Funded by the European Union

# CYBERSECURITY SOLIDARITY ACT

## Policy brief

| | |
|---|---|
| **Weblink** | http://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity |
| **Relevance** | ☐ National policy x EU policy ☐ other: ________________ |
| **Briefing done by** | Mélina Di Matteo, UWE |

## Short summary of the policy

Adopted by the European Commission in April 2023, the Cybersecurity Solidarity Act entered into force on 4 February 2025. The Act strengthens the EU's collective ability to detect, prepare for, and respond to large-scale cyberattacks. Aimed at closing the gaps in cooperation and responsiveness to cross-border cyber threats – including those targeting critical infrastructure – it comes against a backdrop of growing geopolitical tensions and hybrid threats.

The text proposes a strengthening of the European cybersecurity framework through the creation of new operational structures and instruments, in particular:

- The **Cybersecurity Emergency Mechanism** to improve preparedness, support mutual assistance, and enable the deployment of capacities such as Cyber Rapid Response Teams.
- Support for the **deployment of interconnected SOCs**, forming the European Cyber Shield.
- A **cybersecurity reserve** of pre-qualified service providers, rapidly mobilized to support Member States in the event of major cyber incidents.

The Act also aims to improve resilience through coordinated penetration testing, joint response exercises, and enhanced information sharing between national authorities, European institutions, and the private sector.

## Main objectives of the policy

- Detect cyberthreats rapidly through an EU-wide network of SOCs.
- Enable a coordinated and collective response to major cross-border cybersecurity incidents.
- Strengthen solidarity between Member States through coordinated response mechanisms.
- Improve preparedness for cyber crises (exercises, assessments, joint responses).
- Create a pool of cybersecurity services that can be mobilized in the event of an incident.
- Increase operational cooperation between Member States, ENISA, and the Commission.

## Context and relation to the Digital Europe Programme (DEP)

In general, DEP supports the implementation of the Cybersecurity Solidarity Act by funding actions that improve detection, preparedness, and coordinated responses to large-scale cyber incidents across the EU:

| CYBERSECURITY SOLIDARITY ACT | DEP |
|---|---|
| **European Cyber Shield** | Funds the deployment and interconnection of SOCs to enable real-time threat detection and rapid coordinated responses. |
| **Cybersecurity Emergency Mechanism** | Supports preparedness actions, mutual assistance mechanisms, and the establishment of Cyber Rapid Response Teams through dedicated funding for cross-border cyber crisis response. |
| **Cybersecurity Reserve** | Finances the setup and maintenance of a pool of trusted service providers ready to assist during major cyber incidents across Member States. |
| **Collective cyber crisis management** | Supports initiatives that improve coordination between Member States, the Commission, ENISA, and other stakeholders for effective EU-wide incident response. |
| **Testing and exercises** | Funds penetration testing, simulated crisis response exercises, and vulnerability assessments across critical sectors. |
| **Operational cooperation and solidarity** | Promotes joint actions, common tools, and harmonised procedures to enhance interoperability and mutual support in case of cyber emergencies. |
| **Implementation of EU legislation** | Provides financial and technical assistance to help Member States and operators meet their legal obligations under the new cybersecurity regulatory framework. |

## Parts of the policy directly related to Specific Objectives (SO) in DEP

**SO1 – HPC:** While not explicitly addressed in the Act, it aligns with the emphasis on coordinated preparedness and adoption of cutting-edge technologies for resilience.

**SO2 – AI Continent:** Several calls use AI to enhance cyber resilience.

**SO3 – Cybersecurity:** The Cybersecurity Solidarity Act is most directly linked to SO3. It introduces concrete mechanisms (European Cyber Shield, Cybersecurity Emergency Mechanism, and Cybersecurity Reserve), which align with multiple DEP calls.

**SO4 – Advanced Digital Skills:** Support the training of cybersecurity professionals, in line with the Act's focus on operational readiness.

**SO5 – Accelerating the best use of Digital Capacities:** Align with the Act's emphasis on coordinated preparedness and adoption of cutting-edge technologies for resilience.

**SO6 – Semiconductors**: Not a primary focus of the Cybersecurity Solidarity Act, but semiconductor security and supply chain resilience are implicit enablers of the Act's objectives.

## Activities in the DEP Work Programme 2025-27 contributing to the objectives of the policy

DEP supports the Cyber Solidarity Act by strengthening national and European cybersecurity capacities. It promotes the establishment and enhancement of National Cyber Hubs, which are central entities responsible for collecting, analysing, and sharing cyber threat intelligence using advanced technologies such as AI and automation. These hubs play an important role in early threat detection and cooperation with national actors (CSIRTs, ISACs) and cross-border networks.

Additionally, the programme fosters the development of cross-border platforms, contributes to the deployment of the European Cyber Shield, and supports initiatives that enhance shared situational awareness to improve cooperation between Member States, facilitate contextualized information sharing, and harmonize tools and procedures for managing cyber incidents at the European level.

Strengthening the Cyber Hubs ecosystem also involves developing common data exchange standards, promoting targeted training aligned with the European Cybersecurity Skills Framework, and organizing joint exercises to enhance collective preparedness.

Mutual assistance actions enable rapid, coordinated technical support among Member States during major incidents, reinforcing European solidarity against cyber threats.

## Match of specific activities mentioned in the policy with call topics from the DEP Work Programme 2025-27

| *Title* | *Deadline* | *Type* | *Budget* |
|---|---|---|---|
| **National Cyber Hubs** | 2025<br>2026 | Call of expression of interest | |
| **Cross-Border Cyber Hubs** | 2025<br>2027 | Call of Expression of Interest | |
| **Strengthening the Cyber Hubs ecosystem and enhancing information sharing** | 2026 | Coordination and Support Action | EUR 2 Mio |
| **Coordinated preparedness testing and other preparedness actions** | 2025<br>2026<br>2027 | Simple Grant<br>Simple Grant<br>Simple Grant | EUR 5 Mio<br>EUR 15 Mio<br>EUR 20 Mio |
| **Mutual assistance** | 2026<br>2027 | Grant for named beneficiaries | EUR 2 Mio<br>EUR 2 Mio |
| **DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC: Enhancing the NCC network** | 2025 | Simple Grant | EUR 46 Mio |