

EN

E-003226/2025

Answer given by Executive Vice-President Virkkunen  
on behalf of the European Commission  
(8.10.2025)

The EU faces an evolving cyber threat environment: among other strategies, the ProtectEU Strategy<sup>1</sup> highlights the need to further build resilience against hybrid threats including by reinforcing cybersecurity.

The EU has a robust legal framework for critical sectors' cybersecurity. In particular, the NIS2 Directive<sup>2</sup> sets risk management and incident reporting requirements for entities in 18 sectors. Member States, including Greece, can consider national circumstances when transposing the Directive, in particular by using the minimum harmonisation approach where appropriate.

Other EU policies help tackle malicious cyber activity. For instance, the Cyber Resilience Act<sup>3</sup> bolsters cyber resilience of products with digital elements in the internal market while the EU Cyber Blueprint<sup>4</sup> strengthens cooperation between different actors in responding to cyber crises. Moreover, the Cybersecurity Act is being revised<sup>5</sup> with a view to streamline cybersecurity measures and strengthen cyber resilience.

The Commission is not competent to control the activities of civil society organisations operating in Member States.

To address the risk of foreign interference in democratic processes, Regulation (EU) 2024/900 on the transparency and targeting of political advertising bans the provision of political advertising services to sponsors from third countries in the three months preceding an election or referendum. The Commission is also preparing a new European Democracy Shield which will provide a strategic approach to safeguard, strengthen and promote democracy. Building on existing EU frameworks and legislation, the initiative will reinforce efforts to counter foreign information manipulation and interference, and disinformation.

---

<sup>1</sup> COM(2025) 148 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0148>.

<sup>2</sup> Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>.

<sup>3</sup> Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng>.

<sup>4</sup> Council Recommendation of 6 June 2025 on an EU blueprint for cyber crisis management. <https://eur-lex.europa.eu/eli/C/2025/3445/oj/eng>.

<sup>5</sup> The EU Cybersecurity Act [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14578-The-EU-Cybersecurity-Act\\_en](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14578-The-EU-Cybersecurity-Act_en).