

(English version)

**Question for written answer E-002809/24
to the Commission
Michał Wawrykiewicz (PPE)
(6 December 2024)**

Subject: Action to protect the rule of law in the digital space

Increasing digitalisation and its growing impact on society pose new challenges for the EU in relation to safeguarding the rule of law. Disinformation, cyber-attacks and data manipulation threaten democratic processes, the foundations of the rule of law and fundamental civil liberties. The EU needs a clear strategy to address these threats and ensure security in the digital space.

In light of the above:

1. What action is the Commission taking to counter disinformation that threatens democratic processes in the Member States?
2. Does the Commission plan to create a mechanism to respond to cyber-attacks targeting institutions and organisations in the EU?

Submitted: 6.12.2024

**Answer given by Mr McGrath on behalf of the European Commission
(26 February 2025)**

The Digital Services Act ⁽¹⁾, the Code of Practice on Disinformation ⁽²⁾ and the regulation on political advertising ⁽³⁾ provide a robust framework to mitigate the spread of disinformation on online services.

The regulation will ensure transparency of messages designed to influence elections and regulatory processes and will strengthen the rules for targeting political advertising.

The Code plays a key role in mobilising online platforms, civil society and fact-checking organisations to combat disinformation, including through the Rapid Response System. The EU also supports independent fact-checkers and researchers through the European Digital Media Observatory.

The Democracy Shield will aim to combat foreign information manipulation, interference and disinformation. It will strengthen the EU's ability to detect, analyse and counter threats, increase situational awareness and support societal resilience and preparedness, through digital and media literacy.

Mechanisms are being put in place to protect the EU entities ⁽⁴⁾ via the implementation of Regulation (EU) 2023/2841 ⁽⁵⁾. Actions are also being taken by the Interinstitutional Cybersecurity Board ⁽⁶⁾, in cooperation with the Cybersecurity Service for the EU institutions, bodies, offices and agencies (CERT-EU).

Responses can include, on the basis of proposals by CERT-EU, the adoption of mechanisms for incident response coordination and cooperation for significant incidents and for the management of major incidents, including the establishment of cyber crisis management plans at EU entities' and at EU levels.

The recommendation on inclusive and resilient elections also contains measures on election-related cyber threats ⁽⁷⁾.

⁽¹⁾ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC.

⁽²⁾ <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>

⁽³⁾ Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising.

⁽⁴⁾ EU institutions, bodies, offices and agencies.

⁽⁵⁾ Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, which entered into force on 7 January 2024 — <https://eur-lex.europa.eu/eli/reg/2023/2841/oj>

⁽⁶⁾ of which the Commission is a member.

⁽⁷⁾ Commission Recommendation (EU) 2023/2829 of 12 December 2023.