FEEDBACK

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the resilience of critical entities

2020/0365 (COD)

The European Organisation for Security (EOS), as the representative of the European Industrial and Research Security Community, welcomes the Commission initiative of renewing an EU approach to Critical Infrastructure protection.

The proposed directive acknowledges the evolution of threats that Member States (MS) must face, as well as the interconnected and cross-border nature of European Critical Infrastructure (ECI). EOS approves of the widening of the sectoral scope that will fall under the Directive. In the current sanitary situation for instance, healthcare facilities face an increasing number of threats and must therefore be included within the list of critical entities. Likewise, the digital aspect cannot be disregarded when addressing the resilience of ECIs. That is why EOS strongly supports the synergies with the NIS 2 Directive. In fact, the resilience of critical entities can only be ensured through a joint cyber-physical approach.

Positively, the NIS 2 Directive also acknowledges the importance of managing supply chain and supplier-related cybersecurity risks when used by essential and important entities, but the Critical Entities Directive proposal regrettably lacks references to ensuring supply chains contribution to the resilience of the entities they supply to. We would stress that the resilience of critical entities can only be assured when supply chains are clearly controlled and bound to the same requirements, and call for legislators to take this into account when adopting the proposal.

From a legal basis, EOS endorses the reliance of the proposed directive on Art.114 TFEU. This allows, in EOS opinion, for a better level playing field, which in turn contributes to defragment the European market of technology solutions aimed at the protection of infrastructures. Market defragmentation is key to fostering a sustainable European strategic autonomy in security technologies. Linked to this is the need for an alignment of practices and standards among MS. EOS recommended in the past the adoption of a set of common EU criteria for the definition of ECIs. The procedure provided by this directive, which enables MS to identify critical entities using common criteria on the basis of a national risk assessment, together with Annex 1, are a steppingstone in that direction.

Finally, EOS welcomes Art.11 (1) underlining the need of ECIs to ensure adequate protection of defined facilities thanks to technological solutions. EOS believes that research and innovation activities, and most importantly their link with actual capabilities development and procurement, are key to providing such solutions. EOS hence encourages decision-makers to prepare the ground for European programmes aimed at the protection of critical entities. The implementation of such programmes at a European scale, making use of both national and European funds, will allow not only to defragment the security market, but also to ensure a better uptake of EU research results, in particular in critical domains such as cybersecurity, artificial intelligence and secure communications.

Within this approach, the close collaboration of public and private entities, including MS authorities, industry and research centres, is a prerequisite. Only by including all these relevant actors will it be ensured that critical entities take the most suitable technical and organisational measures for their resilience, as per Art.11. EOS therefore suggests that the announced Critical Entities Resilience Group (Art.16) assumes the role of a platform committed to fostering a robust innovation ecosystem based on information sharing between relevant national competence centres – including industry and RTOs.