Cyber solidarity act

In April 2023, the European Commission proposed a regulation to strengthen solidarity and capacities in the EU to detect, prepare for and respond to cybersecurity threats and incidents ('cyber solidarity act'). During its April II part-session, the Parliament is set to vote on the agreement reached in negotiations with the Council.

Background

Russia's war on Ukraine has revealed the extent of our dependence on digital technology and the fragility of the digital space. It has triggered a surge in cyber-attacks that have been particularly disruptive when targeting critical infrastructure – such as energy, health or finance – increasingly reliant on technology, which renders it more efficient but also more susceptible to cyber disruption. Against this backdrop, the Commission has proposed a regulation on a cyber solidarity act that would address the urgent need to strengthen solidarity and capacities in the EU to detect, prepare for and respond to cybersecurity threats and incidents. Funding for the establishment of a cybersecurity alert system ('cyber shield') and of a cyber emergency mechanism supporting preparedness actions, including a cybersecurity reserve, would be provided by amending the Digital Europe Programme (DEP) Regulation.

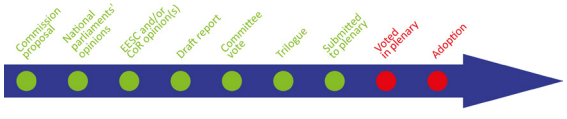
European Parliament position

Parliament's Committee on Industry, Research and Energy (ITRE) adopted its report in December 2023, along with a mandate to enter into interinstitutional negotiations. Likewise, the Council agreed its position in December 2023. The co-legislators reached a political agreement on the text in March 2024. The agreed text maintains the initial Commission proposal's components while clarifying and expanding certain definitions and aligning provisions with existing legislation, namely the Directive on the security of network and information system (NIS2), to avoid duplication. The regulation would thus be based on three pillars:

- a pan-European **cybersecurity alert system**, consisting of an infrastructure network of '**cyber hubs**', both **national** (single entities established by and acting under the authority of a Member State, which may cooperate with private sector entities) **and cross-border** (consisting of a hosting consortium composed of at least three participating Member States), that will share information on cyber incidents to strengthen joint resilience;
- a **cybersecurity emergency mechanism**, comprising a **cybersecurity reserve** – a pool of private companies (including non-EU actors) offering support for Member States (and certain third countries) on request, to assist them in the event of a significant or large-scale cyber incident;
- a **cybersecurity incidence review mechanism** by which the EU Agency for Cybersecurity (ENISA), at the request of the Commission or the Cyber crisis liaison organisation network (EU-CyCLONe), reviews and assesses threats, known exploitable vulnerabilities and mitigation actions of significant or large-scale incidents, delivering an incidence review report with lessons learned.

Parliament secured the addition of development of workforce skills, capabilities and competencies to the proposal's specific objectives, and an increased role and resources for ENISA, in particular with regard to the EU cybersecurity reserve. Parliament also secured that funds earmarked for the cybersecurity reserve would not jeopardise other DEP objectives, such as digital skills and artificial intelligence.

First-reading report: 2023/0109(COD); Committee responsible: ITRE; Rapporteur: Lina Gálvez Muñoz (S&D, Spain). For further information see our 'EU Legislation in progress' briefing.



Outcome of the Conference on the Future of Europe: This proposal is relevant for measures 28(1), (2); 33(3).

EPRS | European Parliamentary Research Service
Author: Polona Car, Members' Research Service
PE 760.431 – April 2024