EOS Position Paper

on a

Open Public Consultations as part of the 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

February 2019

The European Organisation for Security (EOS), as the representative of the European Industrial and Research Security Community, believes the European Critical Infrastructure Directive (ECI Directive) has helped to emphasize the importance of a robust and resilient protection of Critical Infrastructures (CI). However, EOS believes that, in assessing the follow-up to the directive, the Commission should take into account some considerations as described in the following position paper that will go together with EOS’ reply to the Public Consultation.

THE BACKGROUND

The ECI Directive is one pillar of the European Programme for Critical Infrastructure Protection (EPCIP). The latest review of the ECI Directive done in 2012 has identified a number of deficiencies, including a limited and uneven application of the ECI Directive on the part of the Member States; as well as, a narrow sectoral scope that was not aligned with the systematic approach to critical infrastructure used in many Member States. Building on those outcomes, and in light of the conclusions of the 2017 Comprehensive Assessment of EU Security Policy, the Commission has launched an evaluation of the ECI Directive.

THE CHALLENGES AND RELATED RECOMMENDATIONS

The current text of the directive fails to take into consideration a common level of Critical Infrastructure protection 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.

• EOS recommends that 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 current text of the directive focuses on critical infrastructures the disruption or destruction of which would have significant cross-border impact. The directive requests the EU Member States to perform an assessment aimed at the identification and designation of the European Critical Infrastructures. Member States must go through a cooperative designation process of identifying potential ECIs. As a matter of fact, this approach has shown not to be the optimal route to ensure a EU-wide level of protection. The identification process has proved to be slow while the increasing interconnection and interdependence among infrastructures requires a more integrated approach across Europe.

• EOS recommends the definition of a set of common EU criteria to evaluate the status of a European Critical Infrastructure, independently from a single Member State evaluation. These criteria should be elaborated and applied across the EU to avoid situations whereby a critical infrastructure is not adequately protected, notwithstanding its potential for cross-border impact, because a single Member State has failed to identify it as such.
Finally, **EOS would like to underline the importance of Research, Development and Innovation (RD&I) in the field of Critical Infrastructures.** The ECI Directive is focused on building a strong Critical Infrastructure protection across the EU, that can withstand a wide range of threats. To achieve the desired levels of protection, what is needed is a robust innovation ecosystem across the EU, as well as sufficient incentives to innovate. The initiative taken in the cybersecurity domain with the proposal to create a network of National Competence Centres coordinated by a European Competence Centre provides an interesting model, including the proposed legal basis, that can be replicated in the CI protection domain.

- **EOS promotes the idea to constitute a EU Critical Infrastructure Competence Centre connected to a network of Member State Critical Infrastructure Competence Centres.** EOS believes it would be appropriate to take inspiration from what has been proposed in the cybersecurity domain by establishing National Competence Centres connected through a coordinating European Competence Centre. In this way, Member States can 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. The EU Critical Infrastructure Competence Centre should be founded on the same legal basis as the cybersecurity one, in order to ensure that both research and industry competitiveness are taken into account.