Cybersecurity: MEPs back plans to increase cooperation against threats

- Aims to boost EU ability to detect and prepare for cyber threats
- A new EU-wide network of Security Operations Centres
- MEPs propose stronger focus on protecting public services and SMEs

The “Cyber Solidarity Act” adopted on Thursday aims to build a more resilient, collective EU response against cybercrime.

This legislative proposal seeks to bolster the European Union’s ability to detect, prepare for, and respond to cybersecurity threats and incidents. The proposal’s key objectives include strengthening EU-wide detection and situational awareness of cyber threats, enhancing preparedness and response capabilities for significant cybersecurity incidents, and fostering European technological sovereignty in cybersecurity.

These objectives would be primarily achieved through a pan-European network of Security Operations Centres (SOCs) and by establishing a Cyber Emergency Mechanism and a European Cybersecurity Incident Review Mechanism.

In the amendments adopted by the Industry, Research and Energy Committee, MEPs note that cyberattacks frequently target local, regional or national public services and infrastructure due to their lack of financial resources. They highlight the need to build more resilience among small and medium-sized enterprises (SMEs), microenterprises and start-ups. They also advocate for greater collaboration among member states and with the private sector, as well as for sustained funding.

The adopted report includes proposals to support the development of cybersecurity skills across the EU, and to get citizens more involved and aware. MEPs also want the legislation to support
the EU’s industrial capacity and cybersecurity ecosystem in order to boost its technological sovereignty and open strategic autonomy. Finally, they call for working in cooperation with trusted, like-minded international partners.

Quote

Lead MEP Lina Gálvez Muñoz (S&D, ES) said: "Strengthening cooperation will be key to guaranteeing cybersecurity in the EU. This proposal comes from the need to increase cooperation between member states and strengthen EU capacity to be better prepared for cyberattacks, which are increasing in number, intensity and regularity throughout the EU. These are often targeted at local, regional or national critical infrastructure, affecting citizens directly”.

“To be more resilient, a common European response is urgently needed, based on stronger cooperation at the European level, beyond the national. Cybercrime has no borders and it is increasing exponentially”, she added.

Next steps

The legislation was adopted in the Industry, Research and Energy Committee with 43 votes to 10, with 1 abstention. MEPs also voted to open negotiations with Council with the same majority. A decision to start the talks will be submitted during the 11-14 December plenary session in Strasbourg.

Background

A briefing from the European Parliament’s research service highlights that Russia’s war against Ukraine has revealed the extent of our dependence on digital technology and the fragility of the digital space. It has triggered a surge in cyberattacks that have been particularly disruptive when targeting critical infrastructure – such as energy, health or finance – because of the increasing reliance on information technology, rendering this infrastructure all the more vulnerable. Against this backdrop, the Commission has proposed a regulation on a cyber solidarity act that would address the urgent need to strengthen solidarity and the EU’s capacity to detect, prepare for and respond to cybersecurity threats and incidents.

Further information

EP research briefing
Legislative observatory file
Legislative train: cyber-security package
Committee on Industry, Research and Energy
Contacts

Baptiste CHATAIN
Press Officer
(+32) 498 98 13 37
baptiste.chatain@europarl.europa.eu
indu-press@europarl.europa.eu
@EP_Industry