Resilience of critical entities

Protecting critical infrastructure against physical and digital threats is more than ever high on the EU agenda, not least in the light of the recent Nord Stream gas pipelines sabotage. During the November II plenary session, the European Parliament is due to vote on a provisional agreement on rules to enhance critical entities' resilience.

Background

Critical infrastructure is not only exposed to natural disasters and severe weather events, but also targeted in hybrid attacks by hostile state and non-state actors. In the EU and its internal market, increasing interconnectivity of key infrastructure, networks and providers of essential services leads to an urgent need for coordinated efforts to reduce vulnerabilities. It also requires shifting the focus from protecting specific assets towards strengthening the resilience of the critical entities that operate them. To respond to these challenges, the European Commission proposed to review the 2008 Directive on European critical infrastructure, establishing a procedure for its identification and a common approach to its protection.

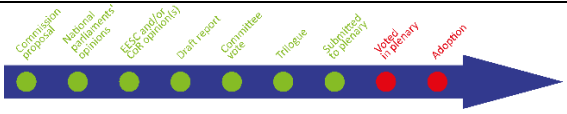
European Commission proposal

The Commission proposal for a directive on the resilience of critical entities (CER) expands the scope of the current rules, which only apply to energy and transport, to cover 10 sectors: energy, transport, banking, financial market infrastructure, health, drinking water, waste water, digital infrastructure, public administration and space. The proposal seeks to establish an all-hazards framework to support Member States in ensuring that critical entities are able to prevent, resist, absorb and recover from disruptive incidents, be they caused by natural disasters, accidents, terrorism, insider threats or public health emergencies such as pandemics. Member States would have to identify and list critical entities, adopt a national strategy, and carry out regular risk assessments, while the entities would have to conduct their own risk assessments, take resilience measures, and report disruptive incidents. The proposal also envisages on-site inspections and penalties for non-compliance. Entities of particular European significance – those providing essential services to, or in more than, one third of Member States (i.e. nine) – would be subject to specific oversight. The CER proposal, focusing on resilience against physical risks, was presented together with the review of the Network and Information Security Directive (NIS2), which aims to enhance cyber-resilience. To ensure alignment, NIS2 provisions would apply to all critical entities identified under the CER.

European Parliament position

In the European Parliament, five committees have been working on the proposal, with the Committee on Civil Liberties, Justice and Home Affairs (LIBE) taking the lead. The LIBE committee adopted its report on 15 October 2021. The Council agreed its general approach on 20 December 2021. The political agreement reached by the co-legislators on 28 June 2022 in the end covers 11 sectors (with the addition of the food sector) and include public administration entities, except for the judiciary, parliaments and central banks. As wished for by the Council, a clause allows Member States to exclude entities active in defence, national security, public security and law enforcement from obligations. Parliament negotiators ensured that the scope covers systems safeguarding the rule of law, and that the thresholds for entities to qualify as being of particular European significance is lowered to six or more Member States (instead of nine). Member States will need to transpose the new rules into national law within 21 months.

First-reading report: 2020/0365(COD); Committee responsible: LIBE; Rapporteur: Michal Šimečka (Renew, Slovakia).



EPRS | European Parliamentary Research Service

Author: Sofija Voronova, Members' Research Service

PE 738.212 – November 2022