

Action Plan on Cybersecurity and AI

Anna Pingen

News

On 7 July 2026, the European Commission presented an [Action Plan on Cybersecurity and Artificial Intelligence](#). The plan sets out an initial EU response to the changing cybersecurity landscape created by advanced AI models. According to the Commission, AI can significantly improve preparedness, threat detection, incident response, and vulnerability management, but it can also be used to automate cyberattacks, identify weaknesses, and increase the speed and scale of malicious cyber operations.

The Action Plan builds on the existing EU legal framework for AI and cybersecurity, which includes the AI Act, the Cyber Resilience Act, the NIS2 Directive, the Digital Operational Resilience Act for the financial sector, and the Cyber Solidarity Act. The Commission stresses that these instruments already provide important legal and operational foundations, but that additional measures are needed to address the specific risks and opportunities created by advanced AI-enabled cyber capabilities.

Seeking to make the AI frontier safe, accessible, and deployable for cybersecurity purposes, the Commission will support the creation of an EU evaluation capacity for AI models, including cybersecurity aspects – expected for 2027. This capacity is intended to strengthen third-party assessment of advanced AI capabilities and support the regulatory work of the AI Office. In addition, the Commission, together with the European Union Agency for Cybersecurity (ENISA), will develop a European blueprint for structured access to advanced AI capabilities for cybersecurity purposes. The blueprint is intended to help public and private European actors, including critical infrastructure operators and cybersecurity providers, access such capabilities safely and without undue delay.

The Action Plan is structured around three main pillars:

- The first pillar provides for the creation of a secure testing platform for AI in cybersecurity. The ENISA and the Commission's Joint Research Centre, in cooperation with other EU bodies and Member States, are to develop a platform where AI tools can be tested in controlled environments. The platform is intended to support testing for cybersecurity use cases, including vulnerability scanning, incident response, threat intelligence, and deployment in simulated critical infrastructure environments.
- The second pillar focuses on preparing the EU's cyber ecosystem for AI-powered threats. The Commission underlines the need to fully apply existing cybersecurity fundamentals, including cyber hygiene, security by design, vulnerability management, and timely patching. To upgrade vulnerability management processes for an environment in which AI can accelerate vulnerability discovery, the ENISA and other actors are to work on making EU vulnerability management tools and practices fit for the AI age. The Commission, the ENISA, Member States, Union entities, industry, and open-source communities are to launch the first pilot of a Critical Open Source Resilience Campaign in 2026. The

AUTHOR

Anna Pingen 

Researcher
Max Planck Institute for the
Study of Crime, Security and
Law

Preprint eucrim 2026, Vol. 21(2)

ISSN: 1862-6947

<https://eucrim.eu>



aim is to help identify, maintain, and secure open-source components relevant to critical infrastructure, including by using AI-supported vulnerability scanning and remediation tools.

- The third pillar concerns the scaling of European AI capabilities for cybersecurity. The Commission plans to launch an EU Grand Challenge on AI-powered cybersecurity solutions in the fourth quarter of 2026. The initiative is designed to bring together cybersecurity companies, AI developers, research organisations, critical infrastructure operators, and open-source communities, with a particular focus on AI-assisted vulnerability remediation.

Finally, the Action Plan contains an international dimension. The Commission emphasises that AI-enabled cyber risks are global and that cooperation with like-minded partners is necessary to avoid fragmentation, strengthen trusted access to advanced AI capabilities, and adapt vulnerability management practices. The EU intends to pursue these objectives in bilateral and multilateral settings, including the G7, cooperation with partner countries, international AI evaluation networks, and exchanges with NATO.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and “criministrative” law.

All news items are freely accessible at: <https://eucrim.eu/news/>

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.

The project is co-financed by the [Union Anti-Fraud Programme \(UAFP\)](#), managed by the [European Anti-Fraud Office \(OLAF\)](#).



**Co-funded by
the European Union**