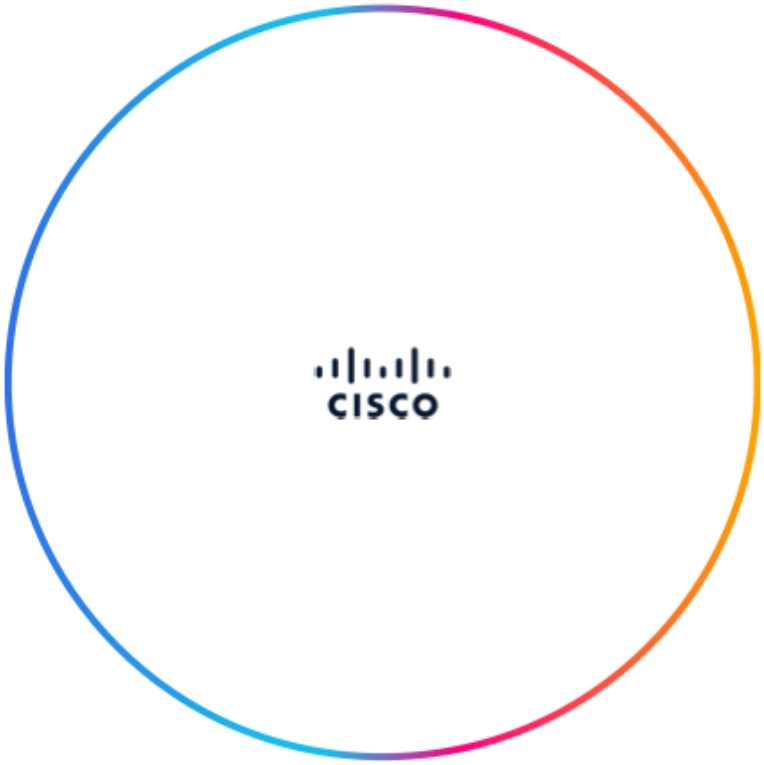

Unlocking the EU AI Potential

Cisco’s recommendations for the AI Continent Action Plan and Cloud and AI Development Act

Contents

EXECUTIVE SUMMARY

The EU AI Continent Action Plan correctly focuses on five key components for achieving a true European AI Continent. This paper follows a similar structure, in suggesting key critical areas to focus future European action on AI, through the Cloud and AI Development Act, the Applied AI Strategy and the deployment of the InvestAI funding scheme.

The EU will benefit from the AI revolution by **strengthening its AI and cloud infrastructure capabilities**. The proposed **AI Factories and Gigafactories** funding schemes are an ambitious step in the right direction, to ensure that Europe builds up its AI and cloud infrastructure. As these new projects will be developed, a fundamental aspect will be to ensure that funding mechanisms and procurement **consider quality criteria such as security, resilience and energy efficiency**. Additionally, European preference clauses should not prevent Europe from accessing the best available technologies. European AI infrastructure will greatly benefit from the flexibility of determining whether sovereignty requirements or approaches would be best suited for specific projects, while in other cases these requirements may not be warranted.

The development of **EU energy infrastructure** will be a fundamental step in ensuring AI success, especially as AI compute demands outpace the addition of new energy generation to the grid. European AI infrastructure would benefit from an approach that focuses on both **efficiency of the energy infrastructure** supporting AI and **access to energy for data centers**. At the same time, grid modernization and diversification of energy sources are key in strengthening the resilience and reliability of the energy infrastructure that will power an AI-driven economy.

The EU AI Continent Action Plan correctly focuses on the need to strengthen the AI and cloud infrastructure of Europe. This is a foundational need for the success of European ambitions on AI. At the same time, **these actions should be accompanied by strong AI security foundations, to ensure the resilience and safety of European AI**. The AI Act recognizes this necessity, and the EU will greatly benefit from taking a **whole-of-value-chain approach to AI security** as it further develops its infrastructure. AI is also a key enabler of security, and the **EU should support the uptake of AI tools in cybersecurity, at the public and private level**, to further strengthen trust in the technology.

AI uptake will be greatly influenced by key policies in key areas. The EU should continue to **foster international data flows**, to ensure access to high quality data for AI. Similarly, it should continue to engage, and strengthen this engagement, in the **development and adoption of international standards**.

While AI infrastructure is essentially foundational to the success of European AI ambition, it cannot truly achieve these objectives without a workforce and population that have the skills to reap the benefits of AI. The **EU Union of Skills program is a cornerstone of European AI development**, and the EU should continue to **foster skilling, reskilling and upskilling programs, especially in partnership with the private sector**.

INTRODUCTION

Cisco Systems, Inc. (Cisco) submits these comments in response to the consultation for the Cloud and AI Development Act, and following the release of the EU AI Continent Action Plan.

Cisco is a global provider of networking, security, observability, and collaboration solutions that power the internet and securely connect people. Cisco connects and protects the AI era. With the trusted infrastructure to power and secure AI, Cisco helps maximize AI's value across the economy. Leveraging its industry-leading expertise, Cisco has developed best practices for designing AI-ready infrastructure[1], whilst developing and deploying cutting-edge AI tools to secure and protect the AI lifecycle, from development to deployment. Cisco has published extensively on AI principles and policy considerations to support the adoption of trustworthy AI. Cisco's journey on responsible AI begun in 2018, when we published our commitment to proactively respect human rights in the design, development, and use of AI. This commitment was formalized in 2022 through the Cisco Responsible AI Principles,[2] which are operationalized by the Cisco Responsible AI Framework. [3] This sets the foundation for our Responsible AI assessment process, modeled after our Privacy and Security assessment processes, whose objective is to identify, understand and mitigate any issues related to Cisco's Responsible AI Principles – transparency, fairness, accountability, reliability, security and privacy.

Cisco is at the forefront of innovation, providing AI-ready networking and data center technologies, AI-enabled cybersecurity, and security solutions to support the trustworthy development and deployment of AI. As a signatory of the EU AI Pact, Cisco has shown strong commitment to the development and deployment of safe and responsible AI in Europe and globally. Cisco is also a signatory of the Rome Call for AI Ethics[4] and aligns with the G7 Hiroshima Process International Guiding Principles for Advanced AI Systems.[5]

Cisco recently launched Foundation AI, a Cisco organization of leading AI and security researchers and engineers dedicated to creating open cutting-edge AI technology to empower cybersecurity applications. Foundation AI's first release is a base model purposefully built for security applications. The model is an 8B parameter model, pre-trained on Llama using publicly-available cybersecurity data. In addition to a base model, Cisco will be releasing a model with reasoning capabilities designed to understand the complex relationships and context within security data, enabling more sophisticated analysis and decision-making.

As Cisco observed in its recent AI Briefing: CEO Edition, 97% of CEOs say they are planning an AI integration, but only 1.7% report they are fully ready to do so.[6] Similarly, Cisco's 2024 AI Readiness Index, found that only 6% of organizations in the European Union consider themselves to be AI-ready.[7] These findings indicate

---

[1] Cisco Systems, Inc., *Cisco Data Center Networking Blueprint for AI/ML Applications* (March 2024), https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/cisco-data-center-networking-blueprint-for-ai-ml-applications.html.

[2] Cisco Systems, Inc., *Cisco Responsible Artificial Intelligence Principles* (2024), https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-responsible-artificial-intelligence-principles.pdf.

[3] Cisco Systems, Inc., *Cisco Responsible Artificial Intelligence Framework* (2024), https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-responsible-artificial-intelligence-framework.pdf.

[4] RenAIssance Foundation, Rome Call for AI Ethics, Rome Call | What is the Matter with AI Ethics? (Last visited May 21, 2025)

[5] Ministry of Foreign Affairs of Japan, Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI System, 100573471.pdf (Last visited May 21, 2025)

[6] Cisco Systems, Inc., *Cisco Study: CEOs Embrace AI, but Knowledge Gaps Threaten Strategic Decisions and Growth* (Feb. 2025), https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2025/m02/cisco-study-ceos-embrace-ai-but-knowledge-gaps-threaten-strategic-decisions-and-growth.html.

[7] Cisco Systems, Inc., *AI Readiness Index* (2024), https://www.cisco.com/c/m/en_us/solutions/ai/readiness-index.html.

that companies may not be prepared to leverage AI to its full potential. Infrastructure limitations, security concerns, and skills and knowledge gaps are the main barriers.[8] While there are undoubtedly challenges to the unlocking of the benefits of AI across the EU economy, there are clear actions which the EU, its Member States and the private sector can partner on to address these barriers and sustain European competitiveness and growth in AI. Cisco welcomes the opportunity to assist the European Commission in identifying actions that strengthen AI innovation, encourage secure deployment of AI, and support European competitiveness.

The consultations on the AI Continent Action Plan and possible Cloud and AI Development Act come at a critical juncture for Europe, and Cisco would like to offer comments and recommendations to reap the benefits of cloud and AI. Against this context, this submission goes beyond the scope of the proposed questions for the consultation, as Cisco strongly believes that while compute capacity, energy efficiency and access and cloud and AI policy are fundamental keystones for Europe's ambitions, there are other areas that are equally important, and should be considered holistically in preparing future EU actions in this space. In particular, ensuring the security and resilience of cloud and AI infrastructure, empowering European networks and especially skills will be fundamental to unlock Europe's AI potential. While these issues are partially addressed in other European Commission initiatives, Cisco would recommend recognizing their importance also in the context of AI and Cloud-specific projects and programs.

[8] Cisco Systems, Inc. *supra* note 6.

I. INFRASTRUCTURE NEEDED FOR AI GROWTH

Robust digital, physical, and energy infrastructure is necessary to develop and deploy AI across all sectors of the EU economy. Cisco plays a pivotal role in AI infrastructure by providing scalable and secure solutions that support the increasing demands of AI workloads.[9] Cisco's AI-native infrastructure is designed to enhance data center operations, offering integrated systems that simplify AI deployment and management. These solutions are part of Cisco's broader strategy to connect people everywhere to the internet and the digital tools they need to succeed.

A. Support investments in and buildout of data centers, high-speed connectivity infrastructure, and high-performance networks

Digitization of the global economy and growing adoption of data-intensive technologies like AI require infrastructure that can securely hold and quickly transfer vast amounts of data. This AI-native infrastructure at the edge, cloud and data center includes components like routers, switches, processors, storage devices, and servers, as well as data center and network management solutions and systems for power and cooling. EU public and private sector organizations need to ensure they are equipped with infrastructure that can keep pace with increasing AI workloads.

The AI Continent Action Plan correctly recognizes the need to invest in European capabilities from an AI infrastructure perspective. To reinforce this pressing necessity, the Cisco AI Readiness Index found that only 8% of business leaders in the EU believe their organizations to be ready from an infrastructure perspective, versus 15% globally. The planned AI Factories and Gigafactories investment projects have the potential to address the urgent need for AI infrastructure in Europe.

Data centers – from the hyperscale to the modular level – are critical to support AI innovation and adoption. Cisco is supporting AI data centers through our accelerated compute, network fabric, and hyperscale fabric solutions. Cisco shares the AI Continent Action Plan's ambition of tripling EU data centers in the next 5 to 7 years, which would be a key step in ensuring the EU can achieve its Digital Decade objectives.

It will also be critical for the EU to consider the burgeoning influence of edge AI and the proliferation of IoT devices. Edge AI, by processing data closer to its source, significantly alters traditional AI workload distribution, shifting processing from centralized data centers to distributed edge devices. This shift not only impacts network traffic patterns but also introduces novel cybersecurity challenges.[10]

The AI Continent Action Plan sets very ambitious targets for an AI-ready Europe, and Cisco is strongly supportive of these objectives. The EU will need to ensure that European companies and citizens can continue to access and leverage the most advanced AI technologies, in particular from an infrastructure perspective. AI's potential can be fully realized through a hybrid approach that leverages both global public cloud capabilities and local specificities. AI relies on vast amounts of data and computational power, primarily housed in public cloud infrastructures. Public cloud is the indispensable starting point, providing the scalable infrastructure needed to support AI's demands. For example, the initial training and development of large

---

[9] With products like the Cisco UCS X-Series Modular System, Nexus 9000 Series Switches and Intersight Cisco ensures high-performance computing, networking and management capabilities essential for AI applications.

[10] With millions of IoT devices generating and processing data at the edge, the attack surface could expand exponentially, necessitating robust security protocols and real-time threat detection capabilities. Scalable solutions at the network's edge, like Cisco's Secure DDoS Edge Protection on routers, can detect and mitigate attacks in real time, keeping attack traffic off the network. *See* Cisco Systems, Inc., *Cisco Secure DDoS Edge Protection Technical White Paper* (Jan. 25 2023), https://www.cisco.com/c/en/us/products/collateral/security/secure-ddos-protection/secure-edge-protection-tech-wp.html.

language models will largely continue to happen on public cloud infrastructure. While public cloud provides the necessary backbone, the true power of AI emerges when models are refined and tailored to specific local and industry needs, and addressing government and customer expectations on governance, dataset training and data and infrastructure location. The choice to require certain AI or cloud infrastructure to be provided by local companies must be guided by the specific needs of the data and the desired outcomes. Certain use cases, particularly those involving highly sensitive data (e.g. central government, defense), may benefit from local cloud solutions that prioritize local control, and are tailored to specific governance frameworks. Cisco works with European and non-European companies along the cloud and AI stack, providing services that are tailored to different specificities as above. Against this background, Cisco cautions against including European preference clauses in the upcoming CAIDA, which would likely have the unintended consequence of limiting access to cutting-edge technologies and hampering the EU's ambitions for an AI-ready continent. European ambitions in AI will truly be realized only if businesses and public sector are provided with flexible options that are adaptable to their needs, which may shift and not always overlap.

Networks must have the right hardware, software, architecture and configuration to facilitate the rapid exchange and processing of data and prevent bottlenecks that would impede AI training efficiency and use of AI applications in real-time. High-throughput and low-latency networks help to avoid packet drops which can disrupt the deployment of time-sensitive AI applications.[11] Overall, AI models need scalable and reliable network connectivity. While centralized networking can support the massive requirements for AI training, a more distributed network transport model will be required for real-time inferencing applications – often occurring closer to the end user and data sources.[12] AI will continue to transform the flow of traffic across networks. Downstream traffic is expected to increase as AI applications often require substantial data inputs from cloud-based services to deliver personalized and real-time responses to users. Upstream traffic is also likely to increase due to AI-driven devices collecting and transmitting data for processing and analysis. Overall increases in downstream and upstream traffic will require greater bandwidth. Cisco has developed our Agile Services Networking solution to enhance the deployment and performance of AI applications by optimizing and modernizing network infrastructures to meet the demand for high-bandwidth and secure connectivity necessary for AI.

Current EU connectivity infrastructure may be ill-equipped to handle this rising demand. According to Cisco's 2024 AI Readiness Index, 66% of EU respondents acknowledged their infrastructure has limited or moderate scalability and flexibility to accommodate the increasing demands from AI.[13] As the volume and complexity of AI data flows increase, it will be critical for the European Commission to help address challenges related to legacy infrastructure. Outdated infrastructure is more vulnerable to security threats and can be an inhibitor to AI adoption, as legacy systems often have performance limitations and lack the capacity to handle the data and the high-speed processing that AI applications require. Public and private sector organizations will need to consider how to identify, prioritize, and replace equipment that has reached its end of life. The EU has created a strong legal framework to require critical infrastructure operators to adopt cybersecurity measures (NIS 2) and for manufacturers to ensure their products are supported (CRA). A binding measure to identify obsolete assets, replace them by default and mitigate those that cannot be removed in the near term would address the gap between these regulations.

Reliable internet access is vital for deploying AI tools and ensuring their accessibility to end-users. High-speed, low-latency broadband is key to realizing the return on investment from AI technologies, as it enables

---

[11] Cisco Systems, Inc. *supra* note 1.

[12] Rakesh Chopra, *A Service Provider Architecture for AI-Ready Connectivity*, Cisco Blogs (Feb. 10 2025) https://blogs.cisco.com/sp/a-service-provider-architecture-for-ai-ready-connectivity.

[13] Cisco Systems, Inc., *supra* note 7.

individuals and businesses to leverage AI tools effectively in real-time. However, only 18.5% of households had gigabit connection in 2024.[14] Broadband access has been shown to boost the productivity of workers and businesses and to improve market access, strengthening economic competitiveness.[15] Cisco is focused on improving the cost of broadband deployment[16] and supports the EU's efforts to close the digital divide and connect all Europeans to vital internet resources.

Additionally, one of the major challenges broadband providers face is the complex and lengthy permitting requirements. We welcome the EU Gigabit Infrastructure Act adopted in 2024 that is looking at removing these barriers and ensuring that connectivity infrastructure keeps pace with technological advances.

Ensuring that all Europeans have access to AI technology will help strengthen and grow the EU economy. We encourage the European Commission and EU Member States to promote policies that enable investment in data centers, broadband infrastructure, and the development of future-proofed networks. To this end, the European Commission should:

- Encourage strategic investments in new data center capacity as well as the modernization of legacy data centers, looking at quality criteria such as security, resilience and energy efficiency;
- Promote best practices for building AI-ready networks;[17]
- Strengthen European AI and cloud infrastructure by ensuring that flexible funding mechanisms are available, reflecting the need for both sovereign and public cloud services in Europe;
- Enact binding measures to identify obsolete assets on critical networks infrastructure, with the objective of replacing them or mitigating those that cannot be removed in the near term;
- Incentivize broadband investments and ensuring that they are implemented efficiently and quickly to ensure all Europeans have access to AI tools; and
- Review the Digital Decade targets, implement the Gigabit Infrastructure Act as soon as possible and continue to further streamline regulatory requirements with permitting agencies to expedite the construction of data centers and the deployment of high-speed broadband to all Europeans.

B. Ensure data centers have reliable and affordable energy and energy efficient technology

Modern data centers for AI applications require reliable energy to power complex processing operations and to provide adequate cooling systems.[18] While Europe has one of the most interconnected and resilient electricity grids of the world, electricity consumption driven by the deployment of data centers is expected to increase by around 60% between now and 2030[19]. Moreover, the electricity grid needs the capacity to accommodate more distributed and variable energy sources and to withstand extreme weather impacts. Aging infrastructure also carries a higher risk of failure that could negatively impact local communities. Given

---

[14] European Commission, State of the Digital Decade 2024, https://digital-strategy.ec.europa.eu/en/factpages/state-digital-decade-2024-report

[15] Bert Kroese, *Can Internet Access Lead to Improved Economic Outcomes?,* World Bank Blogs (April 5, 2022), https://blogs.worldbank.org/en/digital-development/can-internet-access-lead-improved-economic-outcomes.

[16] Cisco Routed PON, which simplifies service providers' end-to-end architecture, helps to lower operating expenses. *See* Bill Gartner, *Transforming the Economics of Superfast Broadband with Cisco Routed PON*, Cisco Blogs (March 15 2024), https://blogs.cisco.com/sp/transforming-the-economics-of-superfast-broadband-with-cisco-routed-pon.

[17] Cisco Systems, Inc. *supra* note 1.

[18] Electricity and water are critical resources for the power subsystems, as well as uninterruptible power supplies, ventilation and cooling systems, fire suppression, and backup generators in data center facilities.

[19] European Commission, EU Action Plan for Grids, 2023

the establishment of data centers as critical infrastructure, ensuring data centers have reliable and affordable energy is a challenge governments and industry must work together to meet.

AI currently accounts for less than one-fifth of total data center energy demand globally, but this share is expected to grow rapidly in the coming years.[20] However, in the medium to long term, AI energy usage and the efficiency gains for digitalization do not have to be at odds and can instead be complementary.[21] With this challenge comes an opportunity to modernize the electricity grid and embed energy efficiency within data center operations to ensure the EU can meet future power demands. An energy grid equipped with digital solutions (such as Cisco's Distribution Automation and Advanced Metering Infrastructure technologies) provides smart monitoring and energy management capabilities for intermittent and distributed generation to ensure efficient and reliable power delivery, advanced analytics to manage load shedding and peak shaving, and automated data collection to reduce maintenance costs.[22]

Data centers can also reduce energy costs and maximize resources with energy efficient technology. [23] Through its future Sustainability Rating Scheme of Data Centers, the European Commission should promote the use of energy efficient IT equipment in data centers (e.g., routers, servers, and processors) and complementary Operational Technology (OT) to help reduce energy consumption and lower the costs from AI workloads. This should be a priority for all new data center capacity but there is also an opportunity to reap the benefits of energy efficient technology by modernizing legacy systems.

EU energy infrastructure development is crucial as AI compute demands outpace the addition of new energy generation to the grid. The EU Commission should adopt a dual approach that accelerates energy acquisition but also enhances the efficiency of technology infrastructures supporting AI. Initiatives that enhance the efficiency of data center hardware and software, optimize algorithms for reduced computational load, and foster research into computing paradigms that minimize energy consumption should be prioritized. Simultaneously, strategic investments in grid modernization and diverse energy sources are crucial to ensure reliable power delivery to support an AI-driven economy. To strengthen the resiliency of EU energy grid for AI and to achieve the objectives outlined in EU grid initiative, the European Commission should:

- Encourage investment in grid modernization in the future EU grid initiative through the use of grid enhancing technologies;
- Encourage Member States to finalize the implementation of NIS2 as soon as possible for modernization efforts to include security in the underlying control network as attacks on the power grid are easier than attacking the hardened security of the data center;
- Encourage in the future Sustainability Rating Scheme for Data Centers the use of energy efficient ICT equipment in data centers to maximize available energy; and consider developing fiscal incentives to support the use of energy-efficient hardware;
- Harmonize regulatory requirements related to energy efficiency and sustainability of data centers across Europe to facilitate modernization and addition of diverse energy sources – including lower and no-carbon sources – to the grid.

---

[20] Nature Climate Change, *Aligning artificial intelligence with climate change mitigation,* 2022

[21] Global Counsel, *Enabling Digital efficiency,* February 2025

[22] Cisco Systems Inc., *Digitize the Power Automation Grid Reliably, Safely, and Efficiently* (2023), https://www.cisco.com/c/dam/en/us/solutions/global-partners/cisco-se-grid-modernization-so-r2.pdf.

[23] *See* Cisco Systems Inc, *Comments of Cisco Systems Inc.*, National Telecommunications and Information Administration and U.S. Department of Energy Request for Comments on Bolstering Data Center Growth, Resilience, and Security (Docket No. NTIA-2024-0002) (Nov. 4 2024), https://www.regulations.gov/comment/NTIA-2024-0002-0027

II. STRENGTHENING EU CYBERSECURITY AND RESILIENCE WITH AI

Although cyber threats are constantly evolving, the increasingly sophisticated threats introduced by AI necessitate a paradigm shift in how organizations approach cybersecurity. Cisco is integrating AI across the network, cloud, and endpoints to provide comprehensive protection by improving threat detection, prediction, and response. This approach not only assists security teams by simplifying management and improving outcomes but also augments human insight, allowing cybersecurity teams to operate at machine speed and focus on critical tasks.

To achieve a truly resilient AI Continent, the EU should encourage strong AI cybersecurity policies and funding programs, which would ensure that the growing AI infrastructure is secure and protected. This should not be considered a secondary requirement, following investments in infrastructure, but rather a primary necessity as infrastructure projects are approved and launched. As AI is then designed, developed and deployed in Europe, it can benefit from a resilient infrastructure, but will need equally strong cybersecurity policies to ensure that Europeans can safely reap the benefits of the AI revolution.

A. Strengthen EU AI resilience through AI value-chain risk management and protection

Attackers are focused on targeting infrastructure supporting AI systems and applications, particularly on the unique vulnerabilities of AI deployment environments. Compromises in AI infrastructure could result in cascading effects that can impact multiple systems and customers simultaneously, and attackers can proceed to conduct additional operations targeting model training jobs and model architecture, models' training data and configurations, hijacking expensive computational resources, data exfiltration, or numerous other end goals. Addressing security risk to AI models, systems, and applications themselves is an overlooked aspect of the AI development lifecycle.

The AI ecosystem's reliance on shared models, datasets, and libraries expands the attack surface into the AI supply chain. Supply chain attacks exploit the trust organizations place in third-party components—whether they be pre- trained models, open-source libraries, or datasets used to train AI systems. When parts of the supply chain are compromised, it can introduce hidden vulnerabilities that may not be discovered until significant damage has been done. Adversaries targeting an AI system's building blocks and related components can be particularly concerning due to their potential for widespread impact across multiple downstream applications and systems.

The Cisco State of AI Security[24] found several examples of attacks that have successfully targeted parts of the AI value-chain, for example through direct prompt injection (i.e. a technique used to manipulate model responses through specific inputs to alter its behavior and circumvent an AI model's built-in safety measures and guardrails, usually to re-task an LLM or LLM application to conduct some other task) or training data extraction and tampering.

To strengthen the protection of its AI value chain, the EU and its Member States should:

- Support strong cybersecurity policies in its investment projects, for example by requiring risk management policies be put in place for successfully projects;
- Encourage strong AI security postures by upholding internationally recognized security standards and risk management frameworks, such as the NIST AI Risk Management Framework, OWASP Top 10 vulnerability lists, and the MITRE ATLAS matrix;

[24] Cisco Systems, State of AI Security, The State AI Security Report (last visited May 8, 2025)

- Support education programs for the workforce, especially for companies directly involved in the management of the AI value chain, for the safe and responsible usage of AI.

B. Support deployment of AI-enabled cybersecurity to address growing threat landscape

In the face of an increasingly complex cyber threat landscape, AI-enabled cybersecurity solutions will be critical for protecting EU economic and security interests. AI can quickly analyze vast amounts of data, enabling the identification of anomalies that may signal a cyberattack or the detection of malicious code. Moreover, by automating incident response, AI can also significantly reduce response times and tailor security policies to specific organizational needs. However, the future of AI-enabled cybersecurity lies in its ability to help organizations evolve from reactive remediation to proactive prediction and prevention. With the analytical power of AI, cybersecurity tools can identify potential vulnerabilities and forecast cyberattack patterns so that an organization can strengthen its cybersecurity posture before attacks occur.

AI tools in cybersecurity can provide an edge in ensuring the highest level of protection for EU businesses, governments and citizens. At a time when the threat landscape is evolving at a frantic pace, AI-powered cybersecurity tools can make the difference in ensuring a resilient Europe. Encouraging the uptake of AI-powered cybersecurity tools is not only an ambitious economic objective, it is an imperative necessity to protect Europe.

Policymakers can facilitate these advancements by promoting an innovation-friendly regulatory environment that gives cyber defenders the flexibility to address dynamic cyber threats. To ensure that AI is integrated into cybersecurity solutions in a secure and resilient manner, the EU should:

- Collaborate with the private sector to develop guidance and encourage uptake of internationally recognized standards that define how AI systems and AI-powered technologies are securely deployed; and
- Ensure that AI systems embedded into cybersecurity solutions are not considered high-risk under the AI Act and subject to restrictive regulatory requirements that inhibit the ability of companies to innovate to address emerging threats.

C. Leverage generative AI to enhance cybersecurity and expand cyber workforce capabilities

Generative AI (GenAI) is playing an important role in modernizing cybersecurity operations and expanding workforce capabilities. GenAI enhances system usability and democratizes access to advanced security tools, simplifying complex cybersecurity management tasks through natural language processing. For example, GenAI embedded in Cisco's AI Assistant Firewall allows users to configure firewalls with natural language, eliminating the need for technical command-line syntax. This innovation not only lowers the barrier to entry for non-experts but also enhances the efficiency of security operations centers (SOCs).[25] The recently announced Cisco AI Canvas[26] brings together AI tools used for SOCs and leverages both Generative AI and Agentic AI to provide a comprehensive system overview, while ensuring human oversight. These tools

[25] Cisco's SOC Assistant provides comprehensive situation analysis for SOC analysts, correlating intel across the Cisco Security Cloud platform solutions, relaying potential impacts, and providing recommended actions which reduces the time needed for SOC teams to respond to potential threats. *See* Cisco Systems, Inc., *Cisco Unveils Next-Gen Solutions that Empower Security and Productivity with Generative AI* (Aug. 29, 2023), https://investor.cisco.com/news/news-details/2023/Cisco-Unveils-Next-Gen-Solutions-that-Empower-Security-and-Productivity-with-Generative-AI/default.aspx.

[26] Cisco Systems Inc., Announcing Cisco AI Canvas. Revolutionizing IT with AgenticOps. Announcing Cisco AI Canvas. Revolutionizing IT with AgenticOps

will be fundamental in shepherding the AI revolution, showing clear value in industrial uses whilst providing the best cybersecurity protection.

Leveraging security systems with intuitive GenAI interfaces can help expand the pool of cybersecurity talent with less extensive training.[27] To realize the benefits of GenAI for cybersecurity, the EU should:

- Encourage adoption of cybersecurity systems with GenAI interfaces; and
- Promote the use of GenAI to help address shortages of cybersecurity professionals.

D. Promote regulatory alignment and compatibility to boost adoption of AI-enabled security

Regulatory alignment across markets is essential for the widespread and trustworthy adoption of AI, particularly in critical sectors like cybersecurity. The AI Act correctly clarifies that AI systems used for cybersecurity purposes should not be considered high-risk[28], focusing instead on ensuring that high-risk systems have cybersecurity and robustness requirements.[29] The EU should be a proponent of this approach in its international engagements.

Divergent and conflicting regulations create a complex landscape for businesses, hindering innovation and impeding the deployment of vital AI-powered security solutions. Uniform, risk-based, non-regulatory frameworks – for example those based on international standards – would foster trust, streamline compliance, and enable the rapid deployment of AI-driven cybersecurity tools, promoting a robust, globally competitive AI ecosystem. The EU should:

- Continue to work with strategic partners and allies to align security certifications to accept internationally recognized schemes for certification, attestation, and verification of products and services to reduce the need for duplication of resources in different countries for these checks; and
- Encourage mutual recognition of certification regimes that are substantially similar and discourage the adoption of local requirements that differ from internationally recognized standards.

[27] Cisco Systems, Inc., *Close the Cybersecurity Workforce Gap with AI Position Paper* (May 3 2024), https://www.cisco.com/c/en/us/products/collateral/security/xdr/close-cybersecurity-workforce-gap-with-ai.html.

[28] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act), Recital 54.

[29] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act), Article 15.

III. SECURING AI TO SUPPORT INNOVATION

As AI development and deployment evolves across sectors and use cases, robust security is crucial for supporting innovation that protects national security and promotes economic growth. Trustworthy AI encourages adoption by businesses, underscoring the importance of robust security measures. Safe AI development aligned with human values fosters public trust and supports national security and stability. Without proper safeguards and standards, unintended AI behaviors could harm businesses and security, highlighting the need for AI guardrails and security research. Cisco is committed to protecting AI transformation by developing solutions like Cisco AI Defense designed to continuously detect and protect against emerging threats in AI applications without compromising speed or safety.

As mentioned above, the EU AI Act provides for strong cybersecurity requirements for high-risk AI systems and General Purpose AI models. These requirements are key to ensure that AI models and systems are built with strong safeguards that can deliver innovative products while keeping high cybersecurity standards. In this context, it will be key to align the standardization work required under the AI Act with existing international standards, to ensure that European standards reflect the highest quality requirements and are interoperable with existing international consensus.

A. Support industry-backed technological solutions to secure AI

While integration of AI systems will undoubtedly unlock new innovations and efficiencies across the EU economy, AI systems can also introduce new risks. AI applications add a new layer to the technology stack in the form of models. Additionally, most organizations use multiple models across public and private clouds. This multi-model and multi-cloud landscape will require governments and private sector organizations alike to take a new approach to security. AI-associated risks—like data leakage, data poisoning, training data extraction,[30] prompt injection, and insecure outputs handling—will need to be addressed. Additionally, threats from external actors seeking to exploit vulnerabilities to steal confidential data or otherwise compromise security must be mitigated to reduce risk and liability to businesses and EU security.

The release of the DeepSeek R1 model exemplifies these challenges, highlighting deficiencies in model security, as demonstrated by Cisco and the University of Pennsylvania's research on prompt injection vulnerabilities.[31] This research revealed a 100% success rate in jailbreaking the model, underscoring that there are important risk appetite considerations for organizations adopting AI. High performing models do not always equal highly secure models. This highlights the broader issue of commoditized access to model development, which can result in a proliferation of new models with heightened risks and unreliability due to uncertain provenance and unclear data governance. While all AI models can make mistakes, poor security can exacerbate those risks. Developers and deployers of AI models need to have a comprehensive understanding of where those weaknesses and vulnerabilities are and a willingness to fix any identified problems. Technological solutions can help mitigate these risks. Innovations like automated red teaming can

[30] Cisco's AI research has shown that there are simple methods bad actors can use to extract memorized training data from chatbots, which – if replicable at scale – could have widespread security implications for AI models that are trained on sensitive or proprietary data. *See* Amy Chang, *Extracting Training Data From Chatbots*, Cisco Blogs (Sept. 20 2024) https://blogs.cisco.com/security/extracting-training-data-from-chatbots.

[31] Gopal Devarajan, *Evaluating Security Risk in DeepSeek and Other Frontier Reasoning Models*, Cisco Blogs (Oct. 17 2024), https://blogs.cisco.com/security/evaluating-security-risk-in-deepseek-and-other-frontier-reasoning-models

provide continuous testing and validation of AI models to block adversarial attacks. Real-time protection for AI models, such as through Cisco AI Defense, [32] is critical to securely deploying AI in enterprise environments.

Furthermore, it will be important to ensure that models and applications adhere to existing compliance obligations, a growing challenge as AI-powered application development becomes accessible to a wider audience, including non-traditional developers like healthcare and education professionals. As the pool of developers expands, technology is essential to maintain compliance and monitor the usage of AI models over time, ensuring they remain aligned with security and operational standards. Cisco AI Defense plays a crucial role in this process by providing robust tools and frameworks that help developers adhere to compliance requirements and continuously monitor AI applications.

To support the secure development and deployment of AI, the EU should:

- Ensure that the EU AI Office cooperates with international counterparts to support the uptake of internationally recognized standards and practices in AI cybersecurity and risk management;
- Collaborate with the private sector to support pre- and post- deployment testing of AI models and encourage automated red teaming and the validation of AI systems;
- Promote instruments similar to the NIST Adversarial Machine Learning (AML) taxonomy[33]; and
- Work with private sector stakeholders[34] and support broad business participation in AI standards discussions to ensure technological neutrality, facilitate market access, and reduce duplicative compliance obligations for businesses.

B. Work with industry to secure AI models' supply chains

Development and deployment of open-source models has aided businesses in accelerating AI adoption and helped developers have access to cutting-edge technology to experiment and innovate. However, all organizations should understand the potential risks and vulnerabilities associated with third-party software, AI models, and data. Threat actors have numerous opportunities to create vulnerabilities in AI models such as through the introduction of corrupted data into training datasets or the injection of malicious code in open-source AI repositories. Already industry and its partners are working together to develop methodologies and technologies to assess and mitigate risks in AI models' supply chains.[35] The EU should:

- Task ENISA to work with stakeholders to evaluate weaknesses in publicly available AI models, publish findings and help promote market-based solutions to address these risks.

---

[32] Cisco AI Defense provides two key elements of AI protection: protecting against the risk of sensitive data exposure from employees using third-party systems and sharing IP or other confidential information with AI tools and protecting the development of AI models through validation identification of vulnerabilities, and application of guardrails. *See* Jeetu Patel, *Protecting AI so AI Can Improve the World, Safely*, Cisco Blogs (Jan. 15 2025), https://blogs.cisco.com/news/you-cant-sacrifice-ai-safety-for-ai-speed.

[33] Cisco Systems, Inc., Alie Fordyce & Hyrum Anderson, *Cisco Co-Authors Update to the NIST Adversarial Machine Learning Taxonomy*, https://blogs.cisco.com/security/cisco-co-authors-update-to-nist-adversarial-machine-learning-taxonomy.

[34] The NIST AML taxonomy was developed in partnership with Cisco, NIST, and the UK AI Security Institute and is a successful example of multi-stakeholder collaboration on standards that supports U.S. businesses.

[35] MITRE, *MITRE and Robust Intelligence Tackle AI Supply Chain Risks* (Sept. 27 2023), https://www.mitre.org/news-insights/news-release/mitre-and-robust-intelligence-tackle-ai-supply-chain-risks; and Robust Intelligence, *Robust Intelligence Partners with MITRE to Tackle AI Supply Chain Risks in Open Source Models* (Sept. 27 2023), https://www.robustintelligence.com/blog-posts/robust-intelligence-partners-with-mitre-to-tackle-ai-supply-chain-risks-in-open-source-models.

IV. KEY ENABLERS FOR AN AI CONTINENT

Development of leading AI systems and solutions will require key enablers to be put in place to ensure that public and private sector organizations can maximize use of AI to support industry-wide innovation and economic growth.

A. Support AI development by updating EU rules on processing of data

In order to enable a thriving AI ecosystem in Europe, it is important that GDPR is fit for purpose. A key concern in the current regime is the legal grounds for repurposing personal data for further use. When such further use is envisaged, data controllers are required to either justify it via a compatibility assessment, or revert to obtaining consent. We recommend that the full range of legal grounds for processing personal data under Article 6 should remain available, to fully unlock European potential for AI training, especially in key sectors where the quality of European data is of paramount importance, for example healthcare.

B. Enable cross-border data flows to support innovation and market access

Over the past few years, there has been a growing trend of national governments adopting data localization policies. These policies create barriers to international data flows, hindering companies in their efforts to innovate, leverage AI to strengthen security, and scale data-based products and services to new markets. In fact, numerous independent studies demonstrate the negative impacts of data localization requirements, including: increasing data storage costs; reducing trade volumes; reducing innovation and competitiveness; increased costs for goods and services; and increased regional compliance costs.[36] Moreover, data localization mandates can result in siloed data in remote places offering less opportunity for monitoring, detecting, and remediating cyber intrusions. To support EU competitiveness, the EU should:

- Strengthen the existing international data flows EU policy, in particular by increasing the number of adequacy decisions for international data transfers;
- Foster a multilateral approach to recognizing personal data transfers by way of reference to an international, principle-based standard, such as the OECD Privacy Guidelines and Global Cross Border Privacy Rules;
- Deepen transatlantic data flows by finalizing the EU-US CLOUD Act negotiations;
- Oppose overly restrictive data localization mandates that limit market access, including by negotiating and enforcing provisions in digital trade chapters with trading partners; and
- Seek digital trade provisions that support cross-border data flows, prevent governments from requiring source code as a condition of market access, and ensure non-discriminatory treatment of digital goods and services.

C. Consider options to protect curated AI datasets

AI models are only as good as the data they learn from. Data (personal, enterprise, public) and methods applied to enrich it form the foundation that drives the accuracy, efficiency, and reliability of models. Organizations devote significant resources to creating AI/ML models and training data, which can cost

[36] Nigel Cory & Luke Dascoli, *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them,* Info. Tech. & Innovation Found. (July 2021), https://www2.itif.org/2021-data-localization.pdf; Conan French et al., *Data Localization: Costs, Tradeoffs, and Impacts Across the Economy,* Inst. for Int'l Fin, (Dec. 2020), https://www.iif.com/portals/0/Files/content/Innovation/12_22_2020_data_localization.pdf.

millions of dollars to produce. These datasets are becoming high-value assets for companies. Policymakers should explore what kinds of protections are available for these datasets, including whether intellectual property (IP) protections could and should apply in these situations. Companies are interested in protecting both the data used as inputs and the data that is produced (output) of AI systems, to avoid potential theft in the form of distillation models being trained offshore. The EU should work with stakeholders to come up with ideas to deal with the challenge of how to handle ownership of this data.

D. Lead in the development of global AI standards

Cisco has been a leader in technical standards development since the creation of the internet. As part of our annual investment in research and development, hundreds of Cisco technical experts participate in more than 120 standards development organizations each year. We employ recognized international leaders in standards related to Wi-Fi, security, Internet protocols, optics, software-defined networking, mobility, and numerous other technologies, including AI. The quality of Cisco's contributions is well-recognized within the industry and therefore provides the foundation of many telecommunication standards.

The most important goal of standardization is technical interoperability, which allows web browsers to reach websites, laptops to connect to Wi-Fi, and mobile phones to make calls even though the technology that facilitates each of those connections is provided by many different companies around the world. We encourage the European Commission and European Standardization Organizations, as well as colleagues internationally to continue to serve as global proponents for the open, industry-led, market-driven standardization system at every step of the standardization process. Decades of global experience in standardization have taught us that the open, industry-led, consensus-based model of standardization yields the most innovative and pro-competition outcomes.

Given the dynamic pace of innovation, the EU should support industry-led standards and best practices that allow emerging technologies room to grow. Representation from industry and governments is critical to the development of AI standards that align with common values and support businesses. As the AI Act will rely heavily on standards for compliance, the EU would greatly benefit from aligning these standards with the internationally recognized ones, to further strengthen its position as a global leader and simplify compliance for businesses. The EU should:

- Work with strategic partners and allied countries to increase international collaboration and participation in industry-led standardization processes to help avoid the creation of competing blocs that could lead to global fragmentation on standards; and
- Encourage European Standards Organizations to consider and integrate international AI standards in their standard-making process.

E. Promote digital transformation to support adoption of AI in the public sector

Digital transformation can yield many benefits, including improved and more agile management of resources, better user experience, higher productivity, and reduced costs. Adoption of cloud computing, data analytics, and IoT technologies, creates an AI-ready ecosystem and facilitates the collection, storage, and processing of data, all of which is essential for training and refining AI algorithms. Access to robust, high-quality, and well-structured data is needed for AI to deliver its full potential in enhancing productivity in the public and private sectors.

The Cisco AI Readiness Index found that Culture (i.e. the preparedness of an organization to the changes brought by AI) is a significant weakness for Europe, with only 5% of business leaders estimating full readiness for their organization from a Culture perspective. While the survey collects information from the private

sector, the public sector is similarly placed. The EU should encourage AI adoption at an organizational level, through internal training programs and rewarding uses of AI and successful AI initiatives. AI uptake in the public sector would likely have a positive effect in the private sector too, strengthening trust in the technology and promoting further uptake.

Replacement of legacy equipment and pivoting to the cloud will not only ease delivery of services, helping to close gaps in serving all Europeans, but will also help address some of the energy demand challenges discussed above. At the same time, this shift will also help improve Europe's security posture against potentially disruptive attacks to critical infrastructure by malicious foreign actors. The discovery that state-sponsored actors had successfully prepositioned footholds in EU critical infrastructure systems that deliver electricity and water is a strong indicator that we face unaddressed security risks from technology that has not been effectively patched or in some cases is too old to secure. According to industry association Eurelectric, cyberattacks have doubled between 2020 and 2022 in the power sector, with 48 successful attacks hitting Europe's energy infrastructure in 2022 alone[37]. In this regard we could welcome ProtectEU, the new internal Security Strategy of the EU, to better tackle security threats like terrorism, organised crime, surging cybercrime and attacks against on critical infrastructure[38].

The EU Competitiveness Compass recommends the introduction of European preference in public procurement for strategic sectors and technologies, most likely covering AI and Cloud. We would caution against such requirements. Whichever way they are defined, Local Content Requirements restrain choices for the governments that decide to implement them, generate issues for highly integrated global supply chains, prevent governments from using the most secure technologies and rarely deliver the expected results for local growth in the long-term.

To ensure the EU and its Member States can securely harness the benefits of AI to make the provision of public services more effective and efficient, it should:

- Encourage the digitalization of the public sector by prioritizing cloud migration and modernization of legacy infrastructure;
- Develop an effective data strategy that breaks down fragmented data sets and encourages interoperability of data to support creation of high-quality data sets for AI;
- Encourage the breaking of data silos within public sector organizations, to fully unlock the data potential of Europe for AI training, development and deployment;
- Modernize EU public procurement processes, focusing on pre-tender engagement to help contracting authorities gain a comprehensive understanding of emerging technological solutions and market dynamics;
- Refrain from introducing broad European preference clauses in public procurement for strategic sectors and technologies, especially covering AI and Cloud.

[37] Eurelectric, Cybersecurity in the Power sector, 21 February 2025, https://www.eurelectric.org/in-detail/cybersecurity-in-the-power-sector/

[38] EU Commission, ProtectEU, April 2025, https://home-affairs.ec.europa.eu/news/commission-presents-protecteu-internal-security-strategy-2025-04-01_en#:~:text=The%20ProtectEU%20Strategy%20aims%20to,in%20all%20future%20EU%20policies.

F. Invest in digital skills and workforce development for AI uptake

AI will drive significant economic shifts, reshaping industries, labor markets, and competitiveness. Workforce reskilling is key to staying competitive and ensuring a smooth transition to new opportunities while traditional workflows are disrupted. Harnessing AI's transformative potential will require cultivating digital skills and an AI-ready workforce.

A report from the Cisco-led AI ICT Workforce Consortium found that 92% of technology jobs analyzed are expected to undergo either high or moderate transformation due to AI advancements.[39] Additionally, the Cisco AI Readiness Index found that only 9% of EU businesses feeling they have access to the right talent and skills for AI, compared to 21% of US businesses ranking talent ready for the AI age.

Cisco and other tech companies have made significant investments in training workers and students with employer-recognized certifications for high-demand jobs, including cybersecurity. In March 2025, at the launch of the EU Union of Skills, Cisco's CEO Chuck Robbins pledged that the Cisco Networking Academy will equip 1.5 million Europeans with basic digital skills by 2030, and 5,000 instructors on the new competencies professionals need to succeed in AI, cybersecurity, data science, and the digital transformation of industry.[40] Yet, the skills gap in digital skills, and in particular in cybersecurity, persists – and is likely to persist into the future unless we expand the pool of talent from which these roles can be filled. In this regard, we welcome the initiative of the European Commission's Cyber Skills Academy, bringing together public sector, academies and businesses and aiming at addressing the growing cybersecurity skills and talent shortage in Europe. Cisco also welcomes the nascent project of an AI Skills Academy, which should build upon the success of the Cyber Skills Academy and cooperate with leading private sector actors.

Similarly, the EU and the private sector must work together to bridge the gap so that all workers can harness the power of AI and improve productivity. To that end, we support the EU's ambitious Union of Skills program and the recent announcement of new academies, notably for AI and quantum technologies[41]. Therefore, Cisco recommends that the EU institutions:

- Research AI's impact on key industry workforces and share best practices to help companies of all sizes proactively upskill their workforce;
- Continue to initiate public-private partnerships similar to the EU Cyber Skills Academy Network that leverage the technical expertise and insights into workforce demands of the private sector[42];
- Confirm the launch of an AI Skills Academy, building upon the success of the Cyber Skills Academy, and ensure it partners and cooperates with leading private sector actors;
- Encourage and enshrine skills-based hiring practices in both the private and public sectors.

---

[39] Cisco Systems, Inc., *AI-Enabled ICT Workforce Consortium*, https://www.cisco.com/c/m/ai-enabled-ict-workforce-consortium.html (last visited March 11 2025).

[40] Cisco Systems, Inc. Union of Skills: Cisco to Equip 1.5 Million People in the EU with Digital Skills by 2030, Union of Skills: Cisco to Equip 1.5 Million People in the EU with Digital Skills by 2030 - Cisco News The EMEA Network (last visited May 7, 2025)

[41] European Commission, New digital Academies, https://digital-strategy.ec.europa.eu/en/news/new-digital-skills-academies-support-eus-technological-sovereignty-competitiveness-and-preparedness