

(English version)

**Question for written answer E-002063/26
to the Commission
Piotr Müller (ECR)
(19 May 2026)**

Subject: Risk of restricting access to advanced AI technologies and cybersecurity in the EU

Debates in Parliament on advanced AI systems used in cybersecurity show the increasing importance of Western countries cooperating on technology in the face of threats from authoritarian states, particularly China.

However, there are also concerns that the Commission may try to respond to the development of new technologies primarily through further regulatory or administrative restrictions on providers of advanced digital solutions, including US companies working with European institutions and businesses.

In light of the above:

1. Is the Commission considering introducing new regulatory or administrative restrictions on advanced AI and cybersecurity systems provided by US companies?
2. How does the Commission intend to ensure that EU regulatory policy does not restrict access for European businesses and public administrations to modern strategic technologies developed by allied countries?
3. How does the Commission intend to reconcile the development of European technological capabilities with maintaining strong transatlantic cooperation in the area of cybersecurity and artificial intelligence?

Submitted: 19.5.2026

**Answer given by Executive Vice-President Virkkunen on behalf of the European Commission
(8 September 2026)**

As advances in frontier AI models offer opportunities as well as novel and heightened risks for cybersecurity, the Commission adopted on 7 July 2026 an Action Plan on Cybersecurity and AI with concrete actions to support Member States and organisations across the EU ⁽¹⁾.

A key priority of the Commission is to ensure that frontier AI models are safe, accessible and deployable for cybersecurity in Europe. The action plan proposes a Blueprint as a framework for secure access to frontier AI models with cyber capabilities as well as investment for testing and evaluation of such models.

Europe must also step up its preparedness and resilience in the face of the cybersecurity risks posed by frontier AI. The Commission considers that this requires, first and foremost, the effective implementation of the EU's existing legislation, including the NIS2 Directive ⁽²⁾, the Cyber Resilience Act ⁽³⁾, and the AI Act ⁽⁴⁾ that obliges providers of the most advanced AI models to assess and mitigate systemic risk, including of misuse in the cyber realm.

The action plan also prioritises investments in European AI capabilities for cybersecurity, for which existing investments in research and development under the Horizon and Digital Europe Programmes will be complemented by the launch of an EU Grand Challenge on AI-assisted vulnerability remediation.

In order to finance Europe's tech sovereignty ambitions, the communication on European Tech Sovereignty calls for a reflection on the means to boost a European equity capacity at scale in order to establish a portfolio of equity investments in advanced technologies and infrastructure in critical sectors, including AI ⁽⁵⁾.

As the challenges posed by frontier AI are shared and global in nature, it is imperative that the EU works closely with partners at international level.

⁽¹⁾ COM(2026) 577 final.

⁽²⁾ Directive 2022/2555.

⁽³⁾ Regulation (EU) 2024/2487.

⁽⁴⁾ Regulation (EU) 2024/1689.

⁽⁵⁾ COM(2026) 503 final.