretariat), ENISA, regulated by biannual Work Programmes tasked with: providing guidance for CSIRTs activities, exchange best practices (on incident notification, capacity building, awareness-raising training, R&D, risks and incidents, identification of operators), discussing capabilities and preparedness of MS, discussing standards, examining summary reports, discuss modalities to report notification **Network of computer security incident response teams network (CSIRT)**: national CSIRTs, CERT-EU, EC (as observer), ENISA (secretariat), tasked with exchanging info on operations and capabilities and also on individual accident, identify coordinated response to incidents in MS (if the MS requests), support co-operation for cross-border incidents, discuss and explore further forms of operational co-operation, lessons learned and guidelines **CSIRT or competent authority**: inform other MS of incidents having an impact there Designate a **single point of contact** to liaise with another MS
Obligations: identifications of objects to protect	**MS:** - **Identify potential ECI by applying**: sectoral criteria, definition of CI, transboundary criterion, cross-cutting criteria (whose thresholds need to be defined with second MS)	**MS:** **- Prepare list of essential services** and review on at least every 2 years - Designation of **national competent authorities** (also >1) and **single point of contact** who will be the liaison with authorities in

	ECI Directive	NIS Directive
	- Launch of bilateral discussions for the **identification** and **designation** **- Inform the MS** involved by ECI and the operators/ owners of ECI	other MS, the Co-operation Group and CSIRT - Designation of Computer security incident response teams (**CSIRT**)
Obligations: setting the goals	None	**National strategy on the security of network and information systems**, including: strategic objectives; governance framework; measures on identification of measures relating to preparedness, response and recovery; relevant education, awareness-raising and training programmes; R&D plans; risk assessment plan; list of actors involved in the implementation of the strategy) covering at least the sectors under the directive Designate one or more national competent authorities that should monitor the application of the Directive
Obligations: threat assessments	**MS:** Carry out a threat assessment per subsector if they have designated an ECI	
Obligations: risk analysis	**MS:** - Ensure that operators have developed an Operator Security Plan (OSP) or equivalent and renewed each year - ensure that a communication mechanism with SLO is in place **Operators /owners**: - Identify important assets, carry out risk analysis based on major threat scenario, vulnerability of each asset, potential impact (in the OSP)	**Operators/digital service providers:** **-** assess the security of their network and info systems **CSIRT**: - Provide dynamic risk and incident analysis and situational awareness
Obligations: Risk management	**Operators/ owners**: identify, select and prioritise counter-measures and procedures, distinguishing between permanent and graduated security measures (in the OSP) - Establish the SLO: link between ECI owners/operators and MS authority **MS**: ensure that an OSP or equivalent is in place and Security Liaison Officers (SLO) appointed	**MS:** ensure that operators and digital service providers comply with the below **Operators and Digital service providers:** - take appropriate and proportionate technical and organisational measures to manage the risks, to prevent and minimise the impact of incidents ensuring the continuity of services, - notify the competent authority or CSIRT incidents having significant impact on the service

	ECI Directive	NIS Directive
Obligations: Crisis management	**Operators/ owners**: Identify, crisis management measures (in the OSP)	**CSIRT or competent authority:** inform other MS of incidents having an impact there **CSIRT:** monitor incidents; provide early warning, alerts, and dissemination of info to stakeholders; respond to incidents; provide dynamic incident analysis and situational awareness; promotion of incidents and risk-handling procedures; incident, risks and info classification schemes **Operators and Digital service providers:** - take appropriate and proportionate technical and organisational measures to manage the risks, to prevent and minimise the impact of incidents ensuring the continuity of services, - notify the competent authority or CSIRT incidents having significant impact on the service
Reporting to EC	**MS:** - on annual basis on: the number of infrastructure per sector for which cross-cutting criteria **discussions** were held and the number of **designated ECI** per sector and number of MS dependent - every 2 years on: summary of **threat assessment** (type of risks, threats, and vulnerabilities per ECI sector)	**MS:** - every 2 years on: **national measures** allowing the identification of operators of essential services; the list of essential services; number of operators of essential services per each sector; thresholds - communicate to the EC the **national strategie**s on the security of network and information systems - the **competent authorities** and **single point of contact** - the r**emit and main elements of the incident-handling process of CSIRTs**
Reporting (other than to the EC)		Every year, the single point of contact shall **submit a summary** report to the Co-operation Group **on notifications of incidents received, actions taken**

8.3.4. Other sectoral legislation

8.3.4.1. Space

	ECI Directive	European Satellite Navigation systems Regulation - 1285/2013	Aspects of the deployment, operation and use of the European Global Navigation Satellite System - Council Decision 2014/496/CFSP	SST Decision - 541/2014/EU	Space programme Regulation (proposal) - COM(2018) 447 final	Copernicus Regulation – 377/2014
Legal basis	Article 308 Treaty establishing the European Community (other measures)	Article 172 TFEU (research and technological development and space)	Article 28 Treaty on European Union - (charging expenditures to the Union budget)	Art. 189(2) TFEU (space policy/space programme)	Art. 189(2) TFEU (space policy/space programme)	Art. 189(2) TFEU (space policy/space programme)
Objectives	Provide procedures for the **identification and designation of ECI**, and common approach to the assessment of the need to improve the **protection**	Lay down the **rules in relation to the implementation and exploitation of two satellite navigation systems - the system established under the Galileo programme and the EGNOS system -** under the European satellite navigation programmes, in particular those relating to the governance and the financial contribution of the Union	**Set out the responsibilities to be exercised by the Council and the High Representative of the Union for Foreign Affairs and Security Policy (HR) to avert a threat to the security** of the Union or one or more MS **or to mitigate serious harm** to the essential interests of the Union or of one or more MS arising from the deployment, operation or use of the European Global Navigation Satellite System	Establish a **space surveillance and tracking (SST) support framework**, which will be: -assessing and **reducing** the **risks to in-orbit operations** of European spacecraft **relating to collisions**, enabling spacecraft operators to plan and carry out mitigation measures more efficiently -reducing the **risk** relating **to the launch** of European spacecraft -**surveying uncontrolled atmospheric re-entries** of	Establishing the space programme of the Union and the European Union Agency for the Space Programme, in particular to: - **provide**, or contribute to the provision of, high-quality and up-to-date and, where appropriate, secure **space-related data, information and services** without interruption and wherever possible at global level, meeting existing and future needs and able **to meet the Union's political priorities**, - **enhance the security** of the	Provide accurate and reliable information in the field of the environment and security, tailored to the needs of users and supporting other Union policies, in particular relating to the internal market, transport, environment, energy, civil protection and civil security, co-operation with third countries and humanitarian aid

	ECI Directive	European Satellite Navigation systems Regulation - 1285/2013	Aspects of the deployment, operation and use of the European Global Navigation Satellite System - Council Decision 2014/496/CFSP	SST Decision - 541/2014/EU	Space programme Regulation (proposal) - COM(2018) 447 final	Copernicus Regulation – 377/2014
				spacecraft or space debris, providing more accurate and efficient **early warnings** with the aim of reducing the potential risks to the safety of people and infrastructure	Union and its MS, its **freedom of action** and its strategic autonomy, in particular in terms of technologies and **evidence-based decision-making**	
Sectors covered by security measures	**Energy:** electricity, oil, gas **Transport**: road, rail, air, inland waterways, ocean and short-sea shipping and ports	**Space:** Satellite navigation	**Space:** Satellite navigation	**Space:** spacecraft in general	**Space:** space related infrastructure in general	**Space:** Earth observation and monitoring
Type of threats	All hazards approach while countering threats from terrorism as a priority	Not covered in document	**Threat to the security of the Union or one or more MS arising from the deployment, operation or use of the European Global Navigation Satellite System,** in particular as a result of an international situation requiring action by the Union or in the event of a **threat to the operation of the**	Collision between spacecraft and space objects, uncontrolled re-entry of space objects	Physical attacks, cyber-attacks	Not covered in document

	ECI Directive	European Satellite Navigation systems Regulation - 1285/2013	Aspects of the deployment, operation and use of the European Global Navigation Satellite System - Council Decision 2014/496/CFSP	SST Decision - 541/2014/EU	Space programme Regulation (proposal) - COM(2018) 447 final	Copernicus Regulation – 377/2014
			system itself or its services.			
Operations	Threat assessment, risk analysis, risk management	Risk management, crisis management	Risk management, crisis management	Threat assessment, risk analysis, risk management	Threat assessment, risk analysis, risk management	Risk assessment, risk management
Definition of object to protect (e.g. CI)	**ECI**: CI located in MS the disruption of which would have significant impact on at least 2 MS [**CI:** asset, system or part thereof located in MS which is essential for the maintenance of vital societal functions, health, safety, security, economic and social well-being of people, and the disruption of which would have a *significant impact* in a MS as a result of the failure to maintain these functions]	**Two satellite navigation systems,** the system established under the **Galileo** programme and the **EGNOS** system ('the systems'). Each system's infrastructure consists of satellites and a network of ground stations.	The European Global Navigation Satellite System ('GNSS') / security of the EU and its MS	European and national **space infrastructure, facilities and services** which are essential for the safety and security of the economies, societies and citizens in Europe, Union **citizens** and **terrestrial infrastructure**	**Infrastructure**, both ground and space Sensitive non-classified and classified **information**	Each significant item of Copernicus infrastructure
Operational elements of definition	***significance of impact***: based on sectoral criteria and cross-cutting criteria: casualties, economic effects, public effects; these	None	None	None	None	None

	ECI Directive	European Satellite Navigation systems Regulation - 1285/2013	Aspects of the deployment, operation and use of the European Global Navigation Satellite System - Council Decision 2014/496/CFSP	SST Decision - 541/2014/EU	Space programme Regulation (proposal) - COM(2018) 447 final	Copernicus Regulation – 377/2014
	are defined on a case-by-case basis - JRC has elaborated non-binding guidelines (sectoral criteria are classified and details of cross-cutting criteria); JRC guidelines mention that only one cross-sectoral criterion is necessary ***protection***: all activities aimed at ensuring the functionality, continuity and integrity of CI in order to deter, mitigate and neutralise a threat, risk or vulnerability					
Definition of operators /owners	**Owners/operators of ECI**: entities responsible for investment in, and/or day-to-day operation of, an ECI	None	The European Global Navigation Satellite System Agency ('the GSA') - operator of the Galileo Security Monitoring Centre ('GSMC')	None	**European Union Agency for the Space Programme ('Agency'):** replaces and succeeds the European GNSS Agency **Security Accreditation Board (SAB):** part of the Agency, it is the security	Copernicus users **Copernicus core users**: Union institutions and bodies, European, national, regional or local authorities entrusted with the definition, implementation, enforcement or monitoring of a public service or

	ECI Directive	European Satellite Navigation systems Regulation - 1285/2013	Aspects of the deployment, operation and use of the European Global Navigation Satellite System - Council Decision 2014/496/CFSP	SST Decision - 541/2014/EU	Space programme Regulation (proposal) - COM(2018) 447 final	Copernicus Regulation – 377/2014
					accreditation authority for all the components of the Programme **Entity:** the entity responsible for the management of a component of the Programme (Galileo, EGNOS, Copernicus, SST, GOVSATCOM)	policy in the areas of atmosphere monitoring, marine environment monitoring, land monitoring, climate change, emergency management and security
Provisions on co-operation across MS/with EC	**Before the identification** of potential ECI: discussion on the thresholds of cross-cutting criteria **Before the designation** of ECI: bilateral discussion **ECIP contact point**: to coordinate ECI issues within MS, across Ms with EC	**EC, the European GNSS Agency, ESA, and MS:** -base the public governance of the Galileo and EGNOS programmes shall be based on the principle of **sincere co-operation** **EC:** - **establish coordination mechanisms** between the various bodies involved **MS:** - **take all necessary measures to ensure the good**	**MS:** - designate **point of contact** to assist in the operational management of a threat	**MS:** - **may participate** if they own/have access to adequate infrastructure - if participating, designate a **national entity** to **represent** them in the **consortium** **-** if participating, help the **EC** in the **implementation of the SST** **Consortium of national entities:** - lay down **rules and mechanisms** for their **co-operation** in the **implementation** of the SST	**MS:** - may participate in the Programme by **contributing** with their **technical competence**, **know-how** and **assistance**, in particular **in the field of safety and security**, and, where necessary, by making available to the Union the information and infrastructure in their possession or located on their territory -may be entrusted with **specific tasks** by the EC or the Agency	**EC:** - facilitate coordinated contributions of Member States aiming at the operational delivery of services and the long-term availability of necessary observation data.

	ECI Directive	European Satellite Navigation systems Regulation - 1285/2013	Aspects of the deployment, operation and use of the European Global Navigation Satellite System - Council Decision 2014/496/CFSP	SST Decision - 541/2014/EU	Space programme Regulation (proposal) - COM(2018) 447 final	Copernicus Regulation – 377/2014
		functioning of the Galileo and EGNOS programmes **including measures to ensure the protection** of the ground stations established on their territories		**European Union Satellite Centre (SATCEN):** - may **cooperate** with the **consortium** of national entities	- work **together with the EC** in order to **develop** the **in-situ component** necessary for the **uptake of space systems** and to **facilitate** the **use of in-situ data sets**	
Obligations: identifications of objects to protect	**MS:** - **Identify potential ECI by applying**: sectoral criteria, definition of CI, transboundary criterion, cross-cutting criteria (whose thresholds need to be defined with second MS) - Launch of bilateral discussions for the **identification** and **designation** **- Inform the MS** involved by ECI and the operators/ owners of ECI	**EC:** lay down, where necessary, the measures, required to determine the location of the ground-based infrastructure of the systems **in accordance with security requirements**, following an open and transparent process and ensure its operation	None	None	None	None
Obligations : setting the goals	None	None	Within six months from the adoption of this Decision, the HR shall **prepare,** with the support of	None	None	None

	ECI Directive	European Satellite Navigation systems Regulation - 1285/2013	Aspects of the deployment, operation and use of the European Global Navigation Satellite System - Council Decision 2014/496/CFSP	SST Decision - 541/2014/EU	Space programme Regulation (proposal) - COM(2018) 447 final	Copernicus Regulation – 377/2014
			experts from MS, and submit for approval to the PSC, **the necessary early operational procedures for the practical implementation of the provisions set out in this Decision**			
Obligations: threat assessments	**MS:** Carry out a threat assessment per subsector if they have designated an ECI	None	None	**MS participating in the SST support framework:** - establish and operate a sensor function to survey and track space objects, resulting in a database of such - establish and operate a processing function, to analyse SST data and produce SST information	**Entity:** - carries out a threat analysis	None
Obligations: risk analysis	**MS:** - Ensure that operators have developed an Operator Security Plan (OSP) or equivalent and renewed each year - ensure that a	None	**MS:** - if appropriate, **take the necessary measures to ensure the implementation of this Decision** in their respective area	**MS participating in the SST support framework:** - set up a function to provide the services of risk assessment of both the collision between spacecraft	**Entity:** - carries out a **risk analysis** on the basis of the threat analysis **SAB:** - carries out **risk assessments** to	**EC:** - assess the necessary security measures which shall be designed to avoid any risks or threats for the interest or security of the Union or its

	ECI Directive	European Satellite Navigation systems Regulation - 1285/2013	Aspects of the deployment, operation and use of the European Global Navigation Satellite System - Council Decision 2014/496/CFSP	SST Decision - 541/2014/EU	Space programme Regulation (proposal) - COM(2018) 447 final	Copernicus Regulation – 377/2014
	communication mechanism with SLO is in place **Operators /owners**: - Identify important assets, carry out risk analysis based on major threat scenario, vulnerability of each asset, potential impact (in the OSP)		of responsibility, in accordance with, inter alia, Article 28 of Regulation (EU) No 1285/2013, which means that MS shall ensure the protection of the ground stations on their territories equivalent to that of ECI and shall not take any measures which could be detrimental to the programmes or the services provided through them	and space objects and of the uncontrolled atmospheric re-entry of space objects	prepare **risk reports** to advise the EC and the Agency on residual risk treatment options for a given security accreditation decision	Member States, in particular to ensure compliance with the principles set out in Decision 2001/844/EC, ECSC, Euratom and Decision 2013/488/EU
Obligations: Risk management	**Operators/ owners**: identify, select and prioritise counter-measures and procedures, distinguishing between permanent and graduated security measures (in the OSP) - Establish the SLO: link between ECI owners/operators and MS authority **MS**:	**EC:** - lay down, where necessary, the measures, required to **manage and reduce the risks** inherent in the progress of the Galileo and EGNOS programmes - **establish the necessary technical specifications and other measures** to implement the high-level objectives	**MS:** - if appropriate, **take the necessary measures to ensure the implementation of this Decision** in their respective area of responsibility, in accordance with, inter alia, Article 28 of Regulation (EU) No 1285/2013, which means that MS shall ensure the protection of the	**MS participating in the SST support framework:** - set up a function to provide the service of generation of collision avoidance alerts during spacecraft missions - set up a function to provide the service of generation of information related to the uncontrolled re-entry of space	**EC:** - based on the threat and risk analyses conducted by the entities **determines**, by means of implementing acts, the **general security requirements** **Entity:** - **ensures and monitors the security** of the Component, in	**EC:** - based on the risk analysis, establish the necessary security-related technical specifications for Copernicus

	ECI Directive	European Satellite Navigation systems Regulation - 1285/2013	Aspects of the deployment, operation and use of the European Global Navigation Satellite System - Council Decision 2014/496/CFSP	SST Decision - 541/2014/EU	Space programme Regulation (proposal) - COM(2018) 447 final	Copernicus Regulation – 377/2014
	ensure that an OSP or equivalent is in place and Security Liaison Officers (SLO) appointed	referred **MS:** - **ensure that its national security regulations offer a degree of protection of EU classified information**[167] -**ensure the protection of the ground stations** established on their territories which shall be at least equivalent to those required for the protection of European critical infrastructures within the meaning of **ECI Directive**	ground stations on their territories equivalent to that of ECI and shall not take any measures which could be detrimental to the programmes or the services provided through them	objects, including the estimation of the timeframe and likely location of possible impact - provide access to SST information and services on a need-to-know-basis to all MS, the EC, the Council, the EEAS, public and private spacecraft owners and operators and public authorities concerned with civil protection - ensure the security of SST data	particular setting of technical specifications and operational procedures, and monitors their compliance with the general security requirements **SAB:** - carries out security inspections, audits and tests, **emphasising** the importance of **security** and **effective risk management** and **recommending countermeasures** to mitigate the specific impact of **loss of confidentiality, integrity or availability of classified information** - defines and approves a security	

[167] Equivalent to that provided by the rules on security as set out in the Annex to Decision 2001/844/EC, ECSC, Euratom and by the security rules of the Council set out in the Annexes to Decision 2013/488/EU; (Art. 17(a)).

	ECI Directive	European Satellite Navigation systems Regulation - 1285/2013	Aspects of the deployment, operation and use of the European Global Navigation Satellite System - Council Decision 2014/496/CFSP	SST Decision - 541/2014/EU	Space programme Regulation (proposal) - COM(2018) 447 final	Copernicus Regulation – 377/2014
					accreditation strategy, takes security accreditation decisions **<u>MS:</u>** - transmit to the SAB **all information** they consider **relevant** for the purposes of **security accreditation** - ensure that its national security regulations offer a degree of protection of EU classified information - take measures which are at least equivalent to those necessary for the protection of ECI and to those necessary for the protection of their own national CI in order to ensure the protection of the ground infrastructure on the ground which form an integral part of	

	ECI Directive	European Satellite Navigation systems Regulation - 1285/2013	Aspects of the deployment, operation and use of the European Global Navigation Satellite System - Council Decision 2014/496/CFSP	SST Decision - 541/2014/EU	Space programme Regulation (proposal) - COM(2018) 447 final	Copernicus Regulation – 377/2014
					the Programme and which are located on their territory	
Obligations: Crisis management	**Operators/ owners**: Identify, crisis management measures (in the OSP)	Whenever the security of the Union or its MS may be affected by the operation of the systems, the procedures set out in Joint Action 2004/552/CFSP shall apply	**HR (High Representative of the Union for Foreign Affairs and Security Policy):** If the urgency of the situation requires immediate action to be taken before the Council has taken a decision upon a proposal from the HR, the HR is authorised to issue the necessary provisional instructions to the GSA	None	None	None
Reporting to EC	**MS:** - on annual basis on: the number of infrastructure per sector for which cross-cutting criteria **discussions** were held and the number of **designated ECI** per sector and number of MS dependent - every 2 years on:	**MS:** - without delay **inform EC of the national security regulations**	**HR (High Representative of the Union for Foreign Affairs and Security Policy):** - immediately **informs the Council and EC** of any instructions issued before the Council has taken a decision upon a	Not covered in document	**SAB:** - creates the part of the twice-yearly report by the Agency to the EC that is related to security **Agency:** - creates the rest of the twice-yearly report to the EC	Not covered in document

	ECI Directive	European Satellite Navigation systems Regulation - 1285/2013	Aspects of the deployment, operation and use of the European Global Navigation Satellite System - Council Decision 2014/496/CFSP	SST Decision - 541/2014/EU	Space programme Regulation (proposal) - COM(2018) 447 final	Copernicus Regulation – 377/2014
	summary of **threat assessment** (type of risks, threats, and vulnerabilities per ECI sector)		proposal from the HR If the urgency of the situation required immediate action			
Reporting (other than to the EC)		Not covered in document	**MS, EC or the GSA (as appropriate):** - immediately **inform the Council and the HR** in the event of such a threat **of all the elements at their disposal which they consider relevant**	**EC:** - forward a **report** on the **implementation** of the **SST** support framework to the **European Parliament** and the **Council** concerning the achievement of the objectives of this Decision, from the point of view of both results and impacts, the effectiveness of the use of resources and the European added value	None	**EC:** - provide a report on Copernicus progress at each Copernicus Committee meeting. Those reports shall give a general overview of Copernicus status and developments, in particular in terms of risk management, costs, schedule, performance, procurement, and relevant advice provided to the Commission.
Sanctions		**EC:** - take the appropriate measures to ensure that the **financial interests** of the **Union** are **protected** when actions financed under this Regulation are implemented, by the	None	MS, EC, SATCEN **shall not be held liable** for any damage resulting from the lack or interruption in the provision of the SST services, any delay in their provision, any inaccuracy of the information provided through	**Agency:** recovers **sums unduly paid** where irregularities are detected and, where appropriate, applies effective, proportionate and dissuasive administrative and financial penalties	None

	ECI Directive	European Satellite Navigation systems Regulation - 1285/2013	Aspects of the deployment, operation and use of the European Global Navigation Satellite System - Council Decision 2014/496/CFSP	SST Decision - 541/2014/EU	Space programme Regulation (proposal) - COM(2018) 447 final	Copernicus Regulation – 377/2014
		application of preventive measures against fraud, corruption and any other illegal activities, by effective checks and, if irregularities are detected, by the recovery of amounts unduly paid and, if necessary, **by effective, proportionate and dissuasive penalties**. *(Art. 32(1))* The financial interests of the Union should be protected through proportionate measures throughout the expenditure cycle, including the prevention, detection and investigation of irregularities, the recovery of funds lost, wrongly paid or incorrectly used and, **where appropriate, administrative**		their provision, or any action undertaken in response to their provision		

	ECI Directive	European Satellite Navigation systems Regulation - 1285/2013	Aspects of the deployment, operation and use of the European Global Navigation Satellite System - Council Decision 2014/496/CFSP	SST Decision - 541/2014/EU	Space programme Regulation (proposal) - COM(2018) 447 final	Copernicus Regulation – 377/2014
		and financial penalties in accordance with Regulation (EU, Euratom) No 966/2012.				
Others		The Regulation does not focus on security of the systems. Security is only a small part among other aspects.	-	Focused on the threats resulting from man-made space debris	Possible usage of components for purposes of enhancing security is described	-

8.3.4.2. Financial and banking sector

	ECI Directive	Directive on payment services (PSD2) - 2015/2366	SIPS (systemically important payment systems) Regulation - ECB/2014/28
Legal basis	Article 308 Treaty establishing the European Community (other measures)	Article 114 TFEU - common rules on competition, taxation and approximation of laws, approximation of laws	Article 127(2) TFEU - economic and monetary policy, Monetary policy
Objectives	Provide procedures for the **identification and designation of ECI**, and common approach to the assessment of the need to improve the **protection**	**Put place comprehensive rules for payment services, with the goal of making international payments (within the EU) as easy, efficient and secure as payments within a single country** (-Provide the legal foundation for the further development of a better integrated internal market for electronic payments within the EU; - Seek to open up payment markets to new entrants leading to more competition, greater choice and better prices for consumers;	

	ECI Directive	Directive on payment services (PSD2) - 2015/2366	SIPS (systemically important payment systems) Regulation - ECB/2014/28
		-Provide the necessary legal platform for the Single Euro Payments Area)	
Sectors covered by security measures	**Energy:** electricity, oil, gas **Transport**: road, rail, air, inland waterways, ocean and short-sea shipping and ports	Financial sector	Banking sector
Type of threats	All hazards approach while countering threats from terrorism as a priority	Cyber / IT risks	Risks: credit risk, collateral, liquidity risk, general business risks, custody and investment risks, **operational risks** (security-related risks are part of operational risks - Art. 15)
Operations	Threat assessment, risk analysis, risk management	Risk analysis, risk management, crisis management	Risk analysis, risk management
Definition of object to protect (e.g. CI)	**ECI**: CI located in MS the disruption of which would have significant impact on at least 2 MS [**CI:** asset, system or part thereof located in MS which is essential for the maintenance of vital societal functions, health, safety, security, economic and social well-being of people, and the disruption of which would have a *significant impact* in a MS as a result of the failure to maintain these functions]	Payment services - business activity set out in Annex I	SISP (systemically important payment systems)
Operational elements of definition	***significance of impact***: based on sectoral criteria and cross-cutting criteria: casualties, economic effects, public effects; these are defined on a case-by-case basis - JRC has elaborated non-binding guidelines (sectoral criteria are classified and details of cross-cutting criteria); JRC guidelines mention that only one cross-sectoral criterion is necessary ***protection***: all activities aimed at ensuring the functionality, continuity and integrity of CI in order to deter, mitigate and neutralise a threat, risk or vulnerability	None	Payment system shall identified as SIPS if: (a) it is eligible to be notified as a system pursuant to Directive 98/26/EC by a MS whose currency is the euro or its operator is established in the euro area, including establishment by means of a branch, through which the system is operated; and (b) at least other two criteria apply over a calendar year, related to: value of daily payments, market share, cross-border activity, settlement of other financial market infrastructures 4 have been identified in 2014

	ECI Directive	Directive on payment services (PSD2) - 2015/2366	SIPS (systemically important payment systems) Regulation - ECB/2014/28
Definition of operators /owners	**Owners/operators of ECI**: entities responsible for investment in, and/or day-to-day operation of, an ECI	**Payment service providers**: credit institutions, electronic money institutions, post office giro institutions, payment institutions, ECB and national central banks as well as MS when not acting as public or monetary authorities	**SIPS operator**: the legal entity legally responsible for operating a SIPS
Provisions on co-operation across MS/with EC	**Before the identification** of potential ECI: discussion on the thresholds of cross-cutting criteria **Before the designation** of ECI: bilateral discussion **ECIP contact point**: to coordinate ECI issues within MS, across Ms with EC	**EBA** shall promote co-operation, including the sharing of information, in the area of operational and security risks associated with payment services among the competent authorities, and between the competent authorities and the ECB and, where relevant, the European Union Agency for Network and Information Security	None
Obligations: identifications of objects to protect	**MS:** - **Identify potential ECI by applying**: sectoral criteria, definition of CI, transboundary criterion, cross-cutting criteria (whose thresholds need to be defined with second MS) - Launch of bilateral discussions for the **identification** and **designation** **- Inform the MS** involved by ECI and the operators/ owners of ECI	None	None
Obligations: setting the goals	None	None	The **Board** (administrative or supervisory board of a SIPS operator, or both, in accordance with national law) shall establish strategic aims for the SIPS
Obligations: threat assessments	**MS:** Carry out a threat assessment per subsector if they have designated an ECI	None	None
Obligations: risk analysis	**MS:** - Ensure that operators have developed an Operator Security Plan (OSP) or equivalent and renewed each year - ensure that a communication mechanism with SLO is in place	**MS:** - shall ensure payment service providers provide at least on an annual basis an updated and comprehensive assessment of the operational and security risks relating to the payment services they provide (Art. 95(2))	**SIPS operator**: shall establish comprehensive physical and information security policies that adequately identify, assess and manage all potential vulnerabilities and threats. It shall review the policies at least annually.

	ECI Directive	Directive on payment services (PSD2) - 2015/2366	SIPS (systemically important payment systems) Regulation - ECB/2014/28
	Operators /owners: - Identify important assets, carry out risk analysis based on major threat scenario, vulnerability of each asset, potential impact (in the OSP)		
Obligations: Risk management	**Operators/ owners**: identify, select and prioritise counter-measures and procedures, distinguishing between permanent and graduated security measures (in the OSP) - Establish the SLO: link between ECI owners/operators and MS authority **MS**: ensure that an OSP or equivalent is in place and Security Liaison Officers (SLO) appointed	**MS:** - shall ensure that information are provided to the payment service users on the secure procedure for notification of the payment service provider in the event of suspected or actual fraud or security threats - shall ensure that payment service providers establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks -shall ensure payment service providers provide at least on an annual basis an updated and comprehensive assessment on the adequacy of the mitigation measures and control mechanisms in response to risks - see risk assessment **Payment service providers:** - shall establish and maintain effective incident management procedures, including the detection and classification of major operational and security incidents **EBA** - guidelines for the establishment, implementation and monitoring of the security measures	**SIPS operator:** shall establish a business continuity plan that addresses events posing a significant risk of disrupting the SIPS' operations; shall establish and maintain a sound risk-management framework to comprehensively identify, measure, monitor and manage the range of risks
Obligations: Crisis management	**Operators/ owners**: Identify, crisis management measures (in the OSP)	**Payment service providers**: - shall notify the MS competent authority in case of a major operational or security incident - if impact on financial interests of users, shall inform them and provide measures	None

	ECI Directive	Directive on payment services (PSD2) - 2015/2366	SIPS (systemically important payment systems) Regulation - ECB/2014/28
		they can take to mitigate the adverse effects **MS**: - upon the notification of payment service users, shall inform EBA and ECB, and other MS, after assessing the relevance of the incident to them **EBA**: guidelines for service providers on classification of major incidents, procedures and templates, for MS on assessing the relevance of the incidents	
Reporting to EC	**MS:** - on annual basis on: the number of infrastructure per sector for which cross-cutting criteria **discussions** were held and the number of **designated ECI** per sector and number of MS dependent - every 2 years on: summary of **threat assessment** (type of risks, threats, and vulnerabilities per ECI sector)	None	None
Reporting (other than to the EC)		**Service providers**: report at least on an annual basis, statistical data on fraud relating to different means of payment to competent authorities **MS**: provide the EBA and ECB such data in an aggregated form	The **SIPS operator** shall report to competent authority (Eurosystem central bank) information to assess compliance
Sanctions			
Others		Complemented by: **EBA Guidelines on security measures for operational and security risks of payments services under the revised Payment Services Directive (PSD2)**: require that payment service providers establish a framework with appropriate mitigation measures and control mechanisms to manage operational and security risks. **EBA, Final Guidelines on major incident reporting under PSD2**: on methodology to be used by payment	

	ECI Directive	Directive on payment services (PSD2) - 2015/2366	SIPS (systemically important payment systems) Regulation - ECB/2014/28
		service providers to determine whether an operational or security incident should be considered major and hence reported to the relevant competent authority, and the format and procedures for reporting.	

8.3.4.3. Health (including water)

	ECI Directive	Cross-border threats to health Decision - 1082/2013/EU	Quality of water intended for human consumption Directive - 98/83/EC and Directive (EU) 2015/1787	Recast Quality of water Directive - COM(2017) 753 final (proposal)
Legal basis	Article 308 Treaty establishing the European Community (other measures)	Article 168(5) TFEU - TRANSITIONAL PROVISIONS, public health	Article 130, Treaty establishing the European Community and, in particular	Art. 192(1) TFEU (Union policy on environment)
Objectives	Provide procedures for the **identification and designation of ECI**, and common approach to the assessment of the need to improve the **protection**	1. Lay down rules on **epidemiological surveillance, monitoring, early warning of, and combating serious cross-border threats** to health, including preparedness and response planning related to those activities, in order to coordinate and complement national policies. 2. Support **co-operation and coordination between the MS** in order to improve the prevention and control of the spread of severe human diseases across the borders of the MS, and to combat other serious cross-border threats to health in order to contribute to a high level of public health protection in the Union. 3. Clarify the **methods of co-**	Protect human health from the adverse effects of any contamination of water intended for human consumption by ensuring that it is wholesome and clean.	Protect human health from the adverse effects of any contamination of water intended for human consumption by ensuring that it is wholesome and clean.

	ECI Directive	Cross-border threats to health Decision - 1082/2013/EU	Quality of water intended for human consumption Directive - 98/83/EC and Directive (EU) 2015/1787	Recast Quality of water Directive - COM(2017) 753 final (proposal)
		operation and coordination between the various actors at Union level		
Sectors covered by security measures	**Energy:** electricity, oil, gas **Transport**: road, rail, air, inland waterways, ocean and short-sea shipping and ports	**Health** sector	**Water supply and distribution**: water intended for human consumption	**Water supply and distribution:** water intended for human consumption
Type of threats	All hazards approach while countering threats from terrorism as a priority	- threats of biological, chemical, environmental, unknown origin - events which may constitute public health emergencies of international concern under the International Health Regulations (2005), provided that are bio or chemical threats	Adverse effects of any contamination of water intended for human consumption	Adverse effects of any contamination of water intended for human consumption
Operations	Threat assessment, risk analysis, risk management	Crisis management	Risk management, crisis management	Risk analysis, risk management, crisis management
Definition of object to protect (e.g. CI)	**ECI**: CI located in MS the disruption of which would have significant impact on at least 2 MS [**CI:** asset, system or part thereof located in MS which is essential for the maintenance of vital societal functions, health, safety, security, economic and social well-being of people, and the disruption of which would have a *significant impact* in a MS as a result of the failure to maintain these functions]	**Health** against serious cross-border threat	**Water intended for human consumption**: (a) all water either in its original state or after treatment, intended for drinking, cooking, food preparation or other domestic purposes, regardless of its origin and whether it is supplied from a distribution network, from a tanker, or in bottles or containers; (b) all water used in any food-production undertaking for the manufacture, processing, preservation or marketing of products or substances	**Water intended for human consumption**: all water either in its original state or after treatment, intended for drinking, cooking, food preparation or production, or other domestic purposes in both public and private premises, regardless of its origin and whether it is supplied from a distribution network, supplied from a tanker or, for spring waters, put in bottles

	ECI Directive	Cross-border threats to health Decision - 1082/2013/EU	Quality of water intended for human consumption Directive - 98/83/EC and Directive (EU) 2015/1787	Recast Quality of water Directive - COM(2017) 753 final (proposal)
			intended for human consumption unless the competent national authorities are satisfied that the quality of the water cannot affect the wholesomeness of the foodstuff in its finished form; **human health**	
Operational elements of definition	***significance of impact***: based on sectoral criteria and cross-cutting criteria: casualties, economic effects, public effects; these are defined on a case-by-case basis - JRC has elaborated non-binding guidelines (sectoral criteria are classified and details of cross-cutting criteria); JRC guidelines mention that only one cross-sectoral criterion is necessary ***protection***: all activities aimed at ensuring the functionality, continuity and integrity of CI in order to deter, mitigate and neutralise a threat, risk or vulnerability	serious cross-border threat: a life- threatening or otherwise serious hazard to health of biological, chemical, environmental or unknown origin which spreads or entails a significant risk of spreading across the national borders of Member States, and which may necessitate coordination at Union level in order to ensure a high level of human health protection.	None	**Priority premises:** large premises with many users potentially exposed to water-related risks, such as hospitals, healthcare institutions, buildings with a lodging facility, penal institutions and campgrounds, as identified by MS
Definition of operators /owners	**Owners/operators of ECI**: entities responsible for investment in, and/or day-to-day operation of, an ECI	None	None	**Water supplier:** an entity supplying at least 10 m3 of water intended for human consumption a day as an average; divided into small, large and very large water supply.
Provisions on co-operation across MS/with EC	**Before the identification** of potential ECI: discussion on the thresholds of cross-cutting	In the **Health Security Committee (HSC)**: MS and the EC shall consult each other with a view to	**MS:** Reporting to the EC, as described in Section Reporting	**MS:** Creating data sets and making them available to the EC, as described in Section Reporting

	ECI Directive	Cross-border threats to health Decision - 1082/2013/EU	Quality of water intended for human consumption Directive - 98/83/EC and Directive (EU) 2015/1787	Recast Quality of water Directive - COM(2017) 753 final (proposal)
	criteria **Before the designation** of ECI: bilateral discussion **ECIP contact point**: to coordinate ECI issues within MS, across Ms with EC	coordinating their efforts to develop, strengthen and maintain their capacities for the monitoring, early warning and assessment of, and response to, serious cross-border threats to health. Objectives are: best practices sharing in preparedness and response planning; promoting interoperability of national preparedness planning; addressing inter-sectoral dimension of preparedness and response planning; supporting the implementation of core capacity requirements for surveillance and response. In the **network for epidemiological surveillance of the communicable diseases** coordinated by the European Centre for Disease Prevention and Control ('ECDC'), where EC, competent authorities at MS level and ECDC are in permanent communication. in the '**Early Warning and Response System**' (EWRS), MS and the EC are in permanent communication for the purposes of alerting, assessing public health risks and determining the measures		

	ECI Directive	Cross-border threats to health Decision - 1082/2013/EU	Quality of water intended for human consumption Directive - 98/83/EC and Directive (EU) 2015/1787	Recast Quality of water Directive - COM(2017) 753 final (proposal)
		that may be required to protect public health.		
Obligations: identifications of objects to protect	**MS:** - **Identify potential ECI by applying**: sectoral criteria, definition of CI, transboundary criterion, cross-cutting criteria (whose thresholds need to be defined with second MS) - Launch of bilateral discussions for the **identification** and **designation** **- Inform the MS** involved by ECI and the operators/ owners of ECI	None	None	**MS:** - identify priority premises - identify abstraction points in the bodies of water covered by the hazard assessment - identifying people without access to water intended for human consumption and reasons for lack of access
Obligations: setting the goals	None	**MS:** draft a preparedness and response planning at national level	**MS:** - bring into force the laws, regulations and administrative provisions necessary to comply with this Directive within two years of its entry into force	**MS:** - bring into force the laws, regulations and administrative provisions necessary to comply this Directive
Obligations: threat assessments	**MS:** Carry out a threat assessment per subsector if they have designated an ECI	None	None	None
Obligations: risk analysis	**MS:** - Ensure that operators have developed an Operator Security Plan (OSP) or equivalent and renewed each year - ensure that a communication mechanism with SLO is in place	None	**MS:** - risk assessment conducted to derogate **from the parameters** and sampling frequencies and based on the general principles of risk assessment set out in relation to **international standards** such as standard EN 15975-2 concerning "security of drinking water supply,	**Water suppliers:** - at regular intervals no longer than 6 years perform a supply risk assessment providing for the possibility to adjust the monitoring frequency for any parameter that are not core parameters **MS:** - every 3 years perform a

	ECI Directive	Cross-border threats to health Decision - 1082/2013/EU	Quality of water intended for human consumption Directive - 98/83/EC and Directive (EU) 2015/1787	Recast Quality of water Directive - COM(2017) 753 final (proposal)
	Operators /owners: - Identify important assets, carry out risk analysis based on major threat scenario, vulnerability of each asset, potential impact (in the OSP)		guidelines for risk and crisis management"	hazard assessment of bodies of water used for the abstraction of water intended for human consumption - every 3 years perform a domestic distribution risk assessment, comprising the following elements: (a) an assessment of the potential risks associated with the domestic distribution systems (...) (b) regular monitoring of the parameters listed (...) (c) a verification of whether the performance of construction products in contact with water intended for human consumption is adequate (...)
Obligations: Risk management	**Operators/ owners**: identify, select and prioritise counter-measures and procedures, distinguishing between permanent and graduated security measures (in the OSP) - Establish the SLO: link between ECI owners/operators and MS authority **MS**: ensure that an OSP or equivalent is in place and Security Liaison Officers (SLO) appointed	None	**MS:** - take the measures necessary to ensure that water intended for human consumption is wholesome and clean - ensure that the measures taken to implement this Directive in no circumstances have the effect of allowing, directly or indirectly, either any deterioration of the present quality of water intended for human consumption so far as that is relevant for the protection of human health or any increase in the pollution of waters used for the production of drinking water	**MS:** - take all measures necessary to ensure that regular monitoring of the quality of water intended for human consumption is carried out, in order to check that the water available to consumers meets the requirements of this Directive

	ECI Directive	Cross-border threats to health Decision - 1082/2013/EU	Quality of water intended for human consumption Directive - 98/83/EC and Directive (EU) 2015/1787	Recast Quality of water Directive - COM(2017) 753 final (proposal)
			- take all measures necessary to ensure that no substances or materials for new installations used in the preparation or distribution of water intended for human consumption or impurities associated with such substances or materials for new installations remain in water intended for human consumption in concentrations higher than is necessary for the purpose of their use and do not, either directly or indirectly, reduce the protection of human health	
Obligations: Crisis management	**Operators/ owners**: Identify, crisis management measures (in the OSP)	**MS:** following an alert notification, shall, in liaison with the EC and on the basis of the available information from their monitoring systems, inform each other through the Early Warning and Response System (EWRS) and, if the urgency of the situation so requires, through the HSC about developments with regard to the threat concerned at national level. Info to be communicated with the alert are defined in Art. 9(3) **EC:** following a notification, make available to MS and HSC, through EWRS, a risk assessment of the potential	**MS:** - ensure that any failure to meet the parametric values set is **immediately investigated** in order to identify the cause - if human consumption does not meet the parametric values, ensure that the necessary **remedial action** is taken as soon as possible to restore its quality and shall give priority to their enforcement action	**MS:** - ensure that any failure to meet the parametric values is **immediately investigated** in order to identify the cause - if, human consumption does not meet the parametric values, ensure that the necessary **remedial action** is taken as soon as possible to restore its quality and shall give priority to their enforcement action

	ECI Directive	Cross-border threats to health Decision - 1082/2013/EU	Quality of water intended for human consumption Directive - 98/83/EC and Directive (EU) 2015/1787	Recast Quality of water Directive - COM(2017) 753 final (proposal)
		severity of the threat to public health, including possible public health measures [this is in crisis management because it follows the outbreak of the crisis/notification] **MS and EC**: coordinate national responses, and risk and crisis communication		
Reporting to EC	**MS:** - on annual basis on: the number of infrastructure per sector for which cross-cutting criteria **discussions** were held and the number of **designated ECI** per sector and number of MS dependent - every 2 years on: summary of **threat assessment** (type of risks, threats, and vulnerabilities per ECI sector)	**MS:** - every 3 years: an update on the latest situation with regard to their preparedness and response planning at national level	**MS:** - **inform** within two months of any **derogation** concerning an individual supply of water exceeding 1 000 m³ a day as an average or serving more than 5 000 persons, - **produce a report to** on the measures they have taken or plan to take to fulfil their obligations pursuant to Article 6(3) which states that the MS should advise property owners on remedial actions they could take to avoid their domestic distribution systems making the water non-compliant	**MS:** - establish data sets, to be used as to not generate reports and allow constant access to data, with their monitoring results only where they exceed the parameters in the Directive. - provide additional information such as risk assessments.
Reporting (other than to the EC)		NA	**MS:** - take the measures necessary to ensure that adequate and up-to-date information on the quality of water intended for human consumption is available to consumers - publish a report every three year on the quality of water intended for human consumption with the	**MS:** - ensure that adequate and up-to-date information on water intended for human consumption is available online to all persons supplied

	ECI Directive	Cross-border threats to health Decision - 1082/2013/EU	Quality of water intended for human consumption Directive - 98/83/EC and Directive (EU) 2015/1787	Recast Quality of water Directive - COM(2017) 753 final (proposal)
			objective of informing consumers	
Sanctions		NA	None	**MS:** - lay down the rules on penalties applicable to infringements of national provisions adopted pursuant to this Directive and take all measures necessary to ensure that they are implemented.
Others		In the event of a serious cross-border threat to health overwhelming the national response capacities, an affected MS may also request assistance from other Member States through the **Community Civil Protection Mechanism** established by Decision 2007/779/EC, Euratom		

8.3.5. Other cross-sectoral legislation

	ECI Directive	Seveso III Directive - 2012/18/EU	Union Civil Protection Mechanism-Decision No 1313/2013/EU
Legal basis	Article 308 Treaty establishing the European Community (other measures)	Article 192(1) TFEU (Union policy on environment)	Article 196 TFEU (Transitional provisions, Civil protection)
Objectives	Provide procedures for the **identification and designation of ECI**, and common approach to the assessment of the need to improve the **protection**	**Prevent major accidents which involve dangerous substances**, and the limitation of their consequences for human health and the environment, with a view to **ensuring a high level of protection throughout the Union** in a consistent and effective manner.	Strengthen the co-operation between the Union and the MS and to facilitate coordination in the field of civil protection in order to improve the effectiveness of systems for preventing, preparing for and responding to natural and man-made disasters. in particular, th**e specific objectives** are: (a) to achieve a high level of protection against disasters by preventing or

	ECI Directive	Seveso III Directive - 2012/18/EU	Union Civil Protection Mechanism- Decision No 1313/2013/EU
			reducing their potential effects, by fostering a culture of prevention and by improving co-operation between the civil protection and other relevant services; (b) to enhance preparedness at Member State and Union level to respond to disasters; (c) to facilitate rapid and efficient response in the event of disasters or imminent disasters; (d) to increase public awareness and preparedness for disasters.
Sectors covered by security measures	**Energy:** electricity, oil, gas **Transport**: road, rail, air, inland waterways, ocean and short-sea shipping and ports	All in which dangerous substances are produced, used, handled or stored, apart from certain exceptions noted in the last verse	
Type of threats	All hazards approach while countering threats from terrorism as a priority	Major accidents which involve dangerous substance	Natural and made-made disasters 'disaster': any situation which has or may have a severe impact on people, the environment, or property, including cultural heritage
Operations	Threat assessment, risk analysis, risk management	Risk analysis, risk management, crisis management	Risk analysis, risk management, crisis management
Definition of object to protect (e.g. CI)	**ECI**: CI located in MS the disruption of which would have significant impact on at least 2 MS [**CI:** asset, system or part thereof located in MS which is essential for the maintenance of vital societal functions, health, safety, security, economic and social well-being of people, and the disruption of which would have a *significant impact* in a MS as a result of the failure to maintain these functions]	Human health and the environment, not defined further in the Directive	Protection of people, but also the environment and property, including cultural heritage
Operational elements of definition	***significance of impact***: based on sectoral criteria and cross-cutting criteria: casualties, economic effects, public effects; these are defined on a case-by-case basis - JRC has elaborated non-binding guidelines (sectoral criteria	None	None

	ECI Directive	Seveso III Directive - 2012/18/EU	Union Civil Protection Mechanism- Decision No 1313/2013/EU
	are classified and details of cross-cutting criteria); JRC guidelines mention that only one cross-sectoral criterion is necessary ***protection***: all activities aimed at ensuring the functionality, continuity and integrity of CI in order to deter, mitigate and neutralise a threat, risk or vulnerability		
Definition of operators /owners	**Owners/operators of ECI**: entities responsible for investment in, and/or day-to-day operation of, an ECI	**Operator:** any natural or legal person who operates or controls an establishment or installation or, where provided for by national legislation, to whom the decisive economic or decision-making power over the technical functioning of the establishment or installation has been delegated	
Provisions on co-operation across MS/with EC	**Before the identification** of potential ECI: discussion on the thresholds of cross-cutting criteria **Before the designation** of ECI: bilateral discussion **ECIP contact point**: to coordinate ECI issues within MS, across Ms with EC	**MS and EC:** - cooperate in activities in support of implementation of this Directive, involving stakeholders as appropriate -exchange information on the experience acquired with regard to the prevention of major accidents and the limitation of their consequences	**European Emergency Response Capacity (EERC)**: consists of a voluntary pool of pre- committed response capacities of the Member States and include modules, other response capacities and experts. the EC sets the capacity goals. **MS** register on a voluntary basis the response capacity they commit to it MS in need request assistance through the Emergency Response Coordination Centre (ERCC)
Obligations: identifications of objects to protect	**MS:** - **Identify potential ECI by applying**: sectoral criteria, definition of CI, transboundary criterion, cross-cutting criteria (whose thresholds need to be defined with second MS) - Launch of bilateral discussions for the **identification** and **designation** **- Inform the MS** involved by ECI and the operators/ owners of ECI	None	None

	ECI Directive	Seveso III Directive - 2012/18/EU	Union Civil Protection Mechanism- Decision No 1313/2013/EU
Obligations: setting the goals	None	None	None
Obligations: threat assessments	**MS:** Carry out a threat assessment per subsector if they have designated an ECI	None	None
Obligations: risk analysis	**MS:** - Ensure that operators have developed an Operator Security Plan (OSP) or equivalent and renewed each year - ensure that a communication mechanism with SLO is in place **Operators /owners**: - Identify important assets, carry out risk analysis based on major threat scenario, vulnerability of each asset, potential impact (in the OSP)	**EC:** - assess, where appropriate or in any event on the basis of a notification by a MS, whether it is impossible in practice for a particular dangerous substance to cause a release of matter or energy that could create a major accident under both normal and abnormal conditions **MS:** - when it considers that a dangerous substance does not present a major-accident hazard in accordance with paragraph 1, it shall notify the EC together with supporting justification	**MS:** develop risk assessments at national or sub-national level **EC:** support MS risk assessment and other preventive actions, including best practices and information sharing, as detailed in Art. 5
Obligations: Risk management	**Operators/ owners**: identify, select and prioritise counter-measures and procedures, distinguishing between permanent and graduated security measures (in the OSP) - Establish the SLO: link between ECI owners/operators and MS authority **MS**: ensure that an OSP or equivalent is in place and Security Liaison Officers (SLO) appointed	**Operators:** - take all necessary measures to prevent major accidents and to limit their consequences for human health and the environment **MS** - organise a system of inspections.	**MS:** - develop risk management planning at national or sub-national level - participate on a voluntary basis in peer review of the assessment of risk management capability [only non-sensitive information are shared] **Preparedness:** *M*S should - on a voluntary basis - develop modules, identify response capacities and experts which could be available for the intervention through the Union Mechanism **MS and EC:** through scenario-building for disaster response, asset mapping and the development of plans for the deployment of response capacities

	ECI Directive	Seveso III Directive - 2012/18/EU	Union Civil Protection Mechanism- Decision No 1313/2013/EU
			EC: manage the Emergency Response Coordination Centre - see Art. 8 for details
Obligations: Crisis management	**Operators/ owners**: Identify, crisis management measures (in the OSP)	**MS:** **-** draw up an external emergency plan for the measures to be taken outside the establishment within two years following receipt of the necessary information from the operator pursuant to point (b) **Operators:** - draw up the internal emergency plans for the measures to be taken inside the establishment, supply the necessary information to the competent authority	**MS** - notify the EC in the event of a disaster within the Union, or of an imminent disaster, which causes or is capable of causing trans-boundary effects or affects or is capable of affecting another MS - the MS in which the disaster occurs or is likely to occur shall, without delay, notify the potentially affected Member States and, where the effects are potentially significant, the Commission - shall notify the EC of a possible request for assistance through ERCC **EC:** - inform other MS of a possible request for assistance Response is further detailed in Chapter IV
Reporting to EC	**MS:** - on annual basis on: the number of infrastructure per sector for which cross-cutting criteria **discussions** were held and the number of **designated ECI** per sector and number of MS dependent - every 2 years on: summary of **threat assessment** (type of risks, threats, and vulnerabilities per ECI sector)	**MS:** - inform the EC of **major accidents** meeting the criteria of Annex VI which have occurred **within their territory** for the purpose of **prevention and mitigation** of major accidents	**MS:** - every three years: risk management capability - inform the EC about experts, modules and other response capacities that they make available for assistance, and update this information
Reporting (other than to the EC)		None	None
Sanctions		**MS:** - determine penalties applicable to infringements of the national provisions adopted pursuant to this Directive	None

	ECI Directive	Seveso III Directive - 2012/18/EU	Union Civil Protection Mechanism- Decision No 1313/2013/EU
Others			Preamble (6): The Union Mechanism should take due account of relevant Union law and international commitments, and exploit synergies with relevant Union initiatives, such as the European Earth Observation Programme (Copernicus), the European Programme for Critical Infrastructure Protection (EPCIP) and the Common Information Sharing Environment (CISE). The EC carry out training, exercises, lessons learnt and knowledge dissemination - Art. 13

8.4. Analysis of key aspects of international initiatives in the context of CIP

UN

The scope of Resolution *2341* is boarder that the Directive and covers prevention, protection, mitigation, investigation, response to and recovery from attacks, and the actions that MS are called to implement span from raising awareness, considering the development national strategies, exchanging relevant information, and establishing partnerships with public and private stakeholders. In addition to that Resolution, a "Compendium of good practices" was compiled by the UN Counter-Terrorism Centre and the Counter-Terrorism Committee Executive Directorate, which presents additional case studies as examples related to the topics covered by the Resolution

OECD

The *Recommendation on the* ***Governance of Critical Risks*** recommends that MS:

- establish and promote a comprehensive, all-hazards and **transboundary approach** to country risk governance to serve as the foundation for enhancing national resilience and responsiveness;
- build **preparedness** through foresight analysis, risk assessments and financing frameworks, to better anticipate complex and wide-ranging impact;
- raise **awareness** of critical risks to mobilise households, businesses and international stakeholders and foster investment in risk prevention and mitigation;
- develop adaptive capacity in **crisis management** by coordinating resources across government, its agencies and broader networks to support timely decision-making, communication and emergency responses; and,
- demonstrate **transparency and accountability** in risk-related decision making by incorporating good governance practices and continuously learning from experience and science.

Unlike the ECI Directive, this Recommendation does not define a specific object to protect but adopts a more general approach. CI and transboundary effects of risks are however part of this general approach. Like the ECI Directive, the Recommendation addresses all types of hazards and underlines the role of the private sector and operators. It complements the Directive in recommending the development of national strategies and in focusing on preparedness and resilience, including **crisis management** actions. As for **risk analysis** and **risk management**, the Directive and the Recommendation overlap, and, provided their different legal status, both focus on the need of MS to ensure operators have in place risk prevention measures, including business continuity plans.

The objective of the ***Recommendation on Digital Security Risk Management for economic and social prosperity*** is to ensure an adoption of a digital security risk management approach by the highest level of leadership in government, public and private organisations in all OECD countries. It concerns the protection from all threats affecting the confidentiality, integrity and availability of digital environment or the actions relying on the digital environment. The document does not define how the objects to protect are to be identified but there may be an overlap with the ECI Directive, as some of the actions relying on the digital environment are necessary for the critical infrastructure to function correctly. Unlike the ECI Directive, the Recommendation does not cover the **threat assessment**, which is implied but not explicitly mentioned in the OECD document. A reverse situation exists in case of **crisis management**, as the Recommendation requires that all stakeholders adopt preparedness and continuity plans – while no similar measures are required by the ECI Directive. In the aspects of **risk analysis** and **risk management** there is an overlap, as both the ECI Directive and the Recommendation require that the appropriate stakeholders manage the risk based on cyclic risk analysis.

The 2008 ***Recommendation on the Protection of Critical Information Infrastructures*** is a similar source of duplications in regard to information systems being used by the critical infrastructure. Its objective is introducing and maintaining an effective framework to protect CII from all possible hazards that could cause a disruption or destruction of such infrastructure. The document defines the CII as interconnected information systems and networks, the disruption

or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy. This definition makes it very similar to the NIS Directive in terms of protected objects. Additionally, according to both the ECI Directive and the Recommendation, the MS identify the critical infrastructure and assess the threats and risk. The **risk management** is also overlapping, as the Regulation calls on MS to develop their own requirements for operators in this aspect, like the ECI Directive.

Transport-specific initiatives

The UN Economic Commission for Europe - UNECE has set up the Multidisciplinary Group of Experts on Inland Transport Security. They do not create any documents with regulations or recommendations but they do conduct regular workshops and host discussion forums, whose results are directly related to the security in transport, including CI. UN Agencies are also active in security. Annex XVII of the Chicago Convention on International Civil Aviation by the International Civil Aviation Organization (ICAO) is specifically on security. On the basis of this, the UN Security Council published the Resolution 2309 (2016) calling for enhancing screening, security checks and facility security. Similarly, the International Convention for the Safety of Life at Sea (SOLAS) by the International Maritime Organization (IMO) contains specific security measures (the International Ship and Port Facility Security (ISPS) Code).

Outside the UN, the **International Union of Railways** (UIC) took two main initiatives on the topic of security: the "Guidelines for Cyber-Security in Railways", which focuses on cybersecurity and is based on the ISO27001 standard, and the "Station security for station business - Handbook on effective solutions", which provides detailed and specific recommendations to enhance security.

Energy-specific initiatives

The Industrial Resources and Communication Services Group, part of the **NATO** Civil Emergency Planning Committee, in 2017 drafted the document *Recommendations and best practices on the protection of electricity, gas and oil critical infrastructure* which designs best practices "to support national policy makers and relevant authorities in their efforts to review their national sectoral arrangements"[168] and stresses the importance of resilience. Moreover, NATO also produces also studies, like the *Guidance on improving resilience of national and cross-border energy networks* which discusses the vulnerabilities in the energy supply networks and the security implications of digitalisation of the energy industry and provides specific recommendations. Another 2018 study titled *Recommendations on the importance of critical energy infrastructure (CEI) stakeholder engagement, coordination and understanding of responsibilities* stresses the importance of risk management practices and public-private partnerships.

OSCE is also relevant in CIP in the energy sector. *The Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace* is a document focused resilience against on cyber-threats to energy infrastructures. It contains recommendations on threat analysis, risk assessment and risk management based on ISO/IEC 27000 series of standards and US National Institute of Standards and Technology (NIST) documents. *Protecting Electricity Networks from Natural Hazards* is a handbook strongly focused on crisis management against natural hazards.

The International Energy Agency (IEA) has many publications containing case studies and predictions regarding energy security. These are particularly focused on the security of supply and using resilience-based measures, rather than on CI.

ISO

[168] 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.

Standard	Brief description of the content	Covered categories	Sector	Coherence with the ECI Directive
ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements	Specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of an organisation. This standard also includes requirements for the assessment and treatment of information security risks. It is applicable to all types and sizes of organisations.	Risk assessment, risk management	Cross-sector	Security requirements provided by the ISO standard are quite generic as they can be applied by all organisations regardless of their type, size and nature. Its objective is to establish and implement an information security management system that preserves the confidentiality, integrity and availability of information. It is coherent with the ECI Directive by providing more precise guidelines as to how risk assessment and management should be conducted in case of the Information Technology/Operational Technology systems that are a part of CI.
ISO/IEC 27019:2017 Information technology — Security techniques — Information security controls for the energy utility industry	Provides guiding principles based on ISO/IEC 27002:2013 "Code of practice for information security controls" for information security management applied to process control systems as used in the energy utility industry. It provides guidelines for controlling and monitoring the production or generation, transmission, storage and distribution of electric power, gas, oil and heat, and for the control of associated supporting processes.	Risk assessment, risk management	Energy utility industry	This standard provides detailed information regarding necessary security measures and controls for process control systems of the energy utility industry, their supporting systems and the associated infrastructure. It is coherent with the ECI Directive, overlapping in scope but providing a more drilled down perspective on the processes of risk assessment and management.
ISO 22301:2012 Societal security — Business continuity management systems – Requirements	Specifies requirements for setting up and managing an effective Business Continuity Management System, in particular, to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise. To do so, the standard applies the "Plan-Do-Check-Act" (PDCA) model. The standard is	Risk analysis, risk management	Cross-sector	As the ECI directive, the ISO 22301 standard covers aspects of risk assessment and risk management to ensure protection against incidents. The ISO standard however provides the requirements from the business continuity perspective and targets a broader audience, as it can be applied to every organization.

Standard	Brief description of the content	Covered categories	Sector	Coherence with the ECI Directive
	applicable to all types and sizes of organisations.			
ISO 31000:2018 Risk management — Guidelines	Provides guidelines on managing risk faced by organisations. It provides a common approach to managing any type of risk by organisations regardless of industry or sector.	Risk management	Cross-sector	This standard is focused on the risk management area to assist organisations in setting strategy, achieving objectives and making informed decisions. The guidelines included in the document are generic and can be applied to all types of risks by every organisation.
ISO 14001:2015 Environmental management systems — Requirements with guidance for use	Specifies a framework for organisations to protect the environment and respond to changing environmental conditions in balance with socio-economic needs. It specifies requirements that enable an organisation to achieve the intended outcomes it sets for its environmental management system. The approach underlying an environmental management system presented in the document is based on the concept of Plan-Do-Check-Act (PDCA).	Risk management	Cross-sector	Although specifying terrorism as a priority in terms of threats, the ECI directive adopts an all-hazard approach that includes natural disasters. Also, the cross-cutting criteria for ECI specified by the Directive comprise potential environmental effects. In this respect, the ISO standard complements the ECI Directive focusing, among others, on the issues of protecting the environment by preventing or mitigating adverse environmental impacts as well as on mitigating the potential adverse effect of environmental conditions on the organisation.

8.5. Analysis EU CIP legislation besides energy and transport

Space sector

In the space sector, legislation is in general more developed and imposes stricter requirements than the ECI Directive.[169] There is however room for misalignment, especially on the Galileo ground component.

Galileo is a particularly important infrastructure, being the European Global Navigation Satellite Systems (GNSS). It is both an EU-owned CI to protect and a tool that can be used to enhance security of other CI (e.g. on synchronisation). The Galileo Regulation introduces the concept of "security accreditation"[170] applied to all global navigation satellite system (GNSS) and undertook by the European GNSS Agency (GSA). The security accreditation applies to all components of Galileo and aims at ensuring that they are secure.

[169] Interview: 2 EC DGs and agencies.

[170] Regulation (EU) No 1285/2013 of the European Parliament and of the Council of 11 December 2013 on the implementation and exploitation of European satellite navigation systems and repealing Council Regulation (EC) No 876/2002 and Regulation (EC) No 683/2008 of the European Parliament and of the Council, Article 14.

Specifically, on the protection of Galileo *ground component*, [171] the Galileo Regulation[172] sees the Directive as the minimum standard to which MS should comply for its protection and requires them to adopt measures of protection that "shall be at least equivalent to those required for the protection of ECI". This cross-reference between the two legal texts highlighted a gap: Galileo ground component might not be considered a CI in all MS.

By requiring MS to adopt protection measures equivalent to those applied to ECI, the Galileo Regulation assumed that in all MS ground components were considered as NCI. This is indeed the precondition for MS to apply measures included in the ECI Directive as ECI are *in primis* NCI. However, as shown in the implementation state of play, MS adopted different interpretations of CI that not necessarily bring to the qualification of Galileo ground component as a NCI. This limits the application of the provision of the Galileo Regulation.[173]

The new proposed Regulation on the Space Programme keeps the reference to the ECI Directive, and adds the reference to the measures in place for national CI, so that MS will need to make sure that the ground infrastructure is protected at least to the same level as ECI and national CI. It is thus expected that in some cases the national framework would need to be adjusted (e.g. in the definitions or criteria) to include the Galileo ground component. This will likely increase the coherence of the EU and national CIP framework.

On the use of Galileo instead of GPS to enhance security of other CI, currently there are no relevant provisions and this is an unexploited synergy.[174]

The proposed Space Programme Regulation will introduce requirements on risk and threat analysis also on national space infrastructures (outside Galileo) as well as specific security requirements.[175] Currently, national space infrastructures are regulated at the national level only[176] and since the proposed Regulation is expected to introduce changes at the national level, this is also expected to impact on the overall coherence of the EU and national CIP framework.

Financial sector

In the financial sector, CI are generally defined as CII (hence referring to ICT systems and networks[177] rather than assets or physical components), and to ensure their security cyber security measures have been extensively developed[178] as it is a sector particularly sensitive to cyber-attacks.[179] **Measures to protection CI in the financial sector seem to run in parallel with the ECI Directive, as there is no evidence of synergy at the EU level**. In particular, the Directive is considered too general to be useful, lacking important elements, like benchmarking and recovery, and too much linked to MS, while the financial sector serves the EU as a whole.[180]

Health sector

[171] Galileo ground components include: Galileo Control Centres (GCC) are based in Germany and Italy. European GNSS Agency offices are located in Czechia and France. The European GNSS Service Centre is located in Spain. The Galileo Reference Centre (GRC) is located in the Netherlands The Galileo Security Monitoring Centre is based in France and United Kingdom (however currently relocated to Spain – Available at: https://www.gsa.europa.eu/newsroom/news/european-space-community-steps-security-and-defence).

[172] Regulation (EU) No 1285/2013 of the European Parliament and of the Council of 11 December 2013 on the implementation and exploitation of European satellite navigation systems and repealing Council Regulation (EC) No 876/2002 and Regulation (EC) No 683/2008 of the European Parliament and of the Council, Article 28.

[173] Interview: 1 EC DGs and Agencies.

[174] Interview: 1 EC DGs and Agencies.

[175] Interview: 2 from EC DGs and Agencies. Proposal for a Regulation establishing the Space Programme, Article 34.

[176] Interview: 1 EC DGs and Agencies.

[177] Angori, E., Baldoni, R., Dekel, E., Dingsor, A., & Lucchetti, M. (2012). The Financial Critical Infrastructure and the Value of Information Sharing. Springer, Berlin, Heidelberg.

[178] See for instance Financial Stability Board (2017), Stocktake of publicly released cybersecurity regulations, guidance and supervisory practices, from pg. 66. Relevant instruments containing security-related measures are: Prudential Requirements for Credit Institutions and Investment Firms (CRR) Regulation - 575/201; Directive on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms (CRD IV) Directive 2013/36/EU; Directive on payment services (PSD2) Directive (EU) 2015/2366; SIPS Regulation (ECB/2014/28); Insurance companies Directive 2009/138/EC; Credit rating agencies Regulation (EU) No 462/2013; Central Securities Depositories (CSD) Regulation (EU) No 909/2014; Markets in Financial Instruments Directive (MiFID II) - 2015/2366; Markets in Financial Instruments Regulation (MiFIR) - 600/2014.

[179] Interview: 1 EC DGs and agencies.

[180] Interview: 1 EC DGs and Agencies, specifically tasked in security in the financial sector.

In the heath sector, EU provisions[181] exist to coordinate response in case of cross-border threat to human health and protect human health from the adverse effects of any contamination of water intended for human consumption.[182] In the case of **cross-border threats**, these are **complementary to the ECI Directive, as they focus mainly on crisis management activities and resilience/preparedness, which are not the core of the ECI Directive**. In this context, the aim to protect CI is only indirect insofar as a CI is relevant to business continuity.[183] In the case of **water contamination**, legislation contains **risk and crisis management requirements that could potentially work in synergy with the Directive**. There is however no evidence of synergies at the EU level between the Directive and activities in the health sector.

Cross-sector

As for cross-sectoral EU legislation, the **Seveso III Directive**[184] aims to prevent major accidents involving dangerous substances, and to limit the consequences for human health and the environment. While overall it is complementary to the ECI Directive, **ECI operators** controlling establishment or installations where dangerous substance is used[185] **may be also subject to risk management requirements deriving from the ECI Directive, therefore creating overlap and potential duplication**.[186] There are no evidence of synergies between the Seveso III and the ECI Directive at the EU level.

Finally, the **civil protection mechanism**[187] focuses on the protection of people and the environment in case of a disaster rather than on the CI itself. It includes risk analysis, risk management and crisis management practices, as well as a system of co-operation between MS (e.g. training, peer reviews). There are potential synergies with the ECI Directive as some activities under the civil protection mechanism concern also are common to CIP, e.g. risk assessment and risk management, the civil protection mechanism relies on the very functioning of CI to deliver response.[188] However, **there is no evidence of such synergies at the EU level, and the limited scope of the Directive as well as its protection-centred approach (as opposed to resilience) is considered to limit the room for synergy**.[189]

[181] Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC.
[182] Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption; Commission Directive (EU) 2015/1787 of 6 October 2015 amending Annexes II and III to Council Directive 98/83/EC on the quality of water intended for human consumption; Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the quality of water intended for human consumption (recast) COM/2017/0753 final.
[183] Interview1 EC DGs and Agencies.
[184] Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC.
[185] 'Dangerous substance' is defined as a substance or mixture covered by Part 1 or listed in Part 2 of Annex I of the Seveso III Directive, including in the form of a raw material, product, by- product, residue or intermediate, as per Article 3(19) of Seveso III directive.
[186] Survey: 2 PoCs in open-ended answers mentioned Seveso III as an EU instrument which duplicates some elements of the Directive and 2 CI operators in open-ended answers mentioned Seveso III as one of the factors external to the Directive that contributes to CIP.
[187] Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism.
[188] Interview: 1 EC DGs and Agencies.
[189] Interview: 1EC DGs and agencies, specifically involved in the civil protection mechanism.

9. EVIDENCE SUPPORTING THE ANALYSIS OF THE EFFECTIVENESS

9.1. Contribution of the Directive provisions in achieving the objective of establishing a procedure for the identification and designation of ECI

Provisions of the Directive	Assessment of the contribution	Rationale for the assessment
Scope	Effective	No relevant differences emerged across MS in terms of coverage of the energy and transport sectors, as all MS implemented the Directive in the relevant sectors and sub-sectors, with exceptions due to the specific morphology of the territory.
Definitions	Partially effective	The definition of CI in the Directive has represented for approximately half MS[190] the first step for the development of a CIP framework, hence contributing towards the establishment of a procedure for the identification and designation of ECI.[191] Other definitions in the Directive can be assumed to have contributed to this, for instance the definition of ECI, protection and risk analysis. However, **definitions are often vague**, **giving ample room for interpretation at national level, and hence limiting the extent to which a truly common procedure for the identification and designation of ECI was established**. Specifically, as highlighted implementation state of play, some MS have adapted the definition of CI focused on services, while others on assets, and this may impact the ability of MS to agree on the nature of CI, negatively affecting the identification and designation process.[192] When applying the definition of CI to initiate the process for the identification of ECI, most MS started from their definition and national list of CI, on top of which added the transboundary criterion.[193] As a consequence, if a CI was not already considered critical at the national level, it would have not been taken into consideration for the starting the identification process,[194] thus limiting the effectiveness of the procedure to identify ECI.
Identification process	Partially effective	All MS are aligned in their legislation on the procedural steps, as outlined in the Annex III to the Directive. As for the implementation of the procedures, **almost all MS *initiated* the identification process**,[195] **and this can be considered as a positive effect of the Directive**. The identification process includes the discussion with other MS on

[190] In 12 MS (AT, BG, EE, ES, HR, IT, LU, MT, PL, RO, SI, SK) the Directive introduced the definition of CI in the national CIP framework.
[191] MS did not have a definition of CI before the introduction of the Directive, see the baseline.
[192] Case study: 1 MS.
[193] Workshop: break-out gas pipeline.
[194] 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".
[195] Survey: 96% (N=23) of PoCs answered that the MS they represented did started the identification process.

Provisions of the Directive	Assessment of the contribution	Rationale for the assessment
		cross-cutting criteria, and only a limited number of MS reached this step.[196] Overall, the results of the identification were for the most part of CI negative.[197] If, on the one hand, this result can be partially imputed to the failure of the specific CI to meet the thresholds for the identification; on the other hand, specific difficulties have emerged, pointing at **the application of the transboundary element and reaching an agreement with other MS**[198] **as the main difficulties**, limiting the effectiveness of the identification process. In particular, difficulties concern: • The *difference in the definitions*, as highlighted above. • The *loose interpretation of some elements of the definitions*, as for instance the interpretation of 'alternatives' whose existence should be taken into account in identifying ECI, and that some MS have adopted in a very wide sense (especially in the transport sector).[199] • The *difference in the perception of risks* associated to a particular CI,[200] which may result in different *definitions across MS of the sectoral and cross-sectoral criteria*, as well as in *different thresholds* that the effects of a disruption/destruction should meet for the infrastructure to be considered critical.[201] While the JRC has produced guidelines[202] that could support a common interpretation of the Directive, these *were non-binding and not enough detailed*,[203] thus leaving to MS the decision on whether to use them, as well as to further detail them (e.g. on the methodology to calculate the thresholds or to perform threat analysis), possibly leading to diverging approaches and reducing the harmonisation of the identification process across MS.[204]

[196] Survey: 74% (N=17) of PoCs declaring that their MS started the identification process reported that this was concluded with the identification of an ECI in no or less than half cases.
[197] Survey: in most cases (74%), the identification was not concluded or concluded only for fewer than half ECI.
[198] Survey: 61% (N=11) and 59% (N=10) of PoCs respectively considered that the application of the transboundary criteria and reaching an agreement with other MS on the designation were an element of difficulty to a moderate to a very high extent; 73% (N=8) and 90% (N=9) of other ministries considered them as elements of difficulty from not at all to a low extent.
[199] Case study: 1 MS; Survey: open-ended answers of 3 PoCs; Workshop: PoCs.
[200] Workshop: PoCs.
[201] In most MS criteria and thresholds are not publicly available, but when information has been found, these differ, as highlighted in the implementation state of play.
[202] Bouchon, S., Di Mauro, C., Logtmeijer, C., Nordvik, J. P., Pride, R., Schupp, B., & Thornton, M. (2018). 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. JRC.
[203] 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".
[204] The JRC Guidelines were not considered useful and too complicated and some countries developed their own guidelines (2 case studies, interview with 1 PoC). MS were split in the consideration of the extent to which the increase of co-operation between MS was due to common procedures, as 45% (N=8) of PoCs considered that this was due to the common procedure to a high/very high extent, and 30% (N=7) that this was due to common procedures to no or low extent. Similarly, PoCs are split on the effectiveness of common guidelines in increasing co-operation, with 30% (N=6) PoCs stating that these were not or to a limited extent effective, and 35% (N=7) stating that these were effective to high or very high extent.

Provisions of the Directive	Assessment of the contribution	Rationale for the assessment
		• *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 the identification of an ECI.[205] According to this principle, the level of the information sharing will be balanced and proportional to the feedback received by the counterpart. Of course, this may cause poor results when one MS receives low balanced feedback or encounters difficulties in sharing a common vision of the cross-cutting criteria.[206] Other MS, regardless of the reciprocity, may be reluctant to follow the EU identification procedures, preferring inter-governmental approaches, which may also lead to stricter protection requirements.[207] • The *difference in capabilities across MS*, in terms of human resources allocated to CIP. This creates unbalance in the discussion on identification and designation, potentially leading some MS with strong capabilities and that have to discuss with MS with limited capabilities to not see significant added value from the co-operation pursue a national-only approach, and to pursue a national-only approach to speed up the procedures. • The *definition of roles and responsibilities that does not reflect the stakes that MS have in the identification and designation process*. The identification process starts from MS 1, where the CI is located, and there is little room for MS 2 to initiate the identification process.[208] However, the relevant CI in MS 1 is in most cases already a NCI, and, being the level of protection of ECI and NCI almost the same,[209] the added value of initiating the designation procedure appears to be limited to MS 1. Given these difficulties, the low success rate[210] of the identification process can be taken as a proxy of the variety of approaches that persist at the MS level, and hence as an indication of the limited effectiveness of the Directive in introducing a common framework.
Designation process	Effective – with a caveat	All MS are aligned in their legislation on the procedural steps of the designation outlined in the Annex III to the Directive, although the procedure tends to be poorly formalised. The designation process depends on the outcome of the identification process. Given the negative results in the identification, not surprisingly fewer MS entered in bi/multi-lateral discussions for the designation with other MS, then they entered into discussion on cross-cutting criteria during the identification step. The results of such discussions, however, seem to be slightly more positive than the results of the identification, as in almost half of such cases, the

[205] Such as Spain, which encoded the principle in its transposition measures; case study: 1 MS.
[206] Lazari, A. (2014). European Critical Infrastructure Protection. Springer.
[207] Case study: 1 MS.
[208] Few MS, like France, proactively conduct national risk assessments to identify potential ECI abroad. According to Article 4(2) of the Directive, "a MS that has reason to believe that it may be significantly affected by the potential ECI, but has not been identified as such by the Member State on whose territory the potential ECI is located, may inform the EC about its wish to be engaged in bilateral and/or multilateral discussions on this issue". The EC does not keep record of this, and it does not seem a common practice among MS, as confirmed by the survey (88% (N=15) of PoCs answered that they have never informed the EC on potential ECI in another MS). Three interviews with a representative of DGs have confirmed that the process relies very much on initiative of the MS where the potential ECI is located, excluding EU-wide considerations.
[209] Workshop: PoC, CI owners/operators; Case study: 2 MS.
[210] Survey: 78% (N=18) of PoCs answered that the identification process led to no or less than half CI designated as ECI.

Provisions of the Directive	Assessment of the contribution	Rationale for the assessment
		discussion with other MS ended up with the designation of *all*, *most, or half* of identified ECI.[211] It seems therefore that the designation is slightly less problematic than the identification, and no specific issues have been identified on this. However, a **caveat** should be highlighted: the Directive does not specify how such bilateral/multilateral discussions on the designation should take place, nor the specific content, and MS have been reluctant to share specific details on this, pertaining to traditionally sensitive issues, such as security and diplomacy. As a consequence, it is not possible to have a clear picture on how this step contributes to the final decision on the designation (whether for instance it represents a substantial additional passage, or rather it consists in the ratification of the outcomes of the identification) and on difficulties of the discussion MS encountered.
CIP PoCs	Effective	All MS have appointed a PoC that coordinates ECI protection issues within the MS, with other MS and with the EC and PoCs share a general very positive view on their role.[212] While, the figure of the CIP PoC was already introduced within the EPCIP (see implementation state of play), the Directive provided a stronger legal basis for its role.

9.2. Contribution of the Directive provisions in achieving the objective of establishing a common approach to the assessment of the need to improve the protection of ECI

Provisions of the Directive	Assessment on the contribution	Rationale for the assessment
OSP	Partially effective	While all MS have the OSP obligation in place, there are **differences in terms of methodologies used and specific content**. This is because Annex III to the Directive is described in general terms, the JRC Risk Assessment methodologies are non-binding and constitute one of the multiple references operators may use, including ISO standards.[213] Moreover, they are considered complicated by some MS, which drafted national guidelines.[214] This weakens the extent to which the OSP constitutes an element of a common approach.
SLO	Partially effective	The Directive does not clearly define the figure of the SLO, leaving ample margin on discretion to MS. While all MS have the SLO obligation in place, **these figures vary in terms of competences, roles and background**.[215] Since the SLO is the primary responsible for implementing a common approach to the assessment of risks at the

[211] Survey: 35% (N=6) of PoCs.
[212] Workshop: PoCs.
[213] Workshop: CI owners/operators.
[214] Case study: 1 MS.
[215] European Commission, (2014), Security Liaison Officer Project Final Report, June.

Provisions of the Directive	Assessment on the contribution	Rationale for the assessment
		operational level, such variety is likely to reflect in different implementation approaches, thus undermining the capacity of such figure to deliver a common approach, as per the objective of the Directive.
Reporting	Partially effective	Reporting refers to the obligations of MS to submit a summary of the threat assessment (basic generic data on the types of risks, threats and vulnerabilities) per ECI sector every two years to the EC. All MS with an ECI submitted reports with these data to the EC.[216] The contribution of the reporting to achieving a common approach is however limited. Although the EC and MS have developed a common template, its structure is general and leaves room for different level of details in the information reported. Moreover, the extent to which such reports could be used by the EC to "assess on a sectoral basis whether further protection measures at Community level should be considered for ECI" is also limited. The EC, receiving these reports is well-placed to feeding back MS with a broader perspective on threats and generating a common situational picture. However, there has been no feedback by the EC on MS threat assessment nor the EC acted as collector making the synthesis of national situational pictures into a pan-EU one; rather, such reports have been mainly used by the EC for checking compliance.[217] The reason is that MS reported only limited and difficult to compare information (mainly on which sector was considered as particularly critical), due to their reluctance to share security-related information through open channels as well as the generality of the common template.[218] This leaves an unexploited potential for the reporting, especially in the sense that this may be used by the EC to provide specific support and a comprehensive situational awareness (see below).
EC support	Mostly effective	The EC support consists in making available "best practices and methodologies as well as support training and the exchange of information on new technical developments related to critical infrastructure protection".[219] The JRC has developed guidelines for the implementation of the Directive[220] and methodologies for risk assessment,[221] as well as has organised several workshops on the implementation of the Directive.[222] The CIP PoC meetings have been regularly organised in Brussels by DG HOME. Not strictly linked to the Directive, the EC has developed the CWIN platform, where MS authorities, CI owners/operators and EC representatives could share good practices and methodologies.[223] Moreover, there is evidence on a mainly informal role of DG HOME in providing ad hoc support to MS.[224]

[216] Feedback from DG HOME.
[217] Interview: 2 EC DGs and Agencies.
[218] Interview: 1 EC DGs and agencies.
[219] ECI Directive, Article 8.
[220] Bouchon, S., Di Mauro, C., Logtmeijer, C., Nordvik, J. P., Pride, R., Schupp, B., & Thornton, M. (2018). 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. JRC.
[221] Theocharidou, M., & Giannopoulos, G. (2015). Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. Publications Office of the European Union, Luxembourg.
[222] Giannopoulos, G., & Schimmer, M. (2011). Memorandum on the results of the sixth Workshop on the Implementation and Application of the Directive. JRC.
[223] Review EPCIP
[224] Case study: 1 MS.

Provisions of the Directive	Assessment on the contribution	Rationale for the assessment
		Guidelines, although considered too general by some MS to implement the Directive and to be used as a basis for co-operation (see 'identification process' in previous table) proved to be particularly useful in increasing the level of protection of CI by half of the PoCs, although to a less extent by other ministries and CI operators, who tend to be the ultimate beneficiaries.[225] Operators are also split on the effectiveness of training, access to best practices and exchange of information activities by the EC.[226]The fact that the EC support is more positively seen by PoCs rather than by other ministries and operators may be indicative of a gap in the national uptake and dissemination of these measures at the national level. CIP PoCs meetings, have also been useful to exchange information and sharing good practices, and there is general agreement among MS of their positive effects.[227]

[225] Survey: to a high and to a very high extent for 50% (N=6) of PoCs, 33% (N=3) of other authorities and 37% (N=12) of operators.
[226] Survey: the extent to which, according to operators, these provisions improve the protection of CI (high and very high extent) is 33% (N=12) for best practices and methodologies, 25% (N=9) for training and 34% (N=12) for exchange of information.
[227] Workshop: PoCs.

10. EVIDENCE SUPPORTING THE ANALYSIS OF THE EFFICIENCY

10.1. Main costs and related obligations sustained by stakeholders in relation to Directive 2008/114

Relevant stakeholder	Type of cost	Specific obligation	Recurring cost	Occurring only if ECI is designated	Incidence[228] of costs
MS authorities	Compliance cost	Appointment of a CIP PoC, and setting up and managing the appropriate communication mechanisms to support this function (art. 10)	No	No	**Low incidence** Part of MS already identified a CIP PoC as requested by the 2005 Green Paper and the 2006 Communication.[229] According to the press release accompanying the 2006 Communication, at that time two informal CIP PoCs meetings had already took place.[230] However, evidence available does not allow to estimate the exact number of MS having a PoC. Moreover, while these were non-binding documents, the Directive introduced the binding requirement for all MS.
MS authorities	Compliance cost	Identification of ECI using the sectoral, trans-boundary and cross-cutting criteria set out in the Directive (art. 3)	Yes	No	**Medium incidence** 9 MS already had measures to identify and protect CI before 2008, as reported in the baseline. Even though the exact content of those measures is not known, it can be assumed that they hardly included the consideration of the transboundary element when assessing the impact of the disruption of CI, as the protection of CI is traditionally a national competence.
MS authorities	Administrative costs	Discussions with other MS on relevant thresholds for cross-cutting criteria, and informing the EC concerning the number of	Yes	No	**Medium incidence** Co-operation between MS for CIP already existed in 8 MS, as reported in the baseline, offering a channel for these discussions.

[228] Incidence is defined here in terms of number of MS that could be potentially concerned by a specific obligation introduced by the Directive. The incidence is high insofar as the requirement is new and no too few MS adopted equivalent measure before 2008. The incidence is low when several to all MS already had similar measures before 2008.
[229] European Commission. (2005). Green Paper on a European Programme for Critical Infrastructure Protection. COM(2005) 576 final, Brussels. European Commission. (2006). 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. COM(2006) 787 final, Brussels SEC(2006) 1648.
[230] European Commission. (2006b). Communication from the Commission on a European Programme for Critical Infrastructure Protection. COM(2006) 786 final , Brussels.

Relevant stakeholder	Type of cost	Specific obligation	Recurring cost	Occurring only if ECI is designated	Incidence[228] of costs
		infrastructures per sector for which discussions were held concerning the cross-cutting criteria thresholds (art. 3)			The Directive codified to some extent the discussion on cross-cutting criteria and this could have therefore generated new adjustment costs. The reporting of information to the EC generated new costs for all MS.
MS authorities	Administrative costs	Designation of ECI (art 4), including: - bilateral and multilateral discussions concerning the potential designation of ECI - informing the EC concerning completed ECI designations and the affected MS	Yes	Partially (only informing the EC)	
MS authorities	Enforcement cost	Verification of the existence of Operator Security Plans (OSP) or equivalent and Security Liaison Officers (SLO) (art. 5 and 6)	Yes	Yes	**Medium incidence** Most of the MS (25) already had a requirement for an OSP, and a SLO (20) as reported in the baseline, however whether MS authorities verified or not the compliance to this requirement is unknown. In 12 MS there was co-operation between the national authorities and the operators[231] and it might be assumed that this included some forms of control. However, the cost of controlling the existence of the OSP and the SLO is among the most frequently mentioned costs by PoCs.[232]
MS authorities	Administrative costs	Carrying out a threat assessment within 1 year after each ECI designation (art. 7)	Yes	Yes	**Medium incidence** Threat assessment was performed before the Directive in 11 MS, as reported in the baseline.
MS authorities	Administrative costs	Reporting generic data on the types of risks, threats and vulnerabilities per ECI sector to the EC every 2 years (art. 7)	Yes	Yes	**High incidence** As the reporting is strictly connected to ECI, it is possible to consider the cost as introduced by the Directive, even if the

[231] Survey: 55% (N=12) of PoCs stated that co-operation concerning CIP existed with CI owners/operators before the Directive.
[232] Survey: 7 PoCs mentioned, among the costs entailed by the implementation of the Directive, those related to the verification of the existence of the OSP and SLO (third most quoted).

Relevant stakeholder	Type of cost	Specific obligation	Recurring cost	Occurring only if ECI is designated	Incidence[228] of costs
					collection of this kind of data may have been required in other contexts.
MS authorities	Compliance cost	Implementation of appropriate communication mechanisms between the relevant MS authority and the SLO with the objective of exchanging relevant information (art. 6.4)	Yes	Yes	**Medium incidence** As seen above, in 12 MS there was co-operation between the national authorities and the operators, so it can be assumed that for them the cost was not new. However, the Directive does not specify which communication mechanisms have to be implemented, so the costs are variable.
CI owners/operators	Compliance costs	The development of the Operator Security Plan (OSP) (art. 5)	Yes	Yes	**Low incidence** Most of the MS (25) already had a requirement for an OSP.
CI owners/operators	Compliance costs	The appointment of a Security Liaison Officer (SLO) (art. 6)	Yes	Yes	**Low incidence** SLOs were already appointed before 2008 in a large number of MS (20).[233]
CI owners/operators	Administrative costs	Costs related to cooperating with and informing the relevant competent authorities at the MS level (art. 6)	Yes	Yes	**Medium incidence** As seen above, co-operation between the national authorities and the operators existed in 12 MS.

[233] 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".