European Commission - Press release

Commission presents EU Action Plan on Cybersecurity and Artificial Intelligence

Strasbourg, 7 July 2026

The European Commission has presented an Action Plan for a structured response to address the risks and harness the opportunities of advanced artificial intelligence (AI) models for cybersecurity.

New advanced AI models are redefining cybersecurity. AI can be misused to identify vulnerabilities, automate attacks and increase the scale and speed of cyber incidents at an unprecedented speed.

Building on the EU's unique legal framework for AI and cybersecurity, the Action Plan will bring together Member States, industry and EU-level organisations to strengthen the cybersecurity of our digital landscape against the vulnerabilities posed by advanced AI.

Evaluating AI models

Effective security requires a thorough understanding of how new technologies can be used, misused and exploited. Under the AI Act, advanced AI models must be evaluated, and mitigation measures carefully assessed, before the models are placed on the EU market.

To foster homegrown expertise, the Commission will launch a dedicated call to establish an EU evaluation capacity, covering cybersecurity, expected to be operational in 2027. This new capacity will contribute to the regulatory function of the AI Office by strengthening third-party assessment of AI capabilities and risks globally.

Accessing advanced AI models

Europe also needs clear and transparent conditions for accessing the most advanced AI systems.

The Commission will work with the EU Agency for Cybersecurity (ENISA) to define a European blueprint for structured access to advanced AI capabilities for cybersecurity. This guidance will support relevant European public and private organisations in gaining access to advanced AI models.

Testing AI for cybersecurity

ENISA and the Commission's Joint Research Centre will create a secure platform to test AI for cybersecurity, including using simulated environments. This will bring know-how on the safe use of AI to operators in critical sectors, such as finance, energy, health, transport and the public administration.

Reinforcing the EU's cybersecurity and fixing vulnerabilities

The EU must protect its critical infrastructure against the vulnerabilities arising from the potential misuse of these technologies.

As foreseen by the EU's cybersecurity rules, organisations should intensify cyber hygiene practices, risk management measures, and security by design principles.

Organisations should start using already available AI capabilities, including through open-source models, to identify and fix vulnerabilities faster, as well as to prevent and to respond to cyberattacks.

To assist organisations in this transition, ENISA will support and facilitate partnerships between public authorities, businesses and open-source communities in the cyber ecosystem. This will include guidance, recommendations and best practices as well as a campaign to secure Critical Open Source Software.

Scaling European AI capabilities for cyber

To stimulate the European market to scale up, the Commission will launch the EU Grand Challenge on AI for cybersecurity. This competition will bring together companies, researchers and organisations to develop AI solutions for cybersecurity.

The EU must continue investing in developing its own sovereign advanced AI capabilities, leveraging the infrastructure provided by the AI Factories and future Gigafactories. In this context, the upcoming European Tech equity capacity, announced in the Tech Sovereignty Package, could crowd in private investment to scale up homegrown AI capabilities.

Background

The EU has a legal framework fit to address cybersecurity in the age of emerging tech, like AI. The AI Act requires to assess and mitigate risks from AI models while the General-Purpose AI Code of Practice further specifies these requirements and facilitates compliance by advanced model providers. These provisions will start to be enforced on 2 August 2026.

The Cyber Resilience Act, to be applicable by end of 2027, mandates security by design for hardware and software products. In addition, the Network and Information systems, or NIS2, Directive aims to boost the security of critical sectors such as transport and energy, together with Digital Operational Resilience Act (DORA) for the financial sector. The Cyber Solidarity Act strengthens capacities in the EU to detect, prepare for and respond to significant and large-scale cybersecurity threats and attacks.

For more information

Action plan on Cybersecurity and Artificial Intelligence

Factsheet

IP/26/1544

Quote(s):

"AI is transforming the meaning of cybersecurity. And we must keep pace. The EU has strong foundations in place to adapt its response in the face of vulnerabilities that emerging tech brings with it. We must harness and focus existing capabilities, networks and the legal framework to fortify the cybersecurity protecting our digital landscape."
Henna Virkkunen, Executive Vice-President for Tech Sovereignty, Security and Democracy - 07/07/2026

Press contacts:

Thomas REGNIER (+32 2 29 91099)
Patricia POROPAT (+32 2 29 80485)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email

Related media

Press conference of Henna Virkkunen, Executive Vice-President of the European Commission, on the Action Plan on cybersecurity and AI