

EN

E-003871/2025

Answer given by Executive Vice-President Virkkunen
on behalf of the European Commission
(28.11.2025)

The EU has two landmark pieces of legislation to boost its cyber resilience and to protect its critical infrastructure: the NIS2 Directive¹ and the Cyber Resilience Act²(CRA).

The NIS2 Directive requires Member States to maintain national cybersecurity strategies and imposes stringent risk-management measures and reporting obligations on essential and important entities in critical sectors³.

The CRA, expected to be fully operational by December 2027, mandates horizontal cybersecurity requirements for hardware and software placed on the EU market.

In addition, the implementation of the Cyber Solidarity Act⁴ will bolster the EU capacity to detect, prepare for, and respond to cyber threats. It establishes the EU Cybersecurity Reserve to ensure that Member States and selected beneficiaries receive necessary support during significant and large-scale incidents.

To further reinforce this comprehensive framework, the Commission is currently working at revising the Cybersecurity Act⁵ (CSA), with the aim to: revise the mandate of the EU Agency for Cybersecurity to make it fit for current and future threats and needs; improve the European Cybersecurity Certification Framework; address Information and Communication Technology supply chain security challenges; and make the implementation of the EU cybersecurity framework simpler and more business-friendly.

With these legislative initiatives, supported by further policy measures^{6,7} and making use of the EU Cyber Diplomacy Toolbox, the EU Hybrid Toolbox, and the EU Foreign Information Manipulation and Interference Toolbox⁹, the EU and its Member States contributed significantly to European cyber resilience and countering state-sponsored interference in recent years and will continue to do so in the future.

¹ <https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng>.

² <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847>.

³ <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>.

⁴ <https://eur-lex.europa.eu/eli/reg/2025/38/oj/eng>.

⁵ <https://eur-lex.europa.eu/eli/reg/2019/881/oj>.

⁶ Cyber Blueprint <https://www.consilium.europa.eu/en/press/press-releases/2025/06/06/eu-adopts-blueprint-to-better-manage-european-cyber-crises-and-incidents/>.

⁷ the Action Plan on the cybersecurity of hospitals <https://digital-strategy.ec.europa.eu/en/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers>.

⁸ the Cybersecurity Skills Academy <https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy>.

⁹ EU Council Conclusions from December 2023

<https://www.consilium.europa.eu/media/68967/europeancouncilconclusions-14-15-12-2023-en.pdf>.