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

2023/0109(COD) - 08/12/2023 - Committee report tabled for plenary, 1st reading/single reading

The Committee on Industry, Research and Energy adopted the report by Lina GÁLVEZ MUÑOZ (S&D, ES) on the proposal for a regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents.

The committee responsible recommended that the European Parliament's position adopted at first reading under the ordinary legislative procedure should amend the proposal as follows:

Coordinated governance

Members stressed that close and coordinated cooperation is needed between the public sector, the private sector, academia, civil society and the media. Moreover, the Union's response needs to be coordinated with international institutions as well as trusted and like-minded international partners. To ensure cooperation with trusted and like-minded international partners and protection against systemic rivals, entities established in third countries that are not parties to the WTO Agreement on Government Procurement (GPA) should not be allowed to participate in procurement under this Regulation.

Cybersecurity reserve

Regarding the new cybersecurity reserve, Members believe it has the potential of developing industrial capacities in the EU, including for **SMEs**, with investments in research and innovation to develop state of the art technologies, such as cloud and artificial intelligence technologies. In addition, the report proposed to maintain the participation of the industry, enhance the criteria and trust of their participation (i.e. connecting their participation to a national or local company) by clarifying the criteria and the definition of technological sovereignty and to guarantee a balance between non-EU and EU actors. In addition, Members proposed for the Cyber Emergency Mechanism a certification scheme to be used for private providers to build a longstanding and trusted partnership.

To support the establishment of the EU Cybersecurity Reserve, the Commission could consider requesting ENISA to prepare a **candidate certification scheme** for managed security services in the areas covered by the Cybersecurity Emergency Mechanism. To fulfil the additional tasks deriving from this provision, **ENISA** should receive adequate, **additional funding**.

Funding

Considering geopolitical developments and the growing cyber threat landscape and in order to ensure continuity and further development of the measures laid down in this Regulation beyond 2027, particularly the European Cyber Shield and the Cybersecurity Emergency Mechanism, it is necessary to ensure a **specific budget line** in the multiannual financial framework for the period 2028-2034. According to the report, Member States should endeavour to commit themselves to supporting all necessary measures to reduce cyber threats and incidents throughout the Union and to strengthen solidarity.

Strengthening R&I in cybersecurity

The amended text called for enhanced research and innovation (R&I) in cybersecurity to increase the resilience and the open strategic autonomy of the Union. Similarly, it is important to create synergies with R&I programmes and with existing instruments and institutions and to strengthen cooperation and coordination among the different stakeholders, including the private sector, civil society, academia, Member States, the Commission and ENISA.

Evaluation and Review

The amended text stated that by two years from the date of application of this Regulation and every two years thereafter, the Commission should carry out an evaluation concerning, *inter alia*: (i) both the positive and the negative working of the Cybersecurity Emergency Mechanism; (ii) the contribution of this Regulation to reinforce the Union's resilience and open strategic autonomy, to improve the competitiveness of the relevant industry sectors, microenterprises, SMEs including start-ups, and the development of cybersecurity skills in the Union; (iii) the use and added value of the EU Cybersecurity Reserve.