BRIEFING
Implementation Appraisal

European Parliament

European critical infrastructure
Revision of Directive 2008/114/EC

This briefing is one in a series of implementation appraisals produced by the European Parliamentary Research Service (EPRS) on the operation of existing EU legislation in practice. Each briefing focuses on a specific EU law that is likely to be amended or reviewed, as envisaged in the European Commission's annual work programme. Implementation appraisals aim at providing a succinct overview of publicly available material on the implementation, application and effectiveness to date of specific EU law, drawing on input from EU institutions and bodies, as well as external organisations. They are provided by the Ex-Post Evaluation Unit of the EPRS to assist parliamentary committees in their consideration of new European Commission proposals, once tabled.

SUMMARY

Council Directive 2008/114 is a key pillar of the European programme for critical infrastructure protection (EPCIP). The directive established an EU-wide procedure for identifying and designating European critical infrastructures and a common approach to assess needs so as to improve protection from anthropogenic threats – both intentional and accidental – as well as natural disasters. The scope of the directive is limited to two sectors, namely energy and transport, although, theoretically, its design allows for extension to other sectors.

In its first evaluation of the directive, put forward in July 2019, the Commission concluded that the directive is only partially effective and relevant, as the security context in which critical infrastructures operate has changed substantially since the time the directive entered into force. Consequently, the Commission announced a new legislative proposal for additional critical infrastructure protection (CIP) measures in its 2020 work programme. This proposal came out on 16 December 2020, together with an impact assessment. The proposal aims to enhance the resilience of European critical entities, by shifting from an assets-focused approach to a systems-focused approach, expanding the directive's scope and aligning the new directive with a proposed revision of the EU Network and Information Security Directive ('NIS 2').

1. Background

Council Directive 2008/114/EC, adopted on 8 December 2008, is an integral part of the European programme for critical infrastructure protection, which emerged in the aftermath of the devastating terrorist attacks that shook the US and Europe in the early 2000s. Despite its terrorism-related roots, the EPCIP takes a broad approach regarding causes of threat. While recognising threats resulting from terrorism as a priority, it embraces an all-hazards approach towards the protection of critical infrastructure, encompassing man-made and technological threats (e.g. industrial incidents, black-outs, terrorism) as well as natural disasters caused for instance by earthquakes, or extreme weather conditions, such as flooding and hurricanes.

Author: Irmgard Anglmayer
Ex-Post Evaluation Unit

PE 662.604 – February 2021

The purpose of the directive

The directive established a **step-by-step procedure** for the identification and designation of critical infrastructures located on EU territory that are vital from a European perspective, in the sense that their disruption or loss would have major cross-border impacts. When a Member State has identified potential ECI, it needs to engage in talks with other Member States affected, since the designation of ECI is subject to the agreement of all Member States affected.

Definition of European critical infrastructures

European critical infrastructure (ECI) means an asset, system or part thereof located on EU territory, which is essential for the maintenance of vital societal functions, health, safety, security, economic or well-being of people, and the disruption or destruction of which would have a significant impact on at least two Member States, as result of the failure to maintain those functions.

The significance of the impact is assessed against distinct cross-cutting criteria, which encompass casualties, economic and environmental effects and public effects.

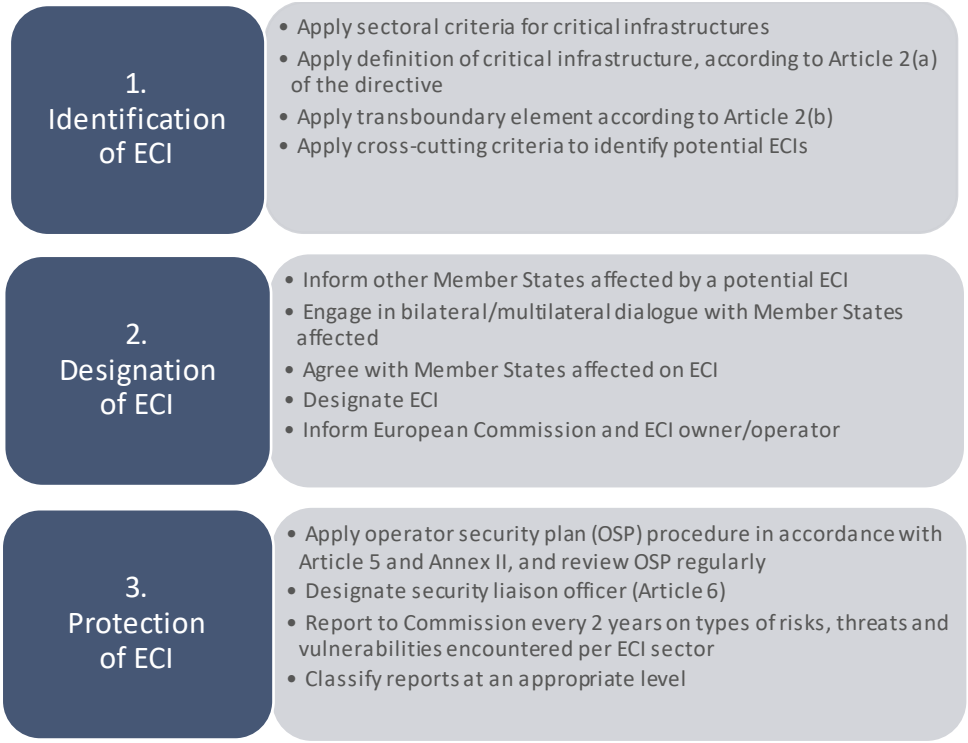
Source: Directive 2008/114/EC, Articles 2 and 3.

Furthermore, the directive set up a common approach to assess the need to improve the protection of ECI. This common approach requires ECI owners/operators to establish for each registered ECI an operator security plan (i.e. an advanced business continuity plan) and to designate a security liaison officer, to act as the contact point for relevant CIP authorities. It also sets out reporting duties, requiring Member States to report generic data on the types of risks, threats and vulnerabilities encountered to the European Commission.

The directive divides the **ECI process** into three stages, which are detailed in the diagram below.

1. identification of potential ECIs (in principal derived from existing national critical infrastructures);
2. designation of ECIs (in agreement with other Member States affected); and
3. protection.

Figure 1 – Steps in the ECI process under Directive 2008/114/EC



Source: Directive 2008/114/EC and its Annex III.

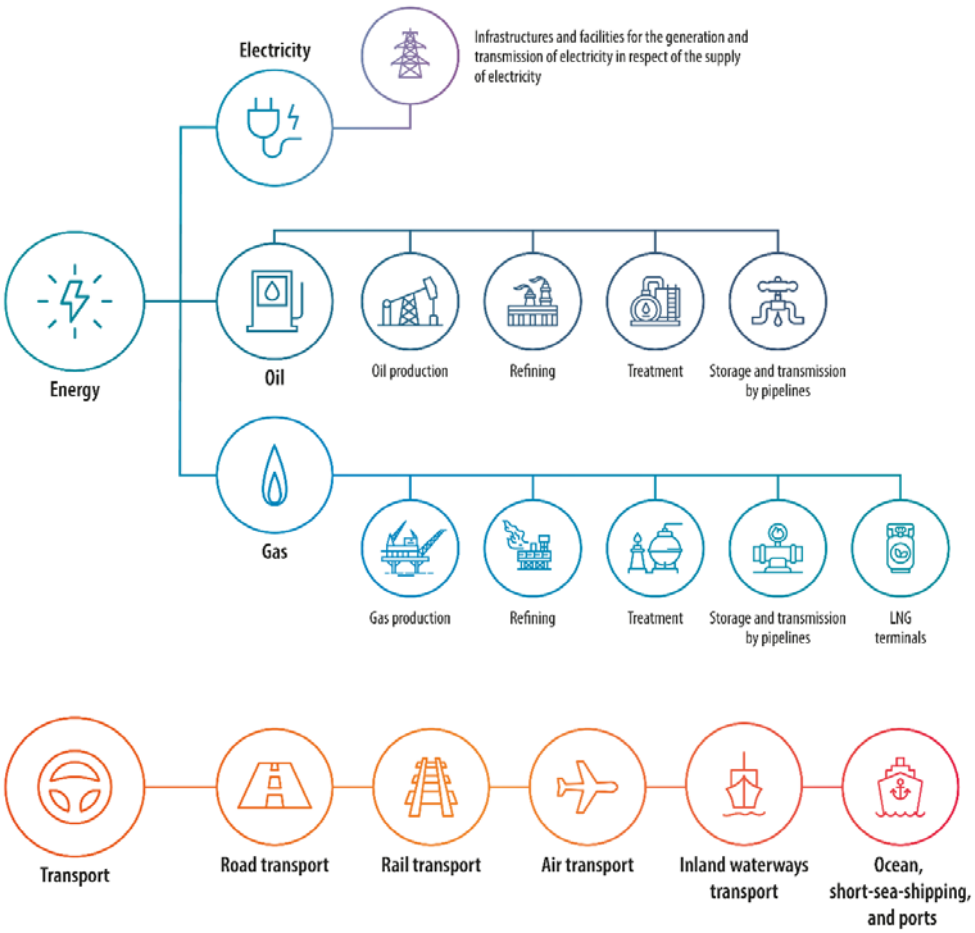
The directive does not enter into much detail. Annex III provides some specifications on procedural steps within the identification stage, while Annex II offers guidance regarding the procedure to establish ECI operator security plans. Additional – albeit non-binding – guidelines on the application of the directive have been prepared by the Commission and the Member States, in particular the Council Working Party on Civil Protection.[1] These guidelines were issued just before the adoption of the directive.

The **rationale** of this common framework was to complement existing national CIP programmes with an integrated EU-wide approach, and to improve coherence across the EU. Given that a large proportion of critical infrastructure is owned and operated by private-sector companies, a trend enhanced through market liberalisation, the protection of vital assets and systems relies on effective cooperation between state and private actors.

Scope of the directive

The scope of the directive is limited to two sectors, namely **energy and transport**, albeit excluding nuclear energy. Annex I provides a comprehensive list of eight subsectors, three pertaining to energy and five to transport (see graph below). In principle, the directive's design allows for sectoral expansion: recital 5 explains that the directive was meant to be the 'first step in a step-by-step approach to identify and designate ECIs', and that other sectors could be added in future, following a legislative review. In this respect, priority should be given to the information and communication technology sector (ICT), as set out in Article 3(3).

Figure 2 – Critical infrastructure sectors covered by Directive 2008/114/EC



Source: EPRS, based on Annex I of the Directive.

Interestingly, the initial Commission proposal (COM(2006) 787) was far more comprehensive in scope than the directive adopted. It provided for nine critical infrastructure sectors in addition to energy and transport: the nuclear industry; information and communication technologies (ICT); water; food; health; financial; chemical industries; space; and research facilities. In the course of the negotiations, following controversial discussions in Council, the list was narrowed down considerably to the two 'priority sectors' energy and transport.

Transposition of Directive 2008/114/EC

Member States had to transpose the directive into their national frameworks by 12 January 2011. This deadline coincided with the date by which Member States had to identify and designate ECIs, in accordance with Article 4 of the directive. All Member States transposed the directive in time, although with great variations regarding the measures chosen and the details of provisions. In the implementation process, some Member States reportedly found the sectoral approach of the directive challenging, because their national CIP programmes were system-focused rather than asset-focused, therefore taking interdependencies between sectors into account.

Although transposition into national law was a smooth process overall, the identification and designation of ECIs across the EU remained way below expectations. By February 2012, only 14 ECIs had been designated: 13 in the energy sector (most of them electricity assets), and only one in the transport sector. This raised doubts as to the completeness of the list.

The latest figures available (2020) suggest that the **current number of designated ECIs has risen to 94**: 95 % pertain to the energy sector, and only 5 % to transport.[2] Neither the Commission nor any other EU body maintains a comprehensive list of ECIs. Member States' notifications to the Commission are restricted to generic information (such as the number of ECIs per sector), but do not contain any information about their identity/location nor technical details.

2. Commission reports

The Commission's first EPCIP review (2012)

Article 11 of the directive required the Commission to commence a review by 12 January 2012. In accordance with this timeframe, the Commission presented its review of the European programme for critical infrastructure protection and Directive 2008/114/EC in June 2012 (SWD(2012) 190).

In the light of the modest initial outcome of the directive, the report raised the question as to whether 'the added value realised could not have been obtained through less resource-intensive means than a directive'. The Commission concluded that the implementation of the directive was uneven across Member States and had no tangible impact on ECI security levels. In particular, it generated only few new operator security plans, a fact closely linked with the low number of designated ECIs. On the positive side, it acknowledged that the directive facilitated effective CIP-related cooperation within and between Member States (though rather on a bilateral than truly European level) and that it generally led to greater CIP awareness.

The report noted that in certain transport subsectors, notably port facilities and airports, legal requirements at EU level comparable to the provisions in Directive 2008/114/EC had already been put in place. With regard to critical infrastructure sectors, one of the perceptions of the report was that the directive lacked a focus on dependencies within and between the sectors. Despite the Commission's announcement (COM(2011) 163 regarding critical information infrastructure protection) of its intention to discuss with Member States the 'ICT sector-specific elements to be considered for the review of Directive 2008/114/EC', the 2012 review contained no concrete references in this respect.

The Commission's new approach to EPCIP (2013)

Building on the 2012 review, the year after, the Commission put forward a 'new approach to the European programme for critical infrastructure protection' (SWD(2013) 318). It placed the focus on **interdependencies** between sectors, actors and individual critical infrastructures on the one hand, and on increased **resilience** of ECIs on the other, thereby expanding the (narrower) concept of protection. Resilience puts the emphasis on minimising the effects of ECI damage or loss in terms of security, services, and the economy. It involves contingency planning in response to threats in order to ensure minimum operations levels during interruptions and timely recovery.

To pilot the 'new approach' to critical infrastructure protection, four major pan-European infrastructures were selected:

- Eurocontrol (the European aviation organisation);
- Galileo (the European global satellite navigation system);
- the European electricity transmission grid; and
- the European gas transmission network.

The pilot project was designed to draw lessons from existing ECIs in order to improve risk assessment, contingency planning and training. It was set to conclude in 2017, however, no reports on the outcome could be identified.[3]

Comprehensive assessment of EU security policy (2017)

The 2017 comprehensive assessment of EU security policy (SWD(2017) 278), which reviewed all currently applicable EU policies and instruments in the area, included a critical appraisal of Council Directive 2008/114/EC. While it deemed the conceptual CIP framework to be of continued validity, it found that the directive had proved to be a 'useful, but not fully sufficient tool'. Considering the increasing level of interconnectivity, interdependence and complexity of critical infrastructures on EU territory, which also makes them more vulnerable, the limited scope of the directive (energy and transport sectors) was deemed a major shortcoming, 'minimising its impact'. The report also identified the 'limited character of the mandate given to the Commission' and the 'limited obligations' imposed upon the Members States as issues of concern.

It concluded that while the directive had brought benefits in awareness raising, exchange of good practice, and increased cooperation and coordination, its overall impact had remained 'more limited than initially expected'. In view of the low number of identified and registered ECIs (89 as per 2017), the report saw 'only limited progress' towards achieving the main objective of increased CIP. It noted that an 'unprecedented level of terrorist threat' and newly emerging threats (e.g. drones, insider infiltration, hybrid threats) put critical infrastructures EU-wide at risk and required an enhanced level of preparedness and response capabilities. Against this background, the report questioned whether the directive was 'the most appropriate tool to produce the expected benefits'. It suggested relaunching the discussion 'on the relevance and suitability' of the directive, and considering whether it could be 'repealed or replaced by a new legislative instrument, and complemented with additional enhanced voluntary measures'.

The report pointed at other, sector-specific CIP initiatives that have emerged in recent years, such as the NIS Directive (on security of network and information systems) and Decision 541/2014/EU regarding space surveillance. Furthermore, it recognised that many national and transnational CIP projects as well as dedicated research projects – many of which benefited from EU funding – had generated important outcomes, in particular as regards the development of tools and methodologies (common models, protocols, guidelines etc.), threat foresight, ECI stress testing and resilience of ECIs in specific threat scenarios.

Most recently, in its new security union strategy (COM(2020) 605), the Commission reiterated that the EU's existing framework for protection and resilience of critical infrastructures had 'not kept pace with evolving risks'. It highlighted the ever-increasing interconnectivity of infrastructures across

sectors, paired with the high dependence of most ECIs on digital infrastructure. In particular, it stressed the need for 'robust critical infrastructure protection and resilience measures, both cyber and physical', which implied 'the ability of a system to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events'.

Commission evaluation of the directive (2019)

The conclusions of the 2017 assessment of the EU's security policy prompted a fully-fledged evaluation of Directive 2008/114/EC, which the Commission presented in July 2019. The evaluation (SWD(2019) 308) was informed by an external study conducted by EY and RAND Europe.

The evaluation took into account those relevant CIP-related EU initiatives that had emerged in the years since the ECI Directive was enacted, above all the NIS Directive (2016). It found complementarities and certain overlaps, the latter however not being 'particularly onerous' for ECI actors at Member State level. Furthermore, it acknowledged that the nature of threats had evolved, as the 2017 comprehensive assessment of EU security policy had already stated. In addition, digital progress had to be considered, along with artificial intelligence. Both rendered critical infrastructures smarter, but at the same time, more vulnerable (e.g. if used by terrorists or hackers). In general, the evaluation found the narrow sectoral scope of the directive to be problematic, as critical infrastructures increasingly rely on services provided by the ICT and space sectors.

The evaluation examined Member States' transposition measures, which appeared to be uneven, and found the application of the ECI Directive to be heterogeneous across the EU. It pointed at striking geographical imbalances: most of the registered ECIs were located in central and eastern Europe, and 60 % of designated ECIs were located in only two Member States, which could only to some extent be explained by strategic considerations (e.g. the strategic role of some Member States in energy transmission/distribution networks).

With regard to risk assessment, the directive envisages the development of common methodological guidelines, the use of which would however be optional for Member States. The evaluation report mentioned the merits of the Commission's Joint Research Centre (JRC) in this respect, as it has authored a series of methodological reports.[4] Member States' reports to the Commission regarding risks, threats and vulnerabilities were described as very limited and difficult to compare, preventing the Commission from gaining an overview of the risks and threats at stake.

One weakness of the directive is that it takes national critical infrastructures as the starting point for identifying European critical infrastructures, as this approach fails to identify critical infrastructures that have a pan-European dimension per se (such as Galileo or Eurocontrol). Another issue addressed in the evaluation report is the lack of provisions regarding third countries. However, an external dimension comes into play where Member States have cross-border interdependencies in neighbouring third countries.

Globally, the EU and its Member States do not act in isolation on critical infrastructure protection, as in recent years international organisations have also stepped up their CIP efforts, notably with regard to cyber security, hybrid threats and energy grids. This concerns in particular NATO, the OSCE (Organisation for Security and Co-operation in Europe) and the OECD (Organisation for Economic Co-operation and Development), and on a global level, also the United Nations (notably its Office of Counter-Terrorism) and the International Organisation for Standards (ISO). In this respect, the evaluation looked into the coherence of the ECI Directive with international initiatives and concluded that while the directive is broadly speaking coherent with them, there is some overlap between the directive and certain OECD recommendations.[5]

Based on targeted consultations, the evaluation report concluded 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). Meanwhile, the focus should be one that includes elements of both protection and resilience […] The consultations with stakeholders clearly*

indicate that the option to revise the Directive is preferable to other solutions, including repealing the Directive and replacing it solely with regional cooperation or other 'soft law' approaches.

Figure 3 – Conclusions of the evaluation in the light of the 'better regulation' criteria

Evaluation criteria	Evaluation findings: the directive ...	Comments
Relevance	remains partially relevant	• The context and nature of threats have changed since the directive was adopted. • The sectoral approach taken is outdated. • The focus is on protection, whereas resilience is just as important.
Coherence	is broadly consistent with relevant sectoral legislation	• There are complementarities and certain overlaps, especially with the NIS Directive. • More could be done to exploit synergies. • There is coherence with international initiatives.
Effectiveness	is partially effective in achieving its objectives	• The procedure of identification and designation is not fully aligned across Member States. • The evaluation results as to whether the directive has raised the level of protection of ECIs are inconclusive.
Efficiency	*no conclusive evidence*	• *lack of quantifiable data*
EU added value	has EU added value	• Results could not have been achieved at national level. • Political momentum had been created on CIP. • Cross-border dialogue and cooperation between Member States had been encouraged.
Sustainability	has long-lasting effects	• Certain elements/structures would continue to exist even if the directive were to be repealed.

Data source: SWD(2019) 308.

3. Activities of the European Parliament

European Parliament resolutions

Resolution of 12 December 2018 on findings and recommendations of the Special Committee on Terrorism

In its resolution, the European Parliament deemed the sectoral approach taken by Directive 2008/114/EC to ECIs to be outdated and called for a revision, to consider the following elements:

- ensuring that designation of ECIs is carried out on the basis of an analysis of the systems supporting vital and cross-border services, rather than a sector-by-sector approach, taking due account of the importance of cybersecurity;
- defining 'operators of essential services' in line with the rules and procedures set out in the NIS Directive;

- enhancing the role of the Commission by allowing it to designate 'assets of pan-European services as ECIs';
- taking due account of interdependencies; and finally,
- creating an obligation for public and private operators of critical infrastructures to report incidents, conduct stress tests, provide appropriate training at the designated contact points, and establish quality requirements as regards business continuity plans, including operational plans, in the event of an incident or attack.

In addition, Parliament demanded that the designation of ECIs with an impact on more than one Member State should follow a multilateral process involving all of the potentially affected Member States.

Resolution of 3 October 2017 on the fight against cybercrime

In its resolution on the own-initiative report on cybercrime, Parliament stressed the importance of enhancing the resilience of critical infrastructures to cyber-attacks. In view of the growing number – and adverse effects – of cyber-attacks on industrial control systems and networks threatening the integrity of critical infrastructures (such as energy and electricity supply and financial structures), Parliament called on the Commission to continue identifying network and information security vulnerabilities of European critical infrastructures. It underlined that the fight against cybercrime should be primarily about 'safeguarding and hardening critical infrastructures and other networked devices, and not only about pursuing repressive measures'. Finally, Parliament called on the Commission 'to invest in the IT capacity as well as the defence and resilience of the critical infrastructure of the EU'.

Selected parliamentary questions

In the years following the directive's entry into force, a number of parliamentary questions – for example E-8498/2010, E-000720/2012, E-002050/2013 and E-002999/2013 – related to **cyber-security**, and in particular to EU plans and measures aiming to protect critical infrastructures against cyber-attacks. It was during this period that the EU shaped its first cyber security strategy (2013) and adopted the NIS Directive.[6]

The most recent parliamentary question relating to critical infrastructures was posed by Aldo Patriciello (EPP, Italy) in 2017 (E-000506/17). Against the backdrop of **earthquakes** and poor dam management, he inquired whether the Commission intended to 'draw up a list of major EU dams, classifying them according to risk', and to 'start cooperating with the operators of hydroelectric power plants to eliminate serious risks and provide assistance in the event of an emergency'. In his answer, Commissioner Vella referred to the Floods Directive (2007/60/EC) which established a framework for measures to reduce risks relating to flood damage, while pointing at the Member States' responsibility to manage flood risks and recalling the Union civil protection mechanism which can be activated in the event of disaster. The Commission explained that 'there is no list of hydroelectric power plants classifying them on a risk basis', thereby referring to Directive 2008/114/EC, as major dams may fall under its scope.

Concerns relating to **seismic risks** had already been voiced in earlier questions:

Maria do Céu Patrão Neves (EPP, Portugal; written question P-009125/2012) inquired whether the Commission intended to put forward a legislative framework requiring Member States to ensure minimum earthquake safety standards for ECIs. Furthermore, she asked about EU funding covering technical measures aimed at mitigating seismis risks. Commissioner Georgieva replied that safety in construction works was an exclusive competence of the Member States. However, the EU had financed the development of European construction standards, including a code on earthquake-resistant design of buildings and other civil engineering works (Eurocode 8). With regard to funding, she pointed at EU funding for risk prevention, including for programmes and projects dealing with seismic risks.

Eurocodes – i.e. non-binding standards applicable to buildings and civil works – were also the subject of a parliamentary question (E-006419/2011) posed by MEP Iannis Tsoukalas (EPP, Greece), who wondered whether major EU energy infrastructures were 'adequately protected against earthquakes'. Commissioner Oettinger explained that there were no plans to extend Eurocodes to energy infrastructure.

In the light of the **WikiLeaks affair** and, in particular, the 2010 leak of a classified US Department of State list of world-wide critical infrastructures ('**Cablegate**'),[7] Diogo Feio (EPP, Portugal) asked the Council in written question E-10802/2010 what impact the Council believed the disclosed information could have on the security of critical ('vital') European infrastructures. He also asked whether the Council thought a similar leak could occur in the case of confidential EU documents and whether the Council had taken special measures to protect those structures. The Council replied on 28 February 2011 that, in the context of Directive 2008/114/EC, the EU had taken 'a deliberate decision not to draw up a list of European critical infrastructure', 'in particular with a view to avoiding the potentially negative impact of possible breaches of confidentiality'. Therefore, the EU would 'not maintain such a list'.

In question E-009336/2012 Rachida Dati (EPP, France) observed that an increased level of threat to critical infrastructures (due to exceptional weather events and deliberate cyber-attacks) generated **costs and administrative burdens** for critical infrastructure operators, which could translate into price increases for the final energy consumers. The Member asked the Commission whether and how it planned to address guaranteeing fair prices for operators, while safeguarding consumer interests.

In the context of the privatisation of Polish **rail infrastructure assets**, which constitute 'an intrinsic part' of the critical infrastructures within the meaning of Council Directive 2008/114/EC, Dawid Bohdan Jackiewicz (ECR, Poland) asked the Commission (P-012504/2015) whether a change in ownership, resulting in a Member State's restricted influence over an integral part of the rail infrastructure, would have negative effects on the operation of critical infrastructures in Europe. He was wondering whether 'a Member State should not be able to keep the assets and the business separate in order to protect the integrity and functionality of the infrastructure'. In her reply, Commissioner Bulc clarified that the owner of a critical infrastructure can be a private entity, and that Directive 2008/114/EC did not include 'any restriction as regards ownership of the infrastructure'.

4. Council of the European Union

Council has also called for action, most recently in its conclusions of 10 December 2019 on complementary efforts to enhance resilience and counter hybrid threats. It emphasised that critical infrastructures are 'primarily a matter of national competence', however, 'the high degree of cross-border and cross-sectoral interdependencies' demanded coordination at EU level. Therefore, based on the Commission evaluation of Directive 2008/114/EC, Council invited the Commission to 'consult with Member States on a possible proposal for a revision of the Directive …, including potential additional measures to enhance the protection and resilience of critical infrastructure in the EU'.

5. Stakeholder positions

Reactions to the Commission evaluation

In response to the Commission evaluation, the Confederation of European Security Services (CoESS), which represents national associations of private security employers, issued a position paper, in which it expressed strong support for a number of conclusions reached by the evaluation:

- to widen the scope of the directive, thereby abandoning the sector-level approach;
- to provide more detailed definitions of key concepts;

- to provide greater detail in the definition and description of operator security plans and the roles and responsibilities of security liaison officers; and
- to raise the level of detail in Member States' risk assessments and reporting to the European Commission.

In addition, CoESS recommended establishing mandatory quality criteria for the procurement of security services. The organisation actively contributes to European standardisation work in this field, which is pursued by the CEN Technical Committee on Private Security Services (CEN TC 439).

Consultations in the context of the evaluation

Targeted consultations among core stakeholders contributed substantially to the evaluation's findings. In addition, the Commission solicited public input on two occasions: when it issued the evaluation roadmap in March 2018, and through a questionnaire-based public consultation conducted between November 2018 and February 2019.

In reaction to the roadmap, the European Federation of National Associations of Water Services (EurEau), the representative organisation of national drinking and waste water service providers, emphasised that water is deemed a critical infrastructure in all Member States. However, due to the lack of cross-border connections between national water service networks it considered the definition of ECI not applicable to the water sector and hence recommended not to include the water sector into the scope of a revised ECI Directive.

Microsoft suggested that, rather than including the ICT sector, the directive should focus on 'issues of hybrid conflict that are beyond the scope of the NIS Directive'. In this vein, it also advocated advancement of 'international norms that regulate hybrid conflict in times of peace'.

The Commission's public consultation yielded 69 responses, almost half of which came from businesses and their associations. The respondents identified cyber attacks and energy supply risks as the most important threats to critical infrastructures, followed by natural disasters, attacks by state-sponsored actors and terrorist attacks. A majority of respondents deemed the effectiveness of Directive 2008/114/EC as being hampered by the exclusion of the ICT sector, and expressed doubts about the Directive's sectoral scope.

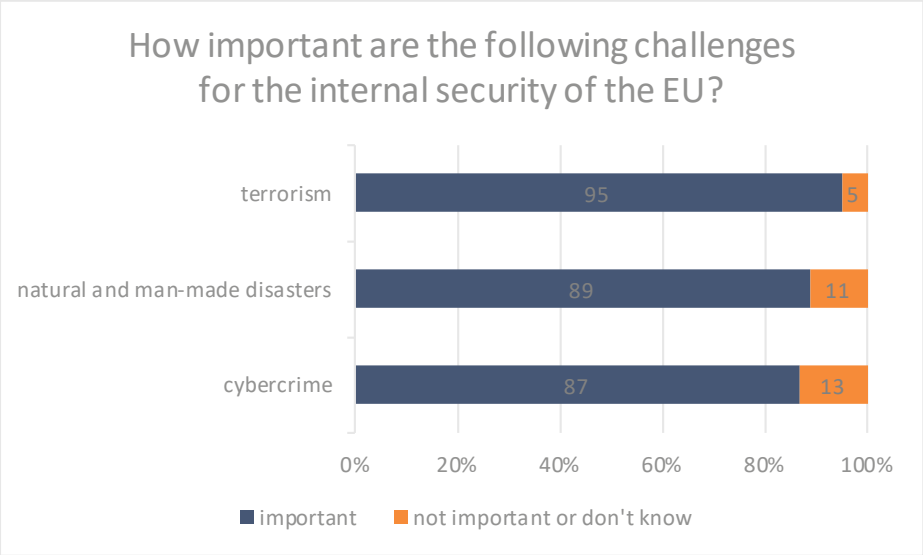
The Commission received also two position papers, one from a national authority and the other from a business organisation:

- The Estonian Ministry of the Interior expressed the view that the protection and continuity of electronic communication services in emergency/crisis situations required further regulation; however, this should be done outside the ECI Directive.
- The European Organisation for Security (EOS), which represents the European security industry and research community, recommended defining common EU criteria for the identification of ECIs, to prevent critical infrastructures on a European scale from not being protected under the directive because of Member States' failure to identify them as ECIs. Emphasising the vital role of research and innovation in the area of critical infrastructures, it proposed establishing a European Competence Centre, to be connected to a network of national competence centres.

6. Public perception

A special **Eurobarometer survey** conducted in 2017 explored the attitude of the European public towards the EU's internal security. An overwhelming majority of respondents deemed terrorism, cybercrime, and natural and man-made disasters to be core security challenges. Of these three categories, respondents expressed greatest concern about terrorist threats (95 %), followed by natural and man-made disasters (89 %).

Figure 4 – Public perception of internal EU security



Data source: Eurobarometer, 2017.

Originally, this specific Eurobarometer survey was undertaken in 2011; it was subsequently repeated in 2015 and 2017.[8] Response patterns varied only marginally over the years, with terrorism continuing to rank as top challenge. However, what did change was the weighting: while in 2011, 58 % of respondents considered terrorism a 'very important challenge' and 33 % a 'fairly important challenge', by 2017 the proportion of respondents considering it 'very important' had risen to 76 %.

7. Revision of the ECI Directive

On 16 December 2020, drawing on the evaluation's findings, the Commission presented a new proposal for a directive on the resilience of critical entities (COM(2020) 829), together with the supporting impact assessment. In view of the importance of cybersecurity for the resilience of critical entities, the Commission submitted in parallel also a proposal for a revised NIS Directive ('NIS 2'). To ensure full coherence, cyber-resilience obligations under NIS 2 would apply also to critical entities identified under the new proposal.

The proposal on critical entities itself reflects a switch from the current approach focusing on the protection of individual assets towards strengthening the resilience of the critical entities that operate them.

While the all-hazards approach of the existing directive remains valid, the new proposal embraces today's complex realities, by considering:

- a broad range of risks, including natural hazards, state-sponsored hybrid actions, terrorism, insider threats, pandemics, and (industrial) accidents;
- new technologies, such as 5G and drones; and
- an interconnected approach, as hazards may generate cascading effects on service provision in other sectors and across borders.

The proposal would require each Member States to adopt a national strategy to reinforce the resilience of critical entities and to undertake regular risk assessments. The procedure of identifying critical infrastructures would be different to that set out in Directive 2008/114/EC. Another novel element in the proposal would be that the Commission would have specific oversight over critical entities of particular European significance, granting it a more central role than under the current procedure.

Another striking difference as compared with the existing 2008 directive is the proposed sectoral expansion. The proposal broadens the directive's scope to include banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, public administration and space, alongside with energy and transport.

MAIN REFERENCES

Erbach G., Cybersecurity of critical energy infrastructure, EPRS, European Parliament, 2019.

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

ENDNOTES

1 Council document 15616/08 of 13 November 2008.

2 According to the Commission evaluation, as per August 2018, 88 ECIs related to energy, and 5 to the transport sector.

3 Although the Commission evaluation includes a reference to the pilots, there is no explicit mention of their outcomes.

4 These include, for instance, 'Risk assessment methodologies for critical infrastructure protection' (2012 and 2015).

5 For details see SWD(2019) 308, footnote 51.

6 A new EU cybersecurity strategy was presented in December 2020 (JOIN(2020) 18), together with a proposal for a revised NIS Directive (Directive on measures for high common level of cybersecurity across the Union, COM(2020) 823).

7 This aspect of WikiLeaks is summarised in D.G. Arce, 'WikiLeaks and the risks to critical foreign dependencies', *International Journal of Critical Infrastructure Protection*, Vol. 11, December 2015, pp. 3-11.

8 Eurobarometer surveys 'Europeans' attitudes towards security', SP464b (2017) and SP432 (2015); 'Internal security', SP371 (2011).

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)
www.eprs.ep.parl.union.eu (intranet)
www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)