COUNCIL OF THE EUROPEAN UNION

Brussels, 26 June 2012

11887/12

PROCIV 108
JAI 480
ATO 110
COTER 73
ENER 329
TRANS 223
TELECOM 132
ECOFIN 653
CHIMIE 55
RELEX 605
ENV 578
SAN 164
RECH 304
DENLEG 64

COVER NOTE

from:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	22 June 2012
to:	Mr Uwe CORSEPIUS, Secretary-General of the Council of the European Union
No Cion doc.:	SWD(2012) 190 final
Subject:	COMMISSION STAFF WORKING DOCUMENT on the Review of the European Programme for Critical Infrastructure Protection (EPCIP)

Delegations will find attached Commission document SWD(2012) 190 final.

Encl.: SWD(2012) 190 final

EUROPEAN COMMISSION

Brussels, 22.6.2012
SWD(2012) 190 final

COMMISSION STAFF WORKING DOCUMENT

ON THE REVIEW OF THE EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION (EPCIP)

COMMISSION STAFF WORKING DOCUMENT

ON THE REVIEW OF THE EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION (EPCIP)

1. Objectives and context

This document presents the main preliminary findings of the review of the European Programme for Critical Infrastructure Protection (EPCIP)[1] and in particular Directive 2008/114/EC on the identification and designation of European Critical Infrastructures[2].

It provides a general analysis of the elements of the critical infrastructure protection programme and describes the on-going development of risk assessment methodology in this field. In addition, it contains the required annual reporting on EPCIP's external dimension[3].

The damage or loss of infrastructures (or services) in one Member State may have negative effects on others and on the European economy as a whole. This is becoming increasingly pertinent with new technologies (e.g. the internet) and market liberalisation (e.g. in electricity and gas supply), since certain infrastructures have become part of a larger network.

In its EPCIP Communication of 12 December 2006, the Commission sets out an overall policy approach and framework for critical infrastructure protection (CIP) activities in the EU. The general objective of EPCIP is to raise critical infrastructure protection capabilities across all EU Member States against all hazards. The underlying rationale is that disruption to infrastructures providing key services could harm the security and economy of the EU as well as the well-being of its citizens.

The EPCIP Communication sets forth a horizontal framework encompassing:

- measures designed to facilitate the implementation of EPCIP, including an Action Plan, the Critical Infrastructure Warning Information Network (CIWIN), the use of CIP expert groups at EU level, a CIP information-sharing process, and the identification and analysis of interdependencies;
- support for Member States concerning National Critical Infrastructures;
- contingency planning;
- an external dimension;

---

1 COM(2006) 786.

2 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, L345/75.

3 Council Conclusions of 9-10 June 2011 on the development of the external dimension of the European Programme for Critical Infrastructure Protection.

- the EU programme on 'Prevention, Preparedness and Consequence Management of Terrorism and other Security-Related Risks' for the period 2007-2013, which provides funding for CIP-related measures;

- a procedure for the identification and designation of European critical infrastructures and assessment of the need to improve their protection (addressed in detail in Directive 2008/114/EC).

In 2009, the Stockholm Programme[4] underlined the importance of critical infrastructure protection by making the need to reduce EU critical infrastructure vulnerabilities one of its objectives. Moreover, the Stockholm Programme invited the Council, the Commission, the European Parliament, and the Member States to draw up and implement policies to improve measures for the protection, security preparedness and resilience of critical infrastructure, including Information and Communication Technology (ICT) and services infrastructure. It also called for Directive 2008/114/EC to be analysed and reviewed in order to consider including additional policy sectors.

The EU Internal Security Strategy[5] highlights that critical infrastructure must be better protected from criminals who take advantage of modern technologies and that the EU should continue to designate critical infrastructure and put in place plans to protect such assets, as they are essential for the functioning of society and the economy. The Strategy also emphasises that the threats to critical infrastructure call for improvements to long-standing crisis and disaster management practices in terms of efficiency and coherence. More specifically, these threats require both solidarity in response and responsibility in prevention and preparedness, with a focus on better risk assessment and risk management of all potential hazards at EU level.

2. Review

2.1. Process

Taking into account the developments since the adoption of the EPCIP Communication, in particular the entry into force of the Lisbon Treaty and the establishment of the Internal Security Strategy, a review of EPCIP has become necessary. Moreover, Article 11 of Directive 2008/114/EC states that a specific review of the Directive should start in January 2012.

To support the review process, an evaluation study on the implementation and application of Directive 2008/114/EC was launched in late 2011 and delivered final results in March 2012[6].

Additionally, a series of stakeholder and other events have been organised. A workshop to validate the first results of the evaluation study, as well as to discuss the particular protection needs of critical networks (in particular the electrical grid), was organised by the Commission on 15 February 2012.

---

4 Conclusions of the European Council of 10/11 December 2009 on 'The Stockholm Programme — An open and secure Europe serving and protecting citizens (2010-2014)'; 17024/09.

5 Council Conclusions of 24-25 January 2011 on the Commission Communication on the EU internal security strategy in action: Five steps towards a more secure Europe; 16797/10 JAI 990.

6 See chapter 1.3, Evaluation of Directive 2008/114/EC.

A CIP review conference with the Member States' Points of Contact and with input from a wide range of Commission services took place on 14-16 March 2012, in Brussels.

Furthermore, the 7th Workshop on the implementation and application of Directive 2008/114/EC was held on 24-26 April 2012. At this workshop, in addition to discussion of the state of play with the implementation of the Directive and the related review process, a session was devoted to risk assessments for CIP[7].

Following the 3rd EU-US-Canada expert seminar on CIP scheduled on 22-23 May 2012, CIP stakeholders meetings will conclude the CIP review process on 25-26 June. In July, the results of an external study looking into the different policy options for a follow-up to Directive 2008/114/EC will feed into the process. The impact assessment itself will be finalised by September 2012.

Finally, the 2012 Commission Work Programme envisages the adoption of a new CIP policy package for late November 2012[8]. This package will propose a reshaped European framework for critical infrastructure protection.

2.2. Legal basis for critical infrastructure protection

Directive 2008/114/EC was based upon Article 308 of the former EC Treaty, now corresponding to Article 352 of the Treaty on the Functioning of the European Union (TFEU) following the Lisbon Treaty. Article 352 does not provide for the ordinary legislative procedure but requires unanimity in the Council and gives only a limited role to the European Parliament. Article 352 TFEU is also only applicable if 'action by the Union should prove necessary and the Treaties have not provided the necessary powers'. It is thus first necessary to examine whether there is a more specific legal basis elsewhere in the TFEU to take legal action on critical infrastructure protection.

Under Article 4(2)(f) TFEU, the area of freedom, security and justice is a shared competence between the EU and the Member States. Article 84 TFEU, provides the EU with the competence 'to establish measures in the field of crime prevention to promote and support the action of Member States' in accordance with the ordinary legislative procedure, while excluding any harmonisation of the laws and regulations of the Member States. However, this limitation to criminal threats does not entirely match the all-hazard approach usually pursued by CIP initiatives.

In line with the notion of 'service continuity' — as followed by CIP programmes — specific security and protection measures are often included in sector-specific Internal Market legislation based on Article 114 TFEU (formerly Article 95 EC Treaty)[9].

Article 6(f) TFEU introduces the competence to 'support, coordinate or supplement' the actions of the Member States in the area of civil protection. Article 196 TFEU also has a new provision on civil protection (TFEU). It calls on the EU to 'encourage cooperation between

---

7 See chapter 1.4, Risk Analysis in the Context of CIP.

8 http://ec.europa.eu/governance/impact/planned_ia/roadmaps_2012_en.htm#HOME.

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

Member States in order to improve the effectiveness of systems for preventing and protecting against natural or man-made disasters'. This again excludes 'harmonisation of the laws and regulations of the Member States' but corresponds well to some of the general CIP objectives.

The framework for the CIP cooperation at EU level should be subsidiary to the competences of the Member States. Measures under Article 196 TFEU, while excluding any harmonisation of Member State laws, can still establish an obligatory framework for the Union. However, participation in this framework would remain voluntary or allow the Member States a large degree of discretion in how they participate. For any measures under Article 196, the main role of the Commission is to monitor the general implementation of any legislation and to coordinate, supplement and support the Member States.

3. Evaluation of Directive 2008/114/EC

This chapter is based on an evaluation study carried out from October 2011 to March 2012 by an external contractor[10].

3.1. Background

In April 2007, the Council adopted conclusions on EPCIP which welcomed the Commission's efforts to develop a European procedure for the identification and designation of European Critical Infrastructures (ECIs) and the assessment of the need to improve their protection.

This eventually led to the adoption of 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.

The scope of the Directive was limited to the energy and transport sectors. It constituted the first step in a step-by-step approach to identify and designate ECIs and assess the need to improve their protection. The Directive outlined the approach all Member States would be required to follow to identify, designate, and protect European Critical Infrastructures in the energy and transport sectors, while indicating the ICT sector as a priority for possible future expansion of its scope.

The objective of the Directive is to identify, designate and adopt protection measures for infrastructures that are critical from a European perspective, i.e. where their disruption would have an impact on at least two Member States. The Directive specifies that Member States had to take the necessary measures to comply with the Directive by 12 January 2011 and sets 12 January 2012 as the start date for the review of the Directive.

In order to establish a common perspective and facilitate implementation, Article 2 of the Directive provides definitions of the key terms used, such as 'critical infrastructure', 'European critical infrastructure', 'risk analysis', 'sensitive critical infrastructure protection related information', 'protection' and 'owners/operators of ECIs'.

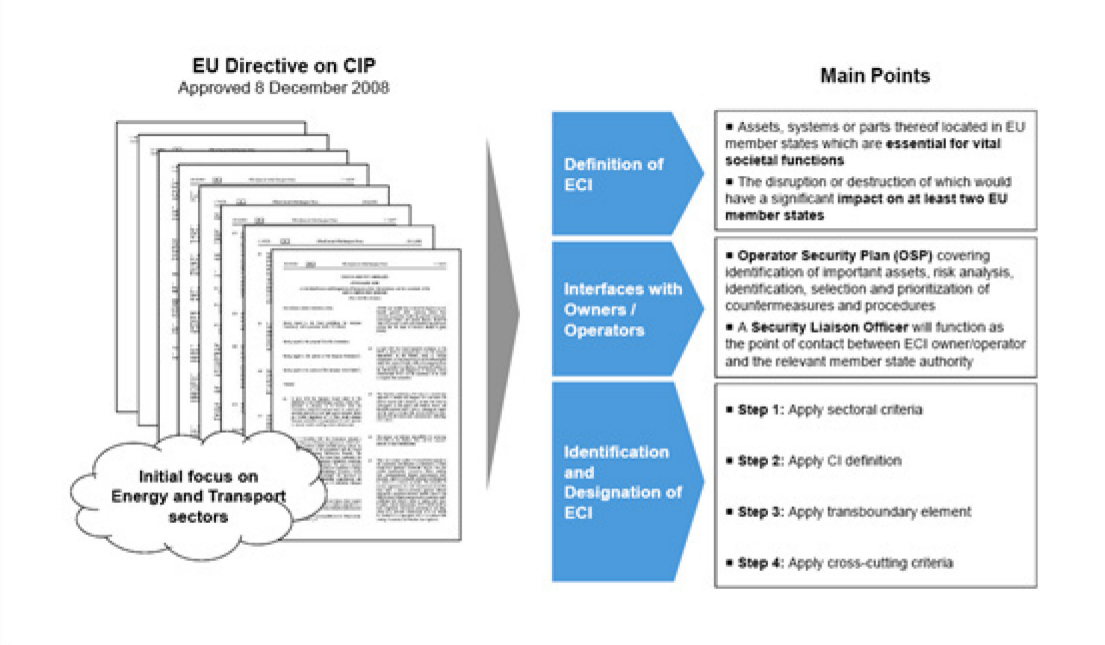
Annex III to the Directive also requires all Member States to adopt a four-step process (see graph below) and to apply cross-cutting and sectoral criteria to identify ECIs in the energy and transport sectors. In order to facilitate a cooperative approach, the Directive also requires

[10] The complete study can be requested by sending an e-mail to: HOME-EPCIP@ec.europa.eu.

the relevant Member States — those within which an ECI is identified and those which may be affected by its disruption — to engage in negotiations leading to the designation of ECIs (Articles 3 and 4).

Once an ECI is identified, the Directive requires a specific set of actions to be taken by its owners/operators in order to develop an Operator Security Plan (OSP) documenting critical assets and security measures. However, concessions exist for ECI entities that already have similar or equivalent requirements in place. The Directive makes the Member State authorities responsible for ensuring that ECIs comply with its requirements.

In order to facilitate coordination on security-related issues between ECI owners/operators and the Member States, the Directive requires an ECI owner/operator to appoint a Security Liaison Officer, and Member States to appoint contact points for European critical infrastructure protection. Member States must then implement appropriate communication mechanisms to facilitate information exchange. Additionally, the Directive specifies ECI-related information handling and reporting requirements.



Summary of Council Directive 2008/114/EC

3.2. Member State legislation related to the Directive

The majority of Member States have implemented the provisions of the Directive by incorporating them within their national legislative and regulatory frameworks through a variety of approaches, such as:

- amendments to existing laws and regulations
- new laws
- resolutions
- procedural changes to existing CIP-related activities

- decrees and executive orders

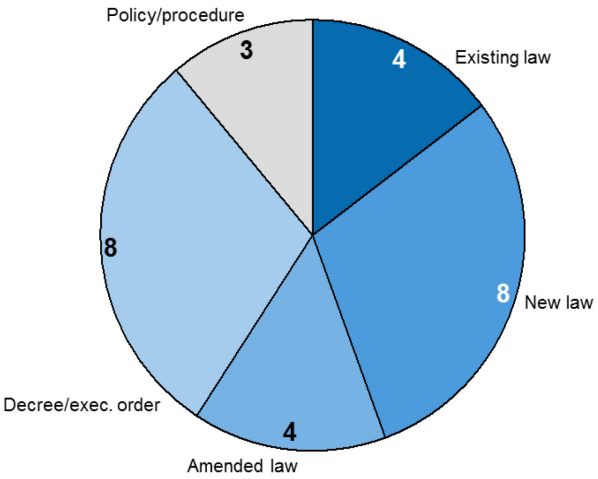
A number of Member States, after evaluating their existing national approaches in the light of the Directive, came to the conclusion that no legislative changes were required to implement the Directive. These Member States (Austria, Estonia, Finland, the Netherlands, and the United Kingdom) have made the necessary procedural changes within their existing national CIP frameworks in order to implement the Directive.

Member States that only needed to adopt procedural changes to implement the Directive, without legislative action, commonly had a relatively high degree of cooperation through public-private partnerships (PPP), with a preference for a consultative approach to national CIP activities. In fact, some of these Member States did not have any overarching national CIP laws in place, even though they had internationally leading CIP programmes (e.g. the Netherlands, UK).

The general approach followed by most Member States in implementing the legislative aspects of the Directive started by identifying gaps in existing legislation with respect to the Directive. This assessment generally resulted in a decision on what types of legislative instruments and/or procedural changes were required to implement the Directive.

Even those Member States that did not implement legislative changes reported having carried out assessments to evaluate if legislative changes were needed. Some of them stated that significant resources were still required to ensure national parliamentary oversight of compliance with the Directive.

Reflecting the differing levels of maturity of CIP programmes in the Member States, as well as the different legal requirements under the various national legislative environments, the distribution of these various options was fairly even across all 27 Member States:



Directive implementation instruments per Member State

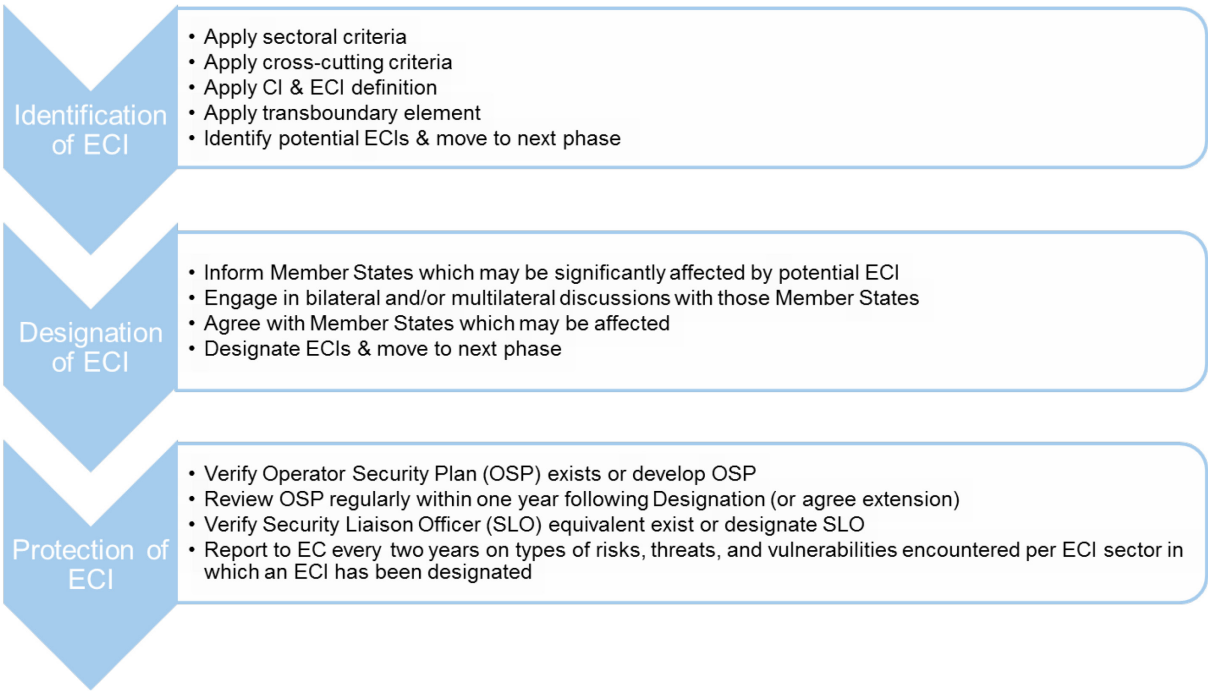
Regardless of the legislative action taken, no major difficulties emerged in implementing the Directive in national programmes. However, some Member States did indicate some specific issues they had to overcome, such as:

- A number of Member States follow system-focused national CIP programmes where the end goal is security and resilience of systems, which may involve activities across multiple sectors. As a result, the sector-focused approach presented a major challenge. Some of these Member States have adopted a 'service'-oriented approach for analysis. For instance they identify vital services from a national perspective, such as energy supply, and then implement processes and procedures to increase the security and resilience of such services. Hence, they are focused on final outcomes and are not restricted by the sectoral boundaries of the Directive. As regards the issue of energy supply, this would for instance involve the energy, transport, and ICT sectors.

- Member States such as Spain and Germany, in which the national government delegates power to provincial/regional authorities, faced additional challenges compared to Member States with a centralised governance structure. They had to take additional legislative steps to coordinate the activities needed to implement the ECI process, including the development and maintenance of Operator Security Plans and Security Liaison Officers.

3.3. Implementing the ECI process

The ECI process, as specified in the Directive, can be divided broadly into three distinct phases: identification of potential ECI, designation of ECI, and protection of ECI. Annex III of the Directive specifies the steps within each of these phases.



ECI Process

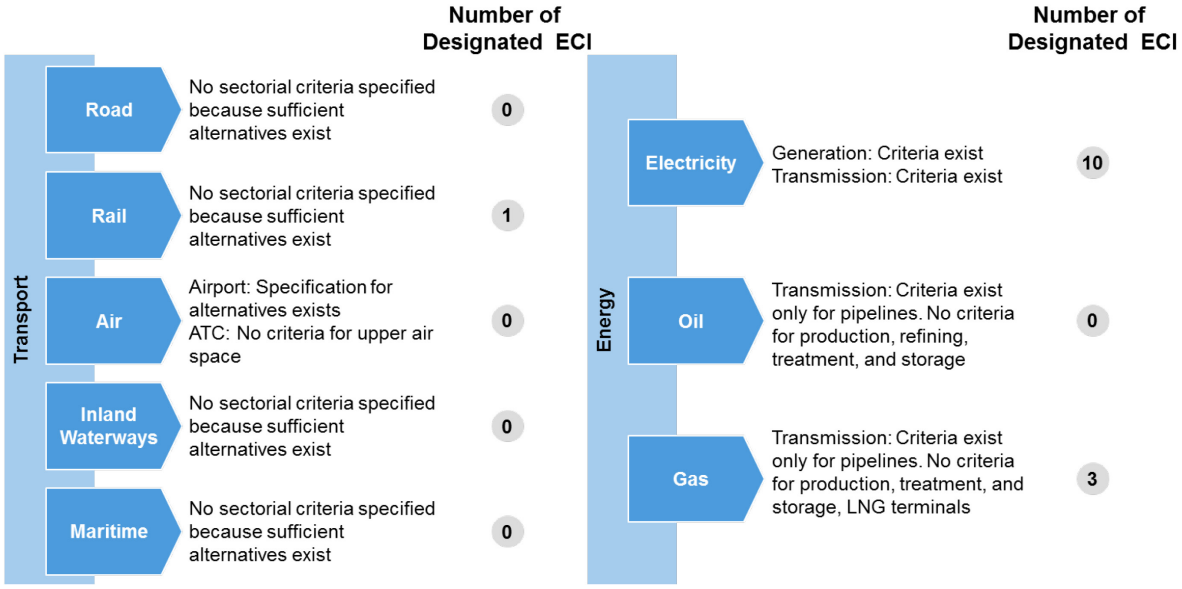
3.3.1. Identification of ECI

The identification of potential ECIs itself comprises four steps. Annex III of the Directive suggests applying sectoral criteria[11] (specifying the infrastructures in transport and energy targeted by the Directive) to make an initial selection of critical infrastructures (CIs) within a sector.

The next step is to confirm that the CIs identified in this first step meet the definition of 'critical infrastructure' in Article 2(a) of the Directive. The Directive then suggests evaluating the impact of any disruption to the identified CIs on other Member States. This can be done by applying either the cross-cutting criteria[12] (CCC), which specify thresholds to assess the general effects of CI disruption, such as the number of casualties, economic effects or public effects, or the national equivalent of such criteria. This impact evaluation should factor in alternatives and disruption/recovery time.

Most Member States have applied the sectoral criteria, with a few making adjustments and adaptations to align them with an existing national approach. For example, some Member States (e.g. the UK) have mapped the sectoral criteria to their national criteria. The non-binding guidelines to support the application of the Directive[13] have also been followed in some cases. In other cases, certain Member States have assigned responsibility for determining the sectoral criteria to the ministries or sectoral regulators concerned.

The figure below shows whether criteria are specified for each sub-sector and highlights the number of ECIs (as of February 2012) designated in each of these sub-sectors.



Sectoral Criteria vs Designated ECIs

---

11 Non-binding guidelines for the application of the Directive on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection; Doc. 15616/08.

12 Sectoral criteria, Doc. 15613/08 ('RESTREINT UE').

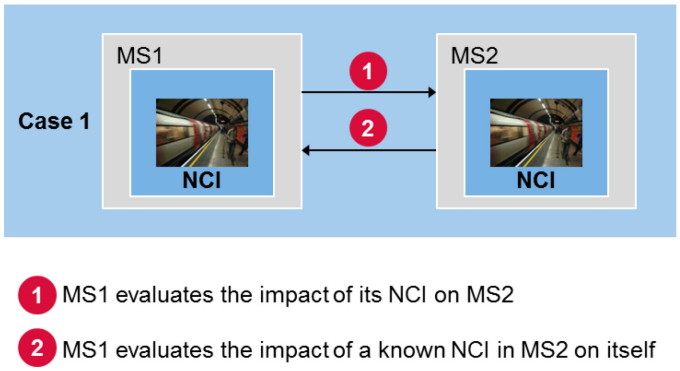
13 Cross-cutting criteria, Doc. 15615/08 ('RESTREINT UE').

The considerable difference between the numbers of ECIs eventually designated in each sector (Transport — 1, Energy — 13) is a point that has continually emerged in discussions with all stakeholders throughout all steps of the ECI process.

Almost all Member States started the process of identifying potential ECIs with a known list of their own national critical infrastructures (NCIs), which they considered to be the 'whole set' from which the 'sub-set' of ECIs should be identified. The figure below illustrates the approach uniformly followed in identifying potential ECIs.

In the figure below, Scenario 1 (applied by almost all Member States) highlights how Member State 1 (MS1) evaluates the impact of disruption to any of its national CIs on another Member State. In addition, Scenario 2 illustrates how some Member States (far fewer) have also considered known national CIs of a second Member State (MS2) and evaluated the possible impact on them (MS1) of a disruption to MS2's NCIs.

Both of these scenarios are well within the approach outlined in the Directive. However, by using the list of national CIs as the starting point and effectively removing items from that list in the course of the four steps of the identification process, stakeholders may be overlooking potential ECIs not already designated as NCIs. For example, none of the stakeholders interviewed systematically evaluated whether or not any non-critical infrastructure in their own (MS1) territory could potentially have a significant impact on another Member State (MS2).



National Critical Infrastructure-Centric Identification Process

Similarly, Member States have not assessed whether a non-NCI asset in their own (MS1) or another MS (MS2) territory, as a result of any disruption, could impact any 'EU-level service' with consequent negative effects on themselves or other Member States. In this regard, the term 'EU-level service' is used to mean a service provided to multiple Member States through infrastructure that is not owned and/or operated by any individual Member State (e.g. air traffic management).

3.3.2. Designation of ECIs

The designation process specified in Annex III to the Directive starts with a Member State that has identified potential ECIs in its own territory contacting other Member States that would be affected by disruption to these potential ECIs. The process also allows a Member State to contact other Member States if it believes that disruption to an asset in another Member State may have a significant impact on itself. The Member States then enter into negotiations and agree through bilateral/multilateral discussion whether or not an

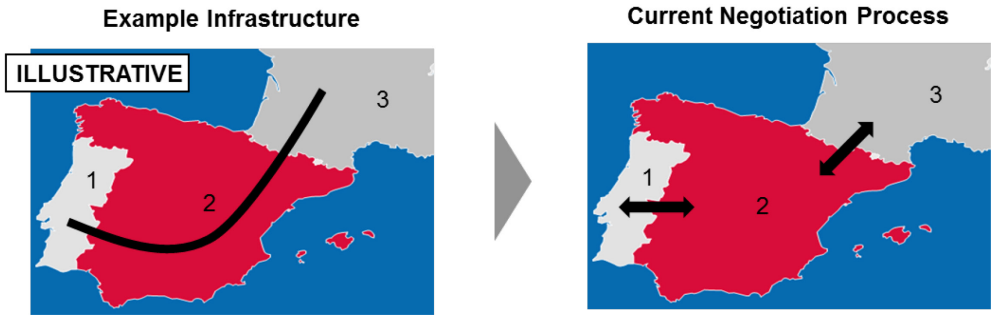
infrastructure should be designated as an ECI. If it is designated, the operator of the ECI is informed.

The EPCIP programme, along with the Directive, has facilitated the designation of national points of contact for CIP-related issues in each of the Member States. All Member States have appointed an ECI point of contact as required by Article 9 of the Directive. The relationships between these points of contact have also been fostered through various conferences and forums organised by the Commission, allowing them to meet periodically.

During implementation of the ECI Directive, this well-established network of national points of contact played a critical role in communication between Member States. This close cooperation and effective communication has also been facilitated by the various workshops on the implementation of the Directive.

In most cases, the ECI designation process has been managed using the ECI points of contact as channels of communication. The actual participants representing the Member States have varied based on how ECI responsibilities are allocated. Member States that have implemented legislative instruments specifically for ECI usually have specified within their legislation the roles and departments responsible for discussions with other Member States. In general, the main actors have been the public authorities in charge of coordinating ECI activities, although the process has often involved ministries responsible for external affairs.

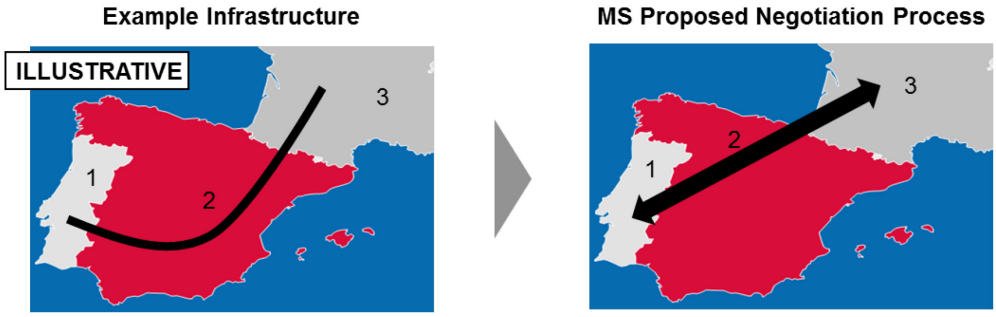
Although not expressly required by the Directive, most of the negotiations on designating ECIs have been bilateral in nature (see below Scenario A). Some Member States (e.g. Italy) have pointed out that the nature of the infrastructure under discussion often involves several Member States, and that bilateral negotiation does not reflect the nature of these infrastructures. This is especially true for energy and transport infrastructure, where disruption may impact more than the two Member States involved in the negotiations. Potentially, this could result in one part of the infrastructure designated as ECI between two Member States, while another part of the same infrastructure may not be designated as such by two other Member States.



Scenario A: Bilateral Negotiations to Designate ECI

In Scenario A, negotiations between MS1 and MS2 could produce different results than the negotiations between MS2 and MS3. This could result in MS2 having to return to MS1 to renegotiate a potential ECI, with perhaps one part of the ECI between MS2 and MS1 being designated ECI and another part between MS2 and MS3 not being designated as ECI.

Some Member States have suggested that the designation of ECI with an impact on multiple Member States should always be a multilateral process, with all the affected Member States involved in negotiations simultaneously, since this would lead to a better understanding of the overall impact and take account of the opinions of all Member States that may be impacted (see Scenario B below).



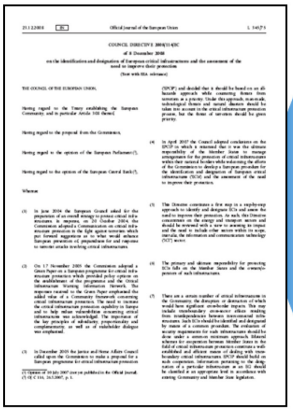
Scenario B: Multilateral Negotiations to Designate ECI

3.4. Conclusions on the impact of the Directive

Member States with comparatively mature national CIP programmes did not see any great added value in the Directive, primarily due to the perceived high level of protection already in place. Other Member States with comparatively less mature programmes saw a greater degree of improvement. Member State perceptions of the Directive's direct impact and side-effects are summarised in the figure below.

For the transport sector in particular, it is necessary to distinguish between the comprehensive safety and security measures already in place in the aviation and maritime sub-sectors and the lack of such measures in the other transport sub-sectors. For instance as far as maritime ports are concerned the implementation of this Directive has often be seen as a competing priority vs. other European legal requirements already in place. A general perception, especially on the part of transport operators, was that the global and European supply chain should be treated as critical infrastructure. In the energy sector, there was a distinct feeling that the lack of criteria for certain sub-sectors and the lack of focus on dependencies within or between the sectors may have influenced outcomes.

ECI Directive



Directive Core Objectives		
Objectives	**MS Opinion**	**Comments**
ECI Identification	◕	EU level service issues
ECI Designation	◕	Limited party negotiation
Improved Security	◔	Lacks evidence

Directive Side Effects		
Objectives	**MS Opinion**	**Comments**
CIP Awareness	●	Majority view
Cooperation – PPP	◕	Some MS benefitted
Cooperation – Among MS	●	Majority view

Level of Objective Achievement

○: None ●: Full Achievement

Summary — MS Perception of Results Achieved

Overall, the opinions of the Member States, operators, and DG officials as to the actual benefits gained from implementation of the Directive in the energy and transport sectors focus on two distinct aspects — CIP (ECI) security levels and CIP-related cooperation and awareness.

There is a strong perception that implementation of the Directive has not resulted in sufficiently clear and tangible improvements to ECI security levels. A number of facts support this viewpoint, most importantly the fact that relatively few ECIs have been identified and consequently very few new Operator Security Plans have been produced.

In addition, there are concerns as to whether the set of identified ECIs is complete, since the assets of pan-European services do not appear to have been evaluated thoroughly as potential ECIs, while it is openly recognised that main energy transmission networks (gas, electricity) are of cross-border dimension. The current ECI designation process does not respond to this particular challenge, as protection measures cannot be the product of a single Member State or operator.

On the other hand, the majority view is that general CIP awareness and the level of cooperation in the EU has increased in the energy and transport sectors through the various activities and forums organised under the Directive. However, the credit for improved awareness and cooperation is not entirely due to the Directive and EPCIP, since other sectoral initiatives, for instance in the area of aviation security, have played an important role as well.

Either way, the opinions on whether there has been any improvement or not are all based on anecdotal evidence. No baseline measurements were undertaken prior to implementation of the Directive, thereby making an objective comparison between the pre- and post-implementation stages virtually impossible.

To further add to the complexity of evaluating the impact, with various operators continually undergoing changes in CIP because of enterprise risk management activities, national and international regulations, and technological advances, it is difficult to attribute changes in CIP status specifically to the Directive, or for that matter to any other similar initiatives.

While there are mixed opinions on the actual improvement of security, there is near consensus on the added value of side-effects, such as increased CIP awareness and cooperation. It appears for instance that the very existence of a legal instrument has nurtured policies on the protection of national critical infrastructures. This has resulted in concrete actions, such as the creation of specific national bodies to deal with CIP policies. In the energy sector both the launch of risk management and protection measures in cooperation with operators have been supported. In the end, however, most Member States express great concern that the primary objective of the Directive — improved security — seems to be the area with the lowest level of perceived improvement.

In addition, given that the outcome of the programme may not have hit its primary mark, Member States then question whether the added value realised could not have been obtained through less resource-intensive means than a Directive.

4. Risk analysis in the context of CIP

For a fully-fledged critical infrastructure protection initiative, a risk assessment component is indispensable. Article 7(2) of the Directive states that Member States must regularly report to the Commission on the types of risks, threats and vulnerabilities for those sectors where ECIs have been designated. Member States have delivered first assessments for such sectors. Moreover, risk assessment must be conducted as an on-going task within the context of an Operator Security Plan for a designated ECI. Moreover, such risk assessments and Operator Security Plans were already compulsory for airports, maritime ports and port facilities under existing European legislation.

In general, the usual approach to risk assessment is rather common and linear, consisting of the following elements: identification and classification of threats, identification of vulnerabilities, and evaluation of impact. This is a well-known and established approach for evaluating risks and forms the backbone of almost all existing risk assessment methodologies.

During the 6th Workshop on the implementation and application of the Directive at the JRC in Ispra in December 2011, the Member States asked for a closer look at a systems approach to critical infrastructures, including a risk analysis component of such systems. For more complex systems, including the interaction of cyber and physical layers, the boundaries of the sectors are no longer clearly defined, so it is often rather difficult to classify a certain infrastructure within sectoral limits. This reflects the complex interconnectivity of infrastructures for the delivery of vital societal services.

Following the workshop, the JRC has written a report analysing existing risk assessment methodologies[14]. The aim has been to obtain a structured review of the existing methodologies at EU and global level, identify gaps, and prepare the ground for proposing a risk assessment methodology at European level.

[14] The complete working paper by the JRC can be downloaded here: http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/RA-ver2.pdf.

The aim has not been to establish a new methodology from scratch, but rather to build on existing knowledge in Europe and worldwide suitable for the risk assessment of European critical infrastructures.

However, there are a huge variety of risk assessment methodologies, based on the scope of the methodology, the audience it addresses (policy makers, operators, research institutes) and the domain of applicability (asset level, infrastructure/system/network level, system of systems level). The domain of applicability defines to a large extent the target group of the methodology. For example, a risk assessment methodology applicable to systems at national or even supranational level is mostly addressed to policy makers and relevant authorities and less to operators or to asset managers at local level.

Methodologies developed for certain assets are well defined, tested and validated, and the vast majority follow the linear approach already mentioned. Methodologies that aim to assess risks at a higher level, e.g. for networked systems, require further refinement. Detailed risk assessment at this level is no longer applicable and a certain level of abstraction is necessary.

An important parameter in risk assessment methodologies for networked infrastructures is the issue of interdependencies. According to the work of Rinaldi et al[15], there are four types of interdependencies for critical infrastructures:

- Physical: the operation of one infrastructure depends on the material output of the other;
- Cyber: dependency on information transmitted through the information infrastructure;
- Geographic: dependency on local environmental effects simultaneously affecting several infrastructures;
- Logical: any kind of dependency not characterised as Physical, Cyber or Geographic.

Apart from interdependencies between sectors (e.g. ICT and Electricity, Satellite Navigation and Transport), intra-sectoral interdependencies can be identified at European level between national infrastructures that form European infrastructures. As a concrete example, we can mention the high-voltage electricity grid, which is composed of the interconnected national high-voltage electricity grids.

The domain of applicability of a risk assessment methodology may be the most important feature. The risk assessment methodologies for CIP can be divided into two major categories accordingly: category 1) Sectoral approach, where each sector is treated separately with its own risk methodologies and risk ranking; and category 2) Systems approach, where critical infrastructures are treated as an interconnected network.

Methodologies initially conceptualised to fit in the 'systems approach' category are rather limited. The vast majority of existing work has been sectoral, mostly at asset level. These methodologies have been extended to networked systems. This reflects the natural extrapolation of risk assessment methodologies at organisational level to address issues at sectoral level, but these methodologies show their limits when cross-sectoral issues must be addressed.

---

[15] Steven M. Rinaldi, James P. Peerenboom, Terrence K. Kelly, Identifying, Understanding and Analysing Critical Infrastructure Interdependencies, IEEE Control Systems Magazine, December 2001, pp. 11-25.

This work is the first of a series of reports that will follow the review of the Directive. Further work in this field will also contribute to Objective 5 ('Improve Europe's resilience to crises and disasters') of the EU Internal Security Strategy, which aims to establish a coherent risk management policy linking risk and threat assessment to decision-making. The improved resilience of critical infrastructure in particular could thus reinforce and feed into the more comprehensive and general national risk assessments that Member States have committed to prepare within the EU civil protection cooperation[16]. A recent proposal for a Union Civil Protection Mechanism[17] envisages that Member States should develop risk management plans on the basis of their national risk assessments and integrating different sector or hazard-specific risk management instruments into a common overall plan. On the basis of the national risk analyses of the Member States the Commission will prepare a cross-sectoral overview of the major natural and man-made risks that the EU may face in the future. This should then lead to an EU-wide risk-based approach to security in a coherent EU risk management policy.

5. Report on the external dimension of EPCIP

This chapter is a follow-up to the 2011 'Council Conclusions on the development of the external dimension of the European Programme for Critical Infrastructure Protection'[18]. Particularly relevant here are points 8 and 9, which invite the Member States to step up cooperation with relevant third countries, and call on the Commission to inform the Council and the European Parliament each year about progress and developments in this area.

5.1. EEA countries

The EEA countries (Norway, Iceland, and Liechtenstein) are invited to all EPCIP-related meetings. To formalise this cooperation with the EEA, the Commission has recently presented a proposal for a Council Decision, which aims to expand the applicability of Directive 2008/114/EC to the EEA countries[19].

Norway in particular participates regularly in the Directive workshops and EPCIP points of contact meetings. Under the cooperation schemes of the Nordic countries, Sweden and Denmark have further specific contacts with Norway, including discussion of potential ECIs in the context of the implementation of Directive 2008/114/EC.

With regard to sectoral CIP activities driven by the Commission, Norway is fully involved in the work on the protection of critical information (CIIP) as well as energy infrastructure (via membership in the pan-European energy operator associations).

---

16 Council Conclusions of 12 April 2011 on further developing risk assessment for disaster management within the EU

17 Proposal for a Decision of the European Parliament and of the Council on a Union Civil Protection Mechanism (COM(2011)0934 final) currently under discussion in the Council and the Parliament.

18 3096th Justice and Home Affairs Council meeting, Luxembourg, 9 and 10 June 2011.

19 Proposal for a Council Decision to the EFTA working party on the position to be taken by the European Union in the EEA Joint Committee concerning an amendment to Protocol 31 to the EEA Agreement, on cooperation in specific fields outside the four freedoms [agreement - doc. 7539/12 EEE 19 AELE 15 PROCIV 40).

5.2. Switzerland

Germany refers to the informal cooperation between its Federal Office of Civil Protection and Disaster Assistance (BBK) and the Swiss Federal Office for Civil Protection (BABS). Since 2006, the results of analyses and projects as well as best practices have been exchanged and methodological and procedural issues discussed at various bilateral meetings.

Since 2008, Germany, Austria and Switzerland have been cooperating under the D-A-CH framework on CIP topics. Several meetings have been held, national approaches to the protection of critical infrastructures have been presented and EPCIP has been discussed. In 2010, for a meeting on CIIP, Austria, Germany and Switzerland were joined by the United Kingdom and the Netherlands.

With regard to sectoral CIP activities by the Commission, Switzerland, although not an EEA member, is also invited to the activities under CIIP (European Forum of Member States, EP3R) and in the Thematic Network on Critical Energy Infrastructure Protection.

A number of Member States have indicated interest in further consolidating EU cooperation with Switzerland. The next steps planned are EU-Swiss expert meetings to exchange best practices on CIP risk assessments.

5.3. United States and Canada

Two EU-US expert meetings have been held (in 2010 in Madrid and in 2011 in Budapest), co-organised by the Commission and the Presidency of the Council. The meeting in Budapest included Canadian experts. The third EU-US-Canada meeting was held on 22-23 May 2012. The meetings have so far served to exchange best practices. A more far-reaching toolkit for cooperation has been under discussion with the US since the meeting in 2011.

Several EU countries (Germany, Poland, and Sweden) refer to on-going or intended bilateral cooperation with the US. In the case of Sweden this also includes Canada. At this stage, all these countries refer to knowledge sharing and exchange of good practices (methodologies to analyse risks and interdependencies, guidelines and recommendations, etc.).

In the case of Germany, cooperation with the US is underpinned by a bilateral agreement with an annual work programme, which could lead to more concrete activities in the future.

In sectoral activities driven by the Commission, regular workshops are held as part of the EU-US Civil Space Dialogue. On 14-15 March 2012, two workshops on Commercial Space Critical Infrastructure Protection and Space Situational Awareness were organised in the US, following previous workshops held in Europe. A joint EU-US issue that has become very pertinent is the protection of Commercial Satellite Communications (SATCOM).

On cyber aspects, significant progress on CIIP has been achieved by the EU-US Working Group on Cyber-security and Cyber-crime.

In the transport area, although not specifically labelled as CIP, close EU-US cooperation exists in certain sub-sectors such as aviation. For instance, a US-EU Joint Declaration on Aviation Security was signed in January 2010 in Toledo ('Toledo declaration').

5.4. Russia

Germany refers to a formal bilateral agreement in place with Russia, defining a multi-annual programme. The protection of critical infrastructures is part of this programme. So far, concrete activities have been developed for the exchange of practices.

Several countries have expressed their interest in enhancing CIP cooperation with Russia, in particular on energy.

5.5. China

Germany supports China in developing crisis management skills. Certain parts of this training are related to critical infrastructure protection.

5.6. Israel

Germany refers to a planned Joint Declaration of Intent on Bilateral Cooperation and Mutual Assistance between Germany and Israel. An exchange of strategic planning and basic legal regulations for civil protection, including the protection of critical infrastructures, is also planned.

5.7. International Organisations

Most EU countries are involved in the NATO working groups concerned with critical infrastructure (including the NATO-Russia energy group), where CIP concepts and practices are discussed with non-EU countries.

Recently, the OSCE[20] (56 participating countries, including all EU countries) has also stepped up its work on CIP, in particular on energy [21] and cyber aspects.

6. Way forward

The review of the different EPCIP elements so far implemented has already led to a number of important findings for the preparation of a reshaped CIP policy package in November 2012:

- All Member States have legally implemented Directive 2008/114/EC by establishing a process 'to identify and designate European Critical Infrastructures', which has contributed to raising CIP awareness in the EU and in the Member States.

- Although there is evidence that the Directive has also helped in 'assessing the need to improve the protection of European critical infrastructures' in the transport and energy sectors, there is no indication that it has actually improved security in these sectors.

- The sector-focused approach of the Directive represents a challenge to a number of Member States, as usually in practice the analysis of criticalities is not restricted by sectoral boundaries and follows rather a 'system' or 'service' approach. Although the Directive has partially fostered European cooperation in the CIP process, in particular through stakeholder meetings and workshops, it has mainly encouraged the bilateral engagement of Member States and not established a European forum for decision-making.

---

20 Organisation for Security and Cooperation in Europe.

21 http://www.osce.org/atu/70078.

In general, risk management and risk assessment methodologies play an important part in any CIP programme from local to international level and, in this regard, Member States have repeatedly asked for EU support. After a first report on existing risk assessment methodologies, the Commission will support the further development of a CI risk management policy with more specific guidelines and recommendations.

In relation to third countries, work on CIP has gained more importance over recent years, especially with the EFTA countries and the US.

A reshaped CIP policy proposal in late 2012 will take due note of the legal and political framework established by the Treaty of Lisbon and the EU Internal Security Strategy, as well as the preliminary findings of the EPCIP review process set out in this document.