EUROPEAN
COMMISSION

Strasbourg, 7.7.2026
COM(2026) 577 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Action Plan on Cybersecurity and Artificial Intelligence

1. Introduction

Artificial Intelligence (AI) at the frontier is marking a shift in cybersecurity. Frontier AI models (i.e. the most advanced AI models available or under development) bring increased capabilities to strengthen preparedness and improve threat detection and response, creating **unprecedented opportunities to enhance cyber resilience**. As these capabilities continue to advance[1], AI will enable cybersecurity teams to operate faster and at a greater scale, empowering organisations to address emerging threats more effectively. At the same time, **advanced AI capabilities that are already available today,** including through open source, **can already be used to strengthen the EU's cyber resilience**.[2]

AI has already become **a defining element of the threat landscape**, enabling more automated, scalable and sophisticated offensive cyber operations including cybercrime activities.[3] While frontier level capabilities are currently concentrated in a small number of AI models and systems (i.e. models and systems that can perform a wide variety of tasks and that approach, reach or exceed the current state of the art)[4], the capability gap is narrowing as open source models continue to improve. As a result, actual frontier capabilities are expected to become increasingly accessible over time, including to malicious actors such as cyber criminals, who may exploit those capabilities to execute more complex attacks.

The EU is entering this new paradigm equipped. Over recent years, it has put in place the fundamentals: the legal and operational foundations to address cybersecurity in the age of AI. The **AI Act** provides the world's first legally binding framework to manage risks stemming from AI systems and models, including systemic risks from the most advanced general-purpose AI models such as risks of cyber misuse[5]. The **Cyber Resilience Act** (CRA, to be fully applicable by the end of 2027) addresses the security of supply chains by mandating security by design and vulnerability management throughout the life-cycle for software and hardware products on the EU market.[6] Together, the AI Act and the CRA help ensuring that AI models and systems and products with digital elements are built and maintained with security in mind. In parallel, the **NIS2 Directive**[7], together with the **Digital Operational Resilience Act**[8] for the financial sector, provides a risk-based framework for the cybersecurity of critical sectors. These legislations provide a solid framework that, if implemented effectively, is robust to technological and threat developments. The **Cyber Solidarity Act** complements this framework with operational mechanisms to support Member States in preparedness, detection

[1] Recent research from the UK AI Security Institute suggests that, in controlled cybersecurity tests, the most advanced AI models are able to complete increasingly long tasks without human help. The estimated length of tasks they can handle has been doubling over months rather than years, and recent results suggest this pace may be getting faster.
[2] "AI is changing the economics of vulnerability discovery. Defenders should adapt now", CERT-EU, April 2026
[3] ENISA, *ENISA Threat landscape 2025,* October 2025.
[4] As defined in Article 2(4) of the proposed Cloud and AI Development Act (CADA), COM(2026) 502 final.
[5] Regulation (EU) 2024/1689
[6] Regulation (EU) 2024/2847
[7] Directive (EU) 2022/2555 – covering 11 sectors of high criticality (energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, ICT service management, public administration and space) and 7 other critical sectors (postal and courier services; waste management; manufacture, production and distribution of chemicals; production, processing and distribution of food; manufacturing; digital providers; and research).
[8] Regulation (EU) 2022/2554

and response to significant and large-scale incidents[9]. Together these measures contribute to the objectives of the **Preparedness Union Strategy**[10] and the **ProtectEU Strategy**[11],

Advanced AI-enabled cyber capabilities are also a critical asset for ensuring the security of our Union. While these capabilities, available through different models including open ones, can already step up the EU's cyber resilience, frontier capabilities are mainly developed outside of the EU, and their availability is often determined by non-transparent, foreign-led processes. Knowledge of and access to these capabilities is therefore a matter not only of digital resilience but also of Europe's technological sovereignty. To preserve this sovereignty, the EU must ensure that the uptake of advanced AI-enabled cybersecurity capabilities does not create new strategic dependencies. At the same time, Europe must accelerate its resilience to keep the pace with this fast-evolving threat landscape.

The EU has already taken **strategic steps towards reducing dependencies on critical technologies and increasing homegrown capabilities**. Through the Horizon Europe and Digital Europe programmes, the EU is already funding the development of advanced AI-enabled cyber capabilities and the European Innovation Council Fund has become an important deep tech investor in Europe, including investments into cybersecurity and AI technology startups and scaleups[12]. In addition, the recently proposed **Cloud and AI Development Act**[13] **(CADA)** would expand EU data centre capacity and cloud and AI autonomy, supporting the wider deployment of AI – including cyber-related tools and applications. It would enable the EU to rely on critical cloud and AI capacities, therefore reducing dependencies against geopolitical and security risks. The proposal builds on the **Apply AI Strategy** and the **AI Continent Action Plan**, recognising notably the need to launch Grand Challenges to support and scale-up frontier AI.

Building on these strong foundations, **the EU must now take further action to address the immediate underlying issues and opportunities brought by AI in cybersecurity**.

This Action Plan provides an **initial and targeted response to support Member States and organisations in the Union to address this new reality**.

First, to ensure a safe and responsible adoption of frontier AI, the EU will step up its capacity to evaluate frontier AI before it is released, including in cybersecurity. This will foster a rigorous external evaluation process and top-tier AI evaluation capabilities in the EU. The EU will also facilitate access to advanced AI-enabled cyber capabilities for European actors and support efforts to test available AI models for cybersecurity use cases.

Second, the EU will accelerate efforts to support critical sectors and SMEs in preparing for AI-powered cyber threats, including through the implementation of cybersecurity fundamentals. Drawing on the full range of available AI, the EU will support their usage for strengthening cyber resilience and to fix the most critical vulnerabilities.

Third, the EU will scale its ability to develop and deploy AI-powered solutions by boosting a European ecosystem around them and continuing to strengthen its own capacity in frontier developments. Achieving the latter will require urgent, large scale equity investment to build Europe's own capacities in frontier AI to boost European solutions meeting our needs.

---

[9] Regulation (EU) 2025/38
[10] JOIN(2025) 130 final
[11] COM (2025) 148 final
[12] Sifted, 20 March 2026: Europe's most active deep tech investors in 2025; EIC Impact Report 2025.
[13] COM(2026) 502 final

Finally, the EU will work with like-minded partners across these objectives to promote a trusted and secure global approach to frontier AI and cybersecurity.

2. Pillar 1: Making frontier AI safe, accessible and deployable for European cybersecurity

As advanced AI-enabled cyber capabilities could in the near future be weaponised against our critical infrastructure and our society, the EU needs as a matter of priority to secure early awareness of these capabilities, build stronger technical capacity to evaluate their risks, shape opportunities to test their potential for deployment in cybersecurity, and define clearer access routes for legitimate cybersecurity purposes in Europe. To this end and building on the legal framework provided by the AI Act, the EU will expand European pre-release evaluation capacities, stimulate a common European approach to access and coordinate testing efforts so that frontier AI can be accessed and used safely for cybersecurity in Europe.

2.1. Assessing and mitigating risks posed by frontier AI

The AI Act sets out requirements for the cybersecurity of **AI systems**[14] and **requires providers of the most advanced general-purpose AI models to assess and mitigate systemic risks**, including from misuse of AI in the cyber domain.[15]

As of 2 August 2026, the Commission will exercise the supervisory and enforcement powers provided by the AI Act to ensure effective oversight of AI systems as well as of general-purpose AI models, including models that present systemic risks related to cybersecurity.[16] This oversight includes assessing the providers' identification of risks associated with model capabilities and their implemented measures to mitigate those risks. These requirements continue to be proportionate to the capabilities of the technology at hand.

The supervisory and enforcement powers will be supported by the **Scientific Panel advising the Commission's AI Office**, **secure reporting channels,** and the **Code of Practice for general-purpose AI.**

2.2. Building European excellence in pre-release frontier AI evaluation

To foster the safe and responsible adoption of AI for cybersecurity in the EU, regulatory action must be complemented by **enhanced European evaluation capacities**. As AI capabilities advance, and as systemic risks may not only occur in the cyber domain[17], conducting external evaluations is emerging as a best practice to ensure the safety of frontier AI, in line with approaches established in other risk bearing industries. The AI Act also highlights the **importance of pre-deployment evaluation** through third-party entities to assess and mitigate

[14] As part of Annex III AI Act, AI systems used in critical infrastructure will be considered high-risk and will be subject to specific provisions, including on cybersecurity.

[15] In the AI Act, systemic risks mean risks that are specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain (Article 3(65) AI Act).

[16] Enforcement powers regarding providers of general-purpose AI models with systemic risk that do not comply with the provisions related to systemic risk mitigation include requesting information about the model, requesting access to the model to carry out evaluations, requiring risk mitigation measures, and, ultimately, issuing fines of up to 3% of global annual turnover or requesting a provider to restrict the making available on the market, withdraw or recall the model.

[17] As an example, one other area where capabilities of general-purpose AI models are continuously increasing and could be misused causing risk to public health and public security is biology.

systemic risks as appropriate. To date, most leading entities performing pre-deployment third-party evaluations of AI models are based outside the EU. In view of their growing importance, it becomes a matter of urgency that some of this evaluation expertise and its associated infrastructure sits within the EU.

The EU therefore needs to reinforce available expertise to create a credible and competitive ecosystem of third-party evaluators to assess advanced AI capabilities and risk mitigations, supporting trust in the EU's AI governance framework. To this end, the Commission will propose **criteria for third-party evaluators for the purpose of the Code of Practice on General-Purpose AI and foster the development of a broader evaluation ecosystem.** This will include facilitating meaningful exchanges among evaluators and relevant experts to improve evaluation methodologies and clarifying qualification requirements.

Regarding the **evaluation of AI models specifically for cybersecurity**, Europe has the potential to lead in this domain with top-level cybersecurity specialists. In view of the urgent context, the EU should leverage and reinforce this expertise. To achieve this objective, the Commission will launch a dedicated call for the **establishment of an EU evaluation capacity for AI models that must include cybersecurity.** This capacity would be a strong contributor to the nascent ecosystem in the EU and build on emerging AI evaluation know-how in the Member States. It will also support the Commission's regulatory activities conducted through the AI Office[18] by providing a European choice for third-party evaluations of AI models and their mitigation measures. It will inform the risk management by providers by independently evaluating models' capabilities and the effectiveness of mitigation measures by model providers[19].

This European capacity will support providers of general-purpose AI models with the compliance to the relevant AI Act obligations and the Code of Practice for General-Purpose AI models[20]. It will ensure a credible and rigorous external evaluation process. Top-tier evaluation capabilities in the EU will also inform the understanding of potential systemic risks, including in the area of cybersecurity, but also in biotech and other areas, by producing early warning signals when risks are identified.

2.3.Facilitating access to advanced AI-enabled cyber capabilities in the EU

Access to frontier AI with advanced cyber capabilities is increasingly governed by provider-specific and often non-European decisions, with some providers limiting access to manage risks of misuse through **structured access programmes** (e.g. staged model releases). While such restriction may be justified on safety grounds, this practice often lacks transparency regarding the criteria applied to determine which organisations, including companies, gain access and through which process access is granted. This may hinder the ability of European actors, including competent authorities and operators of critical infrastructure, to make timely use of these AI capabilities and strengthen their resilience.

[18] The General-Purpose AI Code of Practice's Safety and Security Chapter require providers to conduct model evaluations also through adequately qualified independent external evaluators (Appendix 3.5). These reports will then support AI Office's regulatory activities since providers are required to provide to the AI Office any available reports from external evaluations with the Model Report (Measure 7.4).

[19] Evaluations executed by this capacity will be different from the ones executed on the testing platform in section 2.4. The platform will be mainly used for testing cybersecurity applications of AI models while the capacity will focus on the assessment and mitigations of systemic risk to support compliance with the Code of Practice.

[20] The capacity will not be a conformity assessment body and it will only support compliance through its evaluations.

A coordinated EU approach is urgently needed, to facilitate that relevant **European public and private actors** can access such frontier AI safely and do so without undue delay. To this aim, the EU will foster a state-of-the-art, risk-based process with clear criteria and designed to effectively mitigate misuse risks.

The Commission, in coordination with the EU Agency for Cybersecurity (ENISA), will develop a **European Blueprint for structured access to advanced AI capabilities for cybersecurity purposes** as a guidance document to spell out how providers of AI with advanced cyber capabilities can grant access to European organisations, including companies, and thereby support their mitigation of cyber risks.

This guidance document will include **the criteria that should be considered** for granting access to AI with advanced cyber capabilities for European players. The Blueprint should cover relevant criteria for different types of organisations (e.g. EU institutions, Member State authorities, operators of critical infrastructure, cybersecurity providers and research actors) and describe how these actors would be identified. It should also include security criteria so that access given through the Blueprint does not pose undue risk and **a mechanism to streamline the provision of access** to eligible entities. This mechanism should also facilitate early i**nformation** by providers on planned trusted access programmes as well as knowledge-sharing among EU organisations that were granted access to a given model or system.

While it will **not introduce new obligations for providers**, the Blueprint will support the objectives of the Code of Practice for General-Purpose AI by identifying possible safety mitigation measures that can complement **the systemic risk management** to be implemented by providers of GPAI models with systemic risk[21][22]. By providing a **European reference framework**, the Blueprint will serve as basis for further international cooperation.

The Blueprint should include **contingency measures in case of restricted or withdrawn access to AI with advanced cyber capabilities** to define the actions to be executed at EU level in the situation that access to a relevant model or system is restricted or withdrawn by a provider or a third-country authority. In addition, when timely access to frontier AI is needed for general use, the Commission, in cooperation with Member States, will explore the potential use of funding instruments available, including joint procurement, for **jointly obtaining access to such models or systems**.

2.4. Testing AI with advanced cyber capabilities for timely and secure deployment of AI in cybersecurity

Access to safe and trustworthy frontier AI must be matched with testing of its capabilities for use in cybersecurity operations, such as vulnerability scanning, remediation and incident response. To reap its benefits, critical infrastructure operators and public authorities need to quickly understand how AI with advanced cyber capabilities performs in realistic cybersecurity settings before it is deployed in sensitive environments. Such testing should take place in **safe and controlled environments**.

To create synergies at European level, **ENISA** and the **Joint Research Centre of the European Commission (JRC)**, in cooperation with other relevant Commission services and Union entities, such as CERT-EU, Europol and sectoral authorities, and Member States, will therefore organise a **secure testing platform for AI in cybersecurity use cases[23].** The

[21] In accordance with Article 55(1)(b) of the AI Act.
[22] For example, the GPAI Code of Practice's Safety and Security Chapter mentions 'staging the access to the model' as an example safety mitigation in Measure 5.1.
[23] Existing platform managed by JRC could be upgraded to enable this type of testing.

platform will allow participants to use their own model access keys under shared security and confidentiality rules, with each covering their own costs, using their own tools, and retaining responsibility for their testing methods. ENISA, in coordination with the JRC, should govern access to the testing platform and aggregate outcomes.

This European secure testing platform will also enable **testing the deployment of advanced AI cyber capabilities in critical infrastructure's systems** without exposing real infrastructure to risk ('**cyber ranges**'[24]). This initiative will prioritise the **adaptation and expansion of existing cyber ranges** rather than the duplication of environments. In particular, while new cyber ranges will be developed only in sectors where such capabilities are not currently available, industry across sectors could support this initiative by providing existing environments to be integrated through dedicated pledges. Contributing industry actors may receive aggregated information from relevant testing activities, subject to applicable confidentiality rules.

The usage of this environment will be focused on testing AI to strengthen cyber resilience and not aimed to evaluate general-purpose AI models for compliance with the AI Act[25]. It will foster and accelerate operational experience using AI for cyber resilience, including detection, triage, threat intelligence, and response, to outpace attackers. **ENISA**, to ensure a high level of cybersecurity across the Union, will draw on its knowledge to release and maintain **guidance and advisories on securely using available AI models and systems** for the broader ecosystem.

Key actions:

- **Key Action 1 – The Commission will support the establishment of an EU evaluation capacity for AI models that must include cybersecurity (2027).**
- **Key Action 2 – The Commission in coordination with ENISA will define a European Blueprint for structured access to advanced AI capabilities for cybersecurity purposes to ensure that European organisations can access such capabilities safely and timely (Q4 2026).**
- **Key Action 3 - ENISA and the Joint Research Centre of the European Commission (JRC) will develop a secure testing platform for AI with advanced cyber capabilities for cybersecurity use cases to boost timely and secure deployment of AI in cybersecurity (Q4 2026).**

3. Pillar 2: Preparing the EU's cyber ecosystem for the age of AI

As advanced AI cyber capabilities become increasingly accessible and widely deployed, the EU must be ready both to address their possible misuse against its economy and society and to use them safely for cyber resilience. AI can accelerate the discovery of vulnerabilities with a high degree of automation and at a greater scale, while lowering the expertise, time and resources needed for malicious actors to conduct sophisticated attacks. As an immediate priority, the EU must strengthen its preparedness and support critical sectors in adapting to

[24] Cyber ranges are secure and controlled environments that reproduce, in simulated form, digital systems, networks or infrastructure. They enable testing in realistic conditions, while ensuring that any activity carried out in the environment does not affect real systems or services.

[25] Testing AI for cyber resilience aims to understand the operational suitability of an AI model or an AI system for executing a specific cyber security task, while the evaluation of AI models for supporting compliance with the AI Act aims to provide an assessment of the risks stemming from the model and the effectiveness of the risk mitigations implemented by the model provider. Testing AI for cyber resilience is therefore different from evaluating AI models for supporting compliance with AI Act and requires different skills and resources.

these threats. This includes integrating available AI solutions into cybersecurity operations, drawing on the full range of AI models and in particular those that are open source, while accelerating efforts in identifying and fixing most critical vulnerabilities. ENISA is uniquely positioned to support this transition of the EU cyber ecosystem to the age of AI.

3.1. Applying EU cybersecurity fundamentals and preparedness

In this new technology and security landscape, **cybersecurity fundamentals and preparedness matter now more than ever**, and existing EU cybersecurity tools and instruments must be used to their full extent.

The EU's cyber regulatory framework, notably the **NIS2 Directive[26] and the Digital Operational Resilience Act (DORA)**, provides a strong baseline for the preparedness of critical infrastructures against all types of cybersecurity risks, including those related to AI. These rules must therefore be transposed and implemented by Member States as a matter of urgency. In addition, Member States must consider the risks from advanced AI in their supervisory work. Likewise, critical sector operators and financial entities should review and adjust their risk management framework to the new realities, anticipating AI-powered cyberattacks at a higher frequence and scale, and reduce the time-to-patch by accelerating the patching cadence and having the ability to rapidly patch complex systems.

To further reinforce preparedness, entities should consistently apply **basic cyber hygiene measures** and implement network and system hardening (including through zero trust approaches where appropriate). They should also start **using already available AI capabilities,** including through open source models, to detect vulnerabilities and to improve the detection and prevention of cyberattacks. **Union entities**, with the support of CERT-EU and with the guidance of the Interinstitutional Cybersecurity Board (IICB), can lead by example in that regard to strengthen the Union's overall cyber posture, in line with the regulation on the cybersecurity of Union entities[27]. Member States are also strongly encouraged to make full use of conversion possibilities of the **EU Cybersecurity Reserve** to enhance resilience against AI-powered cyber threats, including through vulnerability scanning, automated penetration testing and risk monitoring, with support for patching recommendations.

In addition, as reflected in the **Cyber Resilience Act**, which will be fully applicable as of 11 December 2027, secure-by-design development practices, systematic vulnerability management, timely patching and secure coding practices – including approaches that eliminate entire classes of vulnerabilities, such as memory-safe software development – remain essential. AI-specific cybersecurity risks, including data and model poisoning, adversarial attacks, and prompt injection must also be carefully assessed and mitigated in line with relevant provisions of the AI Act.

To support these efforts, **ENISA,** in cooperation with European supervisory authorities and other relevant Union entities, will make available and maintain **appropriate guidance, recommendations, advisories and best practices to remain protected against AI-powered**

[26] The NIS 2 Directive sets out the baseline for cybersecurity risk management, requiring essential and important entities operating in 18 critical sectors to protect their network and information systems and to prevent and minimise the impact of incidents.
[27] Regulation (EU, Euratom) 2023/2841

threats[28] **and foster secure integration of AI tools in cybersecurity operations**. Such guidance and advisories should also take into considerations the needs of SMEs that are most vulnerable to attacks. Where relevant, these efforts could be reinforced and enriched by sectoral initiatives and cooperation mechanisms in areas such as finance, transport, energy, agro-food, healthcare[29] and space.

As technologies and associated risks will continue to evolve, **collective situational awareness and structured information sharing on AI-driven cybersecurity threats** through relevant Union networks, both at horizontal and sectoral levels, will be instrumental to strengthen situational awareness. ENISA should explore ways to assist cooperation with AI providers to enhance sharing of threat intelligence.

Similarly, Member States should take advantage of existing structures at Union level in the area of cybersecurity to **assess critical infrastructure preparedness**, by working together in particular in the NIS Cooperation Group, and as appropriate, in cooperation with the AI Board established under the AI Act.

3.2. Accelerating the patching process: upgrading vulnerability management for AI-speed discovery

The immediate challenge for the cyber posture of the EU lies in **fixing existing vulnerabilities before they can be exploited at scale**. As AI reduces the time needed for malicious actors to exploit vulnerabilities, relevant entities must equally accelerate their ability to analyse, prioritise, remediate and deploy fixes quickly enough to prevent exploitation.

Existing vulnerability handling processes must be upgraded to be effective in the age of AI-assisted discovery. ENISA should ensure that Europe's vulnerability management infrastructure and services, including the European Union Vulnerability Database (EUVD) and the CRA Single Reporting Platform, are fit-for-purpose in the era of AI-assisted vulnerability discovery and, jointly with Member States, reinforce interoperability across EU, national and global vulnerability platforms and databases.

As the number of vulnerability reports increase, manufacturers must decide which flaws to fix first across product lines, while users - especially essential and critical important entities - must determine which updates to deploy first, often with limited resources. Organisations must be able to rely on clear EU-wide, risk-based guidance aligned with the CRA and the NIS2 Directive to help patch where the risks are greatest.

As part of their obligations under the NIS2 Directive, **Member States should also update national coordinated vulnerability disclosure (CVD) policies** to address AI-enabled exploitation. The NIS Cooperation Group should revise its guidance on CVD implementation, and the EU should also review whether the ISO/IEC standards underpinning CVD frameworks remain fit for purpose in light of current threats. International cooperation is also essential in this regard as these practices are shaped globally.

Lastly, securing critical infrastructure does not end with disclosing vulnerabilities or releasing fixes. The greater challenge lies in **applying them**. As AI accelerates vulnerability discovery, the bottleneck in deploying patches becomes more acute. With the support of ENISA, Member

[28] An example of such advisories is the CERT EU blog post: *AI is changing the economics of vulnerability discovery. Defenders should adapt now,* 21 April 2026.
[29] European action plan on the cybersecurity of hospitals and healthcare providers: COM(2025)10 final

States should leverage existing networks, such as the NIS Cooperation Group, to address this challenge, which is of utmost urgency.

3.3. Putting into practice: fixing what matters most

The EU must not only build knowledge on how AI can strengthen cyber resilience; it must **apply that knowledge where the need is most urgent**. The challenge is therefore to not only find vulnerabilities faster, but also analyse them, fix them and coordinate deployment at scale. **Critical open source software is the right place to act first**, due to the high penetration in critical infrastructure sectors. Reportedly, 98% of the total codebase contains open source, with critical infrastructure industry averaging to about 80% of codebases with high- or critical-risk vulnerability[30].

The **EU Open Source Strategy**[31], released as part of the Tech Sovereignty Package, includes a series of measures to increase the security and support the maintenance of critical open source components. In this context, the Commission will work with ENISA, the Member States[32] and open source communities, to pilot some actions specifically targeted to cyber and AI.

ENISA, in cooperation with the Commission, Member States and open source communities, will expedite the mapping of critical open source components foreseen under the Strategy and, based on a preliminary list informed by agreed criteria, **pilot a Critical Open Source Resilience Campaign** for open source components relevant to critical infrastructure. The results of the campaign will inform the implementation of the Open Source Maintenance Instrument. The campaign will consist of a voluntary sponsorship scheme to match open source projects with organisations willing to work in close partnership with the projects' maintainers to support their maintenance and security. Sponsors may include Member States, Union entities such as CERT-EU, operators of critical infrastructure, manufacturers and other public or private entities able to provide support for instance by making available skilled people, or AI models and tools to the maintainers of open source projects. Member States and other eligible users can draw on support from private trusted providers in the **EU Cybersecurity Reserve** for vulnerability scanning of open source dependencies in critical infrastructure. In addition, ENISA will build a **service catalogue of AI powered services**, aimed at supporting the patching and remediation of open source vulnerabilities.

Open source maintainers will be able to benefit from the sponsorship scheme and the service catalogue to increase the speed and effectiveness of their work and reduce cyber risks, accelerated by the evolution of AI models. The initiative will reinforce existing open source governance and workflows and act as a proving ground for Europe's wider push on AI-assisted remediation further enhancing the Union's operational know how. It will contribute to reinforce cyber resilience across sectors, including critical infrastructure and SMEs. A first pilot campaign will be launched in 2026, in view of further scaling if proven successful, including in the context of the Open Source Strategy.

Key actions

- **Key Action 4 – <u>ENISA in cooperation with relevant Union entities</u> will issue guidance, recommendations, advisories and best practices on the protection**

[30] Blackduck, 2026 *<u>Open Source Security and Risk Analysis Report</u>*: e.g. for aerospace, aviation, automotive, transportation, logistics - 87%; manufacturing 88%; Healthcare; 88%; Energy 89%; internet and software infrastructure 80%).

[31] COM(2026) 503 final.

[32] In particular, where appropriate, in coordination with the European Digital Infrastructure Consortium (EDIC) on the Digital Commons.

against AI-powered threats and for the secure integration of AI in cybersecurity operations (as of Q3 2026)

- **Key Action 5 – The Commission, Member States, ENISA and industry will cooperate in view of making existing vulnerability management practices and tools fit for the AI Age (as of Q3 2026)**
- **Key Action 6 – ENISA, in cooperation with the Commission, Member States, open source communities, Union entities and industry, will launch a first pilot of a Critical Open Source Resilience Campaign to accelerate patching including by leveraging AI (Q4 2026)**

4. Pillar 3: Scaling European AI capabilities for cyber

In a context where both defensive and offensive cyber operations increasingly rely on advanced AI, the ability to develop and deploy AI-powered cybersecurity solutions is becoming a strategic enabler of cyber resilience and sovereignty. In particular, for sensitive use cases, the EU must be able to rely on sovereign AI capabilities that meet necessary security needs, including in the area of defence. The EU must now enable European providers, including disruptive innovators, to develop, deploy and scale such advanced AI in Europe. Complementing its investment strategy for cyber and AI, the EU must gather its technology ecosystem to address the most urgent operational cybersecurity needs, foster investments in development and uptake of European AI capabilities towards the frontier, and develop the skills needed to deploy them across sectors.

4.1. Boosting the European ecosystem around AI-powered cybersecurity solutions

As AI is already leveraged for malicious purposes, organisations need to move faster than attackers in deploying available AI-powered cybersecurity solutions to protect critical infrastructure across sectors. The EU must stimulate the European market to make available such tools at the speed and scale needed and encourage uptake in our critical infrastructure.

Significant investments are already being made by the EU to **support research and development of homegrown advanced AI-enabled cybersecurity technologies** and for the cybersecurity of AI, with notably EUR 200 million by the end of the current Multiannual Financial Framework under the Horizon and Digital Europe Programmes. For instance, three flagship Horizon Europe projects will be launched at the end of 2026 to support the development, training and testing of AI for monitoring, detection, response and self-healing capabilities in digital processes and systems against cyberattacks, including adversarial AI attacks, as well as the development of generative AI tools and technologies for continuous monitoring, compliance and automated remediation. The EU is also funding the full AI capability cycle when it comes to law enforcement, from researching to testing, validation and operational deployment through Horizon Europe, the Internal Security Fund, Digital Europe, and CERIS. Similarly, the EU is investing through the European Innovation Council (EIC), including via direct investments by the EIC Fund, in European deep tech cybersecurity and AI companies, also extending in 2026 and 2027to relevant dual use and strategic defence technologies.[33] More specifically, by the end of 2026, the Commission will enable investments by the EIC Fund into cyber and AI tech companies as part of EUR 100 million to be invested in strategic defence tech startups and scaleups and continue similar support in 2027. The Scaleup Europe Fund will make its first investment into the growth stage of strategic companies still in 2026. Building on the EU's International Digital Strategy, the EU and Member States

[33] The EIC Fund - European Innovation Council - European Commission.

will also leverage the EU's Tech Business Offer to support the deployment of AI and software solutions.

Complementing these investments, the Union should seek to further **accelerate the sharing of knowledge of advanced AI-powered cybersecurity capabilities against large-scale cyberattacks using AI**. Today, the EU has a rich ecosystem and knowledge base across the academia, industry and government, but AI-powered solutions for cybersecurity remain fragmented, insufficiently tested in operational environments and far from being deployed at scale across sectors[34]. One example is automated vulnerability remediation, which is one of the main operational bottlenecks for cybersecurity in the age of AI: today, AI-enabled vulnerability discovery is advancing faster than AI-assisted remediation, thus creating a structural imbalance to the advantage of the attackers. Answering to calls to address the threats posed by offensive AI[35], the Commission, with the support of the European Cybersecurity Competence Centre (ECCC) and in cooperation with ENISA, will therefore launch a dedicated **EU Grand Challenge on AI-assisted vulnerability remediation**. Bringing together European cybersecurity and AI companies, research organisations, critical infrastructure operators and open source communities around this common mission, the Grand Challenge will support the development of an AI system capable of assisting cybersecurity teams throughout the remediation lifecycle. By linking research and deployment, the Grand Challenge will enable promising solutions to be tested in realistic operational environments and ultimately made available to organisations across Europe, contributing to reducing the operational bottlenecks that hinder timely remediation. Interested Member States will be invited to support such efforts of knowledge sharing.

4.2. Building European frontier capabilities

While existing AI models and systems with cybersecurity capabilities already provide significant opportunities for cybersecurity operations, frontier AI-enabled cyber capabilities also carry major implications for Europe's technological sovereignty, security and defence. Therefore, the EU must **develop its own sovereign general-purpose frontier AI capabilities** to mitigate the risk of new dependencies on what has now become a critical strategic asset with an increasingly dual-use potential of frontier AI that extends well beyond the cybersecurity domain. It represents a broader cross-sectoral challenge for our economy and society that the Commission will continue to monitor closely and address as it evolves.

The Commission has already taken concrete steps to support key European actors in advancing AI capabilities towards the frontier.

- Recently, the Commission awarded the Frontier AI Grand Challenge, granting access to EuroHPC computing capacity, supporting the development of a European open source advanced AI model.[36]
- Under the Resource for AI Science in Europe (RAISE), the Commission is funding a network of Frontier AI Labs to advance research also in this area.
- Under Horizon Europe the Commission is funding activities to scale safe and secure AI towards the frontier.
- The Commission will continue working with France and Germany to set up a collaborative effort (the 'European Frontier AI Initiative') pursuing research and innovation bets, attracting talent and facilitating spinoffs.

[34] Public Letter of Support for a European Grand Challenge in AI and Security - Google Docs.
[35] Idem.
[36] Commission selects EUROPA consortium as the winner of the Frontier AI Grand Challenge, a project to build European open-source frontier AI model in all 24 EU languages | Shaping Europe's digital future.

- The Commission benefits from technical advice through the Frontier AI Forum[37]

These initial steps lay important groundwork, yet a **paradigm shift in ambition and resources is needed** to transform Europe's AI frontier aspirations into a lasting sovereign capacity and competitive advantage. Given the unprecedented scale of resources required for frontier AI development, frontier projects require a collaborative approach at Union level. The proposed CADA identifies them as priority projects and allocates the Union's computing resources complementing those allocated by Member States. **Existing AI Factories and future Gigafactories** should be leveraged to serve as part of a sovereign European infrastructure for AI and cybersecurity, comprising compute, data and connectivity and position the EU as a leading AI continent. Such connectivity is a pre-requisite for the trusted sharing of AI-ready data sets, the federation of resources across borders, the secure operation of controlled environments, and the development, testing, deployment and access of robust, trustworthy and high-performance cyber-AI capabilities. Relevant cyber-focused AI Factories should facilitate access to high-quality AI-ready datasets, ranging from public data to sensitive industrial[38] and cybersecurity data, through trusted, secured and resilient data sharing mechanisms, and support the development and validation of AI models in a controlled, accountable and auditable environment through their data labs.

The Commission will also support the development of sovereign European AI cyber capabilities, including for defence, through the European Competitiveness Fund, ensuring that Europe is better equipped to protect its strategic interests and reduce critical dependencies. In this context the Commission will establish a dedicated working group with relevant agencies, including ENISA and the European Defence Agency (EDA), and the Member States to address the security risks linked to the deployment of frontier AI models in defence and dual-use critical systems.

Developing sovereign frontier capabilities will entail **hundreds of billions of euro investment needs** which can only be partly covered by public finances. This calls for urgently crowding in large amounts of private investments, and especially risk capital and equity to develop and scale innovative European solutions. Without compute, models, and data infrastructure, Europe is bound to remain a vulnerable user of frontier AI systems made elsewhere that others can suddenly switch off – with huge economic and (cyber)security implications. Yet, while the cost for Europe of building its own frontier AI capacity may be very large, the cost of not building it may be even larger and grow every year as the AI-capability gap widens.

With its Tech Sovereignty Package of 3 June 2026, the Commission has launched **consultations with the Member States, the EIB Group and other key stakeholders on the proposal of setting up a new European equity capacity** managing a portfolio of large-scale equity investments in advanced technologies and infrastructure key for our technological sovereignty – including digital technologies such as frontier AI, but also clean energy technologies, biotech, and potentially defence tech. The main advantage of this mechanism would be to create a much-needed equity 'co-investment anchor' crowding in large amounts of private investments, by working in synergy with or investing in financial instruments already existing at EU level, such as the Scaleup Europe Fund. This new strategic tech equity facility would be a game changer in answering this last call for large EU investments in frontier AI. As regards the ECF InvestEU Instrument, such mechanism would have the potential to become

[37] Commission seeks experts for forum on Frontier AI | Shaping Europe's digital future
[38] Subject to compliance with applicable laws, including EU competition law.

an important entity for strategic equity investments for large tickets in advanced technologies and infrastructure.

4.3.Boosting cybersecurity skills for the age of AI

Technology alone will not determine Europe's success. The ability to deploy advanced AI effectively and securely in cybersecurity operations will also depend on the **availability of skilled professionals capable of understanding and using safely AI models with advanced cyber capabilities**, as well as of managing AI-specific risks. As cybersecurity teams will increasingly integrate advanced AI, this may further exacerbate the existing cybersecurity skills gap. The EU must therefore strengthen its cybersecurity workforce, by equipping it with the right AI skills for cybersecurity.

The **EU Cybersecurity Skills Academy**, bringing together industry, training providers and academic institutions around concrete cybersecurity training pledges and partnerships, provides the right framework to address this need at Union level. The Commission, together with Member States, will leverage this growing ecosystem to launch a dedicated action under the Cyber Skills Academy to develop training programmes for cybersecurity professionals to use AI tools. It should also explore potential synergies with the upcoming AI Skills Academy. In addition, ENISA will update the **European Cybersecurity Skills Framework**, integrating AI-related competencies into existing professional profiles and defining new roles where necessary.

Key actions:

- **Key Action 7 – The Commission, with support of the European Cybersecurity Competence Centre, and in cooperation with ENISA, will launch an EU Grand Challenge to help scale European AI-powered cybersecurity solutions (Q4 2026)**
- **Key Action 8 - The Commission, jointly with Member States, will aim to make available access to AI Factories' compute capacity to test, train and deploy available advanced and frontier AI models for cyber resilience on sovereign compute.**
- **Key Action 9: The Commission will work with Member States and industry (under the Cybersecurity Skills Academy) to develop training modules for cybersecurity professionals on the use of AI for cybersecurity (Q4 2026).**

5. Working with like-minded partners towards a global approach to cybersecurity in the age of AI

The cybersecurity implications of AI are inherently global, since AI models and systems, software supply chains, and open source ecosystems operate across borders. The release of an AI model with cyber capabilities developed in one jurisdiction can have significant consequences for the security of critical infrastructure and businesses across the world. Governments, international organisations and industry thus face **a shared challenge, and international cooperation is essential** to avoid fragmentation, promote interoperability among trusted partners, and to pool efforts to mitigate cybersecurity risks associated with AI.

The EU should lead in shaping global practices on trustworthy AI and cyber resilience leveraging the Union's **AI and cyber regulatory framework**. In particular, closer cooperation among like-minded partners is needed to ensure frontier AI capabilities remain both secure and available for trusted uses while preventing their misuse by malicious actors. This Action Plan

is also a call to our international partners to join the efforts to amplify the impact of proposed measures on AI safety and cyber resilience.

In particular, the Commission will pursue these objectives in bilateral and multilateral fora. It will continue to actively engage in the **G7 to promote its approach**, including through the **Digital&Tech and Cybersecurity Working Groups** to support work towards a common understanding of cybersecurity risks stemming from advanced AI capabilities. The Commission will promote G7 cooperation on standards and evaluation of these models. It also invites G7 members and other international partners to join the efforts to support the security of open source software and to cooperate in view of adapting vulnerability management practices. The EU will also continue engaging in the UN.

At bilateral level, the EU will deepen exchanges with partner countries on advanced AI and cybersecurity, including through digital partnerships, digital dialogues, or cyber dialogues and will prioritise model evaluation, protection of critical infrastructure, mitigation of vulnerabilities, and improved cyber resilience as core areas of cooperation as appropriate.

Additionally, the **Network of Advanced AI Measurement, Evaluation and Science, coordinated by the UK AISI** and in close collaboration with the safety and security institutes of partner countries and **the Commission's AI Office,** is an important platform for developing common methodologies for evaluating frontier AI models, exchanging best practices and supporting trusted international cooperation on AI safety and security.

The Commission will also encourage structured dialogue between governments and leading frontier AI developers to promote common approaches to frontier AI security, evaluation and responsible deployment.

Finally, given the mentioned implications for European and national security, the EU will strengthen existing exchanges with **NATO** on opportunities and risks associated with frontier AI capabilities in the cyber domain, including through leveraging the forthcoming NATO's Centre of Excellence on Artificial Intelligence.

6. Conclusion

This Action Plan marks the continuation of a sustained and coordinated European effort. As the development of advanced AI capabilities will continue to accelerate, with new opportunities and risks to emerge, the Commission will regularly assess the implementation of the Action Plan and adapt actions where necessary, to ensure that it contributes effectively to the development of a secure and resilient European ecosystem for the age of AI.