Position Paper

Confederation of European Security Services

Position Paper on the Evaluation of Council Directive 2008/114

Commission Staff Working Document (2019) 308

Summary

Critical infrastructures are, by definition and nature, crucial to the good functioning of States and their economies. Therefore, incidents affecting them can have severe, cross-border, consequences on many aspects of EU citizens' lives, potentially affecting their safety and security. What is more, as noted in the United Nations (UN) Security Council resolution 2341 (2017) on the protection of critical infrastructure against terrorist attacks, there are "*increasing cross-border critical infrastructure interdependencies between countries*" in a large number of sectors.

The Confederation of European Security Services (CoESS) therefore highly welcomes the recommendations of the European Commission's Evaluation of *Council Directive 2008/114*, published in the Staff Working Document (2019) 308 (***SWD (2019) 308***). CoESS sees in Directive 2008/114 an important milestone for providing an EU framework for cross-border cooperation in Critical Infrastructure Protection (CIP). The SWD (2019) 308 however describes significant shortcomings that have been addressed by CoESS in the preceding public consultation, and in its White Paper Critical Infrastructure Security and Protection – a Public-Private Opportunity. As a consequence, CoESS recommends a revision of Directive 2008/114 on the following matters, which it believes would be of clear EU added value, while respecting Member States' competence in CIP:

1. Create an EU framework that takes into account current and emerging ***threats*** against European Critical Infrastructure (ECI) on an ongoing basis.
2. Extend the Directive's ***scope*** from a sector- to a system-focused approach.
3. Provide a more precise and practical ***definition*** of ECI identification, Operator Security Plans (OSPs), Security Liaison Officers (SLOs), and reporting responsibilities in coherence with the Directive on Security of Network and Information Systems (NIS Directive).
4. Establish a CIP framework that fosters ***public-private partnerships***.
5. Prescribe mandatory compliance for private security services protecting ECI with **European Standards**, where applicable.
6. Enforce best value ***procurement*** for private security services protecting ECI.
7. Limit private operators' ***liability*** for acts of terrorism against ECI.

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Jan Bogemansstraat | rue Jan Bogemans 249 | B-1780 Wemmel Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **coess.org**

This Position Paper will refer to the findings of the SWD (2019) 308, and provide additional information on the aforementioned recommendations. The latter are in line with the Report on findings and recommendations of the European Parliament's Special Committee on Terrorism, published in November 2018, and the UN Security Council resolution 2341 (2017).

CoESS Recommendations

CoESS' recommendations in the framework of a revised Directive 2008/114 (1) are driven by the motivation to improve the ECI's level of protection and (2) to create a more relevant and effective horizontal framework for the identification and designation of ECIs, including clearly defined, similar responsibilities and common procedures applying to all ECI stakeholders.

1. Create an EU framework that takes into account the current and emerging threats against critical infrastructure on an on-going basis

CoESS recommends that a revision of Directive 2008/114 creates an updated EU CIP framework that is responsive to current and emerging threats against critical infrastructure and provides clear EU added value. In line with this recommendation, the UN Security Council resolution 2341 (2017) on the protection of critical infrastructure against terrorist attacks encourages "*all States to make concerted and coordinated efforts, including through international cooperation, to raise awareness, to expand knowledge and understanding of the challenges posed by terrorist attacks, in order to improve preparedness for such attacks against critical infrastructure*".

Since the adoption of Directive 2008/114 in 2008, many new threats and challenges for CIP emerged, which led to the rightful conclusion of the SWD (2019) 308, namely that the Directive is only partially relevant. Drones, cyber risks, Insider Threats, CBRN-E and evolved terrorist modus operandi require an enhanced level of protection and resilience of critical infrastructure. Airports across the EU already suffer from drone intrusions. Cyber attacks like WannaCry and NotPetya in 2017 were launched as a "campaign" against multiple infrastructures in different countries. In 2015, a car crashed into a chemical plant in Lyon/France, which could have resulted in the release of dangerous materials. In 2016, two Belgian nuclear power plants were shut down due to a suspected ISIS infiltration. Also, the SWD (2019) 308 correctly states that "*the increasingly intertwined, trans-boundary and 'wired' nature of Europe's critical infrastructure and the services that they together provide would gradually reduce the Directive's relevance*".

In a revision of Directive 2008/114, these developments must not only be accounted for. It is important that the EU fosters a common understanding among ECI operators of these challenges. A revision must ensure that they are addressed on an on-going and dynamic basis in the cross-border exchange of information and reporting; common standards for vulnerability and risk assessments;

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Jan Bogemansstraat | rue Jan Bogemans 249 | B-1780 Wemmel Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **coess.org**

ECI's security plans; and trainings and qualifications of personnel involved in the operation and protection of ECI, including public and private forces. As the SWD 308 correctly states, "*the EU's approach to CIP must be a flexible, risk-based one that corresponds to the spectrum of current and future threats and vulnerabilities facing Europe's critical infrastructures*".

2. Extend the Directive's scope from a sector- to system-approach

CoESS recommends that a revised Directive 2008/114 has a broader scope, which does not focus on the protection of isolated assets and sectors, but takes into account the entire system of existing critical infrastructures and respective interdependencies.

Such a broadened scope would allow for a more correct, coherent and comprehensive designation of ECI and a governance system that avoids the duplication of efforts at national level and mirrors the interdependencies of today's critical infrastructures. For example, the scope of Directive 2008/114 currently does not account for an attack on the energy, financial or telecommunication sectors, which could have severe cascading effects across sectors and Member States.

CoESS' recommendation is supported by the Report on findings and recommendations of the European Parliament's Special Committee on Terrorism, which states that a revision of Directive 2008/114 must ensure that the 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. Also the SWD (2019) 308 states that "*the narrow scope of the Directive, which is limited to the energy and transport sectors, does not fully account for the nature and extent of the cross-sectoral interdependencies that currently exist as compared to when the Directive was adopted*".

CoESS therefore strongly supports the statement of SWD (2019) 308 that there are grounds to examine the scope of the EU's CIP policy framework to encompass additional sectors from a system- instead of asset-focused perspective that emphasises interdependencies between different critical infrastructures in different sectors.

3. Provide a more precise and practical definition of ECI identification, OSPs, SLOs, and reporting responsibilities in coherence with the NIS Directive

CoESS recommends that a revision of Directive 2008/114 creates a more precise, practical, and shared definition of:

- **Criteria and procedures used for the multi- and bilateral identification and designation of ECI;**
- **Minimum requirements for Operator Security Plans (OSP);**

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Jan Bogemansstraat | rue Jan Bogemans 249 | B-1780 Wemmel Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **coess.org**

- **Qualifications, roles, responsibilities and vetting standards of Security Liaison Officers (SLO);**
- **Reporting requirements of Member States to the European Commission.**

This is supported by the SWD (2019) 308, which concludes that the very general definitions of these matters in the Directive provide a valuable foundation for a common CIP framework and identification of critical infrastructure and ECI, but are also responsible for the very diverse interpretation and transposition of the text. According to the SWD (2019) 308, this has limited the Directive's ability "*to achieve the EU-wide 'common approach' to ECI identification and designation*".

Therefore, the revision of Directive 2008/114 should establish more descriptive and clear criteria for the identification and designation of ECI than currently done in Article 3, 4 and Annex III – building up on Point 2 of this Position Paper regarding the scope. CoESS recommends that this is done in coherence with the Network and Information Security (NIS) Directive (2016/1148) and the findings of the Report COM (2019) 546 assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of the NIS Directive:

- The list of ECI sectors in Annex I of Directive 2008/114 should be aligned with Annex II of the NIS Directive.
- Article 3 of Directive 2008/114 should be aligned, where appropriate, with Articles 5 and 6 of the NIS Directive.

CoESS also recommends that the European Commission further reviews whether the existing CIP Expert Group at EU level effectively fulfils the same objectives as the NIS Directive Cooperation Group among Member States, namely to ensure a consistent and harmonised identification of ECI; to facilitate cooperation in the multi- or bilateral designation of ECI; to align cross-cutting criteria thresholds among Member States; to allow regular reviews of designated ECI; and to publish sector-specific reference documents to help the identification of ECI. Also, in view of the fact that a number of critical infrastructures are owned, operated by, or in cooperation with, private stakeholders, it would make sense that the private sector be pro-actively involved in the work of this CIP Expert Group.

This enhanced coherence with the NIS Directive is in line with the recommendation of the European Parliament's Special Committee on Terrorism for a revision of Directive 2008/114 "*to provide similar rules and procedures for 'operators of essential services' as in the NIS Directive*", and of SWD (2019) 308 to "*assess the potential advantages of aligning CIP and NIS policy so as to ensure*

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Jan Bogemansstraat | rue Jan Bogemans 249 | B-1780 Wemmel Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **coess.org**

enhanced complementarity between cyber and physical protection measures relating to CI in different sectors".

In addition, OSP provisions for ECI in Directive 2008/114, including Annex II, should be defined as "minimum requirements" and include public-private partnerships (see Point 4) and recovery measures that can prevent a "cascading" effect of an incident to other sectors and Member States. Furthermore, a revised Directive should clearly define roles and responsibilities, as well as minimum qualifications and vetting standards for SLOs at ECIs.

According to the SWD (2019) 308, today's differences in application and transposition at national level have generated different costs for some operators of ECI and therewith distortion of competition with negative impacts on the Internal Market. It is therefore important that reporting to the European Commission is bound to clear definitions of information, which shall be provided by Member States, to the extent that the Commission is able to effectively track the Directive's implementation by the Member States. The establishment of an efficient monitoring and evaluation framework is crucial for a revised Directive to be relevant, effective, coherent and sustainable.

4. Establish an updated CIP framework that fosters Public-Private Partnerships

CoESS recommends that a revision of Directive 2008/114 ensure that private operators are closely involved in the designation of ECI insofar as they own and/or operate them. The SWD (2019) 308 confirms that "*there are no provisions in the Directive for private CI owners/operators to feed into the work of identifying ECI*". CoESS believes this is a serious shortcoming, as it is the nature of the critical infrastructure that requires it to be under special protection, not depending on who owns it or who operates it.

Further, the revision should create a framework in the ECI OSP Procedure in Annex II, which makes reference to the need for both operators and contracted private security companies to receive clear instructions on roles and responsibilities in CIP missions, and to have competences in the development of OSPs (with respect to national legal frameworks).

According to the United Nations Security Council Report (2017) on "Physical Protection of Critical Infrastructure against Terrorist Attacks", more than 80% of critical infrastructure of Western States are owned and operated by the private sector. It is foremost private operators that are responsible for CIP and investments in physical protection, including the procurement of private security services. Public-private partnerships that establish frameworks for the exchange of information and the set-up of OSPs, clear rules and responsibilities for public and private stakeholders are therefore crucial for effective CIP.

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Jan Bogemansstraat | rue Jan Bogemans 249 | B-1780 Wemmel Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **coess.org**

CoESS' recommendation is supported by Security Council resolution 2341 (2017) on the protection of critical infrastructure against terrorist attacks, which calls on countries "*to establish or strengthen national, regional and international partnerships with stakeholders, both public and private, as appropriate, to share information and experience in order to prevent, protect, mitigate, investigate, respond to and recover from damage from terrorist attacks on critical infrastructure facilities, including through joint training, and use or establishment of relevant communication or emergency warning networks.*" Also the recommendation of the European Parliament's Special Committee on Terrorism advises "*that the private sector be involved when devising programmes for the protection of critical infrastructure and soft targets, including in the context of cybersecurity" and "highlights the need to develop public-private dialogues to this effect*".

CoESS recently published White Paper on the Security Continuum, which includes best practice and guidelines for public-private partnerships. Further recommendations for public-private partnerships in CIP are also assembled by the UN Security Council "Compendium of Good Practices for the Protection of Critical Infrastructures against Terrorist Attacks", published in 2018.

5. Prescribe mandatory compliance of private security companies protecting ECI with European standards, where applicable

CoESS recommends that private security companies that protect ECI be obliged to comply with the relevant European (CEN/CENELEC) and International (ISO/IEC) Industry Standard(s). Whilst two European standards already exist, which list the quality criteria for security services suppliers for Aviation and Airport environments (EN16082:2011) and for Maritime and Port environments (EN16747:2015), CEN TC 439 "Private Security Services" is working on an overarching standard for security services supplied in any type of critical infrastructure (prEN17483), which is supposed to be adopted by Q4 2020. In the future, the TC intends to address other critical infrastructure sectors, such as energy, healthcare/hospitals and water supply in "vertical" standards. The existing standards, as well as the draft critical infrastructure horizontal standard and the future vertical standards maintained and developed by the CEN Technical Committee 439 on Private Security Services, are a highly efficient way to ensure the provision of qualitative private security services for CIP across Europe. They are designed by specialists from the industry and are therefore credible and widely approved means to specify service requirements for quality in organisation, processes, personnel (incl. training and vetting), Insider Threat policies and management of a security service provider.

The ways in which critical infrastructures are currently secured and protected vary in the European countries from a mixture of state authorities (police, specialist protective services and occasionally the military), in-house private security officers, to fully contracted out to private security

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Jan Bogemansstraat | rue Jan Bogemans 249 | B-1780 Wemmel Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **coess.org**

companies. Private security companies provide a wide range of guarding and surveillance services for all kinds of critical infrastructures – including for example nuclear plants, water supply systems, government buildings, healthcare facilities, maritime ports, aviation / airports and other public transport means and hubs. It is undoubtedly a development in Europe that the CIP tasks are increasingly contracted to the private security sector. Due to this trend, it is of high importance that private security services comply with the highest quality standards – specifically in CIP.

CoESS' recommendation is supported by the recommendation of the European Parliament's Special Committee on Terrorism, which "*calls on the Commission to propose a European Certification Initiative for private security companies, aiming to specify the requirements and conditions under which they can operate within the critical infrastructure environment*".

6. Enforce Best Value Procurement for Private Security Services protecting ECI

In order to further improve CIP, at least 60% of criteria in the procurement tenders for private security services for ECI should mandatorily be based on quality. CoESS' view is that only private security companies of the highest quality should be able to offer CIP services.

Low-cost focused procurement in the private security sector can have very far-reaching consequences, especially in CIP. When qualitative criteria, e.g. related to training and working conditions of staff are not met, this can lead to very serious risks to public safety and security, let alone the critical infrastructure's performance itself. Low-cost focused procurement leads to a destructive race to the bottom in the provision of qualitative security services. It provides incentives for non-respect of labour law, non-compliance with legislation, and compromised contract performances. This is why in Spain for example, national law foresees that quality criteria must represent at least 51% in the awarding process of all private security services. CoESS believes that for CIP, this threshold should be even higher at 60%. The Best Value Guide for the private security sector, developed by CoESS and our Social Partner UNI Europa with the help of EU funding, provide important guidelines for the definition of quality criteria in private security services in CIP.

CoESS' recommendation is in line with the recommendation of the European Parliament's Special Committee on Terrorism, which states that "*whereas private security services play a role in ensuring resilient security chains, public procurement of their services should therefore be subject to specific quality criteria, with regard to aspects such as the training, vetting and screening of personnel, quality control and compliance assurance, and the implementation of technological developments and contract management*".

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Jan Bogemansstraat | rue Jan Bogemans 249 | B-1780 Wemmel Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **coess.org**

7. Limit private operators liability for acts of terrorism against ECI

CoESS recommends that the liability of private operators of ECI and private security services protecting ECI in case of a terrorist attack, be limited by a clear legal and contractual framework. This is becoming ever more urgent as current and emerging threats such as cyberattacks and CBRN-E attacks can have increasingly catastrophic and cascading consequences, both across sectors and Member States.

Private operators of ECI and private security companies protecting ECI should not bear unlimited liability further to acts of terrorism. Today, private entities are in many countries not able to face possible third parties' claims in the event of an incident, which could relate to amounts exceeding available insurance coverage – leading to professional operators being unable to manage ECI and professional security providers dropping out of calls for tenders.

Brussels, 06 January 2020

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Jan Bogemansstraat | rue Jan Bogemans 249 | B-1780 Wemmel Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **coess.org**