Measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents

2023/0109(COD) - 18/04/2023 - Legislative proposal

PURPOSE: to lay down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents (EU Cyber solidarity act).

PROPOSED ACT: Regulation of the European Parliament and of the Council.

ROLE OF THE EUROPEAN PARLIAMENT: the European Parliament decides in accordance with the ordinary legislative procedure and on an equal footing with the Council.

BACKGROUND: the magnitude, frequency and impact of cybersecurity incidents are increasing, including supply chain attacks aiming at cyberespionage, ransomware or disruption. They represent a major threat to the functioning of network and information systems. In view of the fast-evolving threat landscape, the threat of possible large-scale incidents causing significant disruption or damage to critical infrastructures demands heightened preparedness at all levels of the Union's cybersecurity framework. That threat goes beyond Russia's military aggression on Ukraine and is likely to persist given the multiplicity of state-aligned, criminal and hacktivist actors involved in current geopolitical tensions.

CONTENT: with this proposal, the Commission aims to set up **Cyber Solidarity Act** which establishes EU capabilities to make Europe more resilient and reactive in front of cyber threats, while strengthening existing cooperation mechanism. It will contribute to ensuring a safe and secure digital landscape for citizens and businesses and to protecting critical entities and essential services, such as hospitals and public utilities.

This Regulation lays down measures to strengthen capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents, in particular through the following actions:

European Cyber Shield

An interconnected pan-European infrastructure of Security Operations Centres (European Cyber Shield) will be established to develop advanced capabilities for the Union to detect, analyse and process data on cyber threats and incidents in the Union. It will be composed of Security Operations Centres (SOCs) across the EU, brought together in several multi-country SOC platforms, built with support from the Digital Europe Programme (DEP) to supplement national funding. The Cyber Shield will be tasked with improving the detection, analysis and response to cyber threats. These SOCs will use advanced technology such as Artificial Intelligence (AI) and data analytics to detect and share warnings on such threats with authorities across borders. They will allow for a more timely and efficient response to major threats.

Cyber Emergency Mechanism

The Cyber Emergency Mechanism will improve the Union's resilience to major cybersecurity threats and prepare for and mitigate, in a spirit of solidarity, the short-term impact of significant and large-scale cybersecurity incidents. It provides for actions to support preparedness, including coordinated testing of entities operating in highly critical sectors, response to and immediate recovery from significant or large-scale cybersecurity incidents or mitigate significant cyber threats and mutual assistance actions.

Also set to be created is an **EU Cybersecurity Reserve** made up of **trusted and certified private companies** ready to respond to major incidents.

European Cybersecurity Incident Review Mechanism

The proposed Regulation would also establish the Cybersecurity Incident Review Mechanism to assess and review specific cybersecurity incidents. At the request of the Commission or of national authorities (the EU-CyCLONe or the CSIRTs network), the EU Cybersecurity Agency (ENISA) will be responsible for the review of specific significant or large-scale cybersecurity incident and should deliver a report that includes lessons learned, and where appropriate, recommendations to improve Union's cyber response.

Budgetary implications

The EU Cybersecurity Shield and the Cybersecurity Emergency Mechanism of this Regulation will be supported by funding under Strategic Objective 'Cybersecurity' of Digital Europe Programme (DEP).

The total budget includes an increase of EUR 100 million that this Regulation proposes to re-allocate from other Strategic Objectives of DEP. This will bring the new total amount available for Cybersecurity actions under DEP to EUR 842.8 million. Part of the additional EUR 100 million will reinforce the budget managed by the ECCC to implement actions on SOCs and preparedness as part of their Work Programme (s). Moreover, the additional funding will serve to support the establishment of the EU Cybersecurity Reserve.

It complements the budget already foreseen for similar actions in the main DEP and Cybersecurity DEP WP from the period 2023-2027 which could bring the total to 551 million for 2023-2027, while 115 million were dedicated already in the form of pilots for 2021-2022. Including Member States contributions, the overall budget could amount up to EUR 1.109 billion.