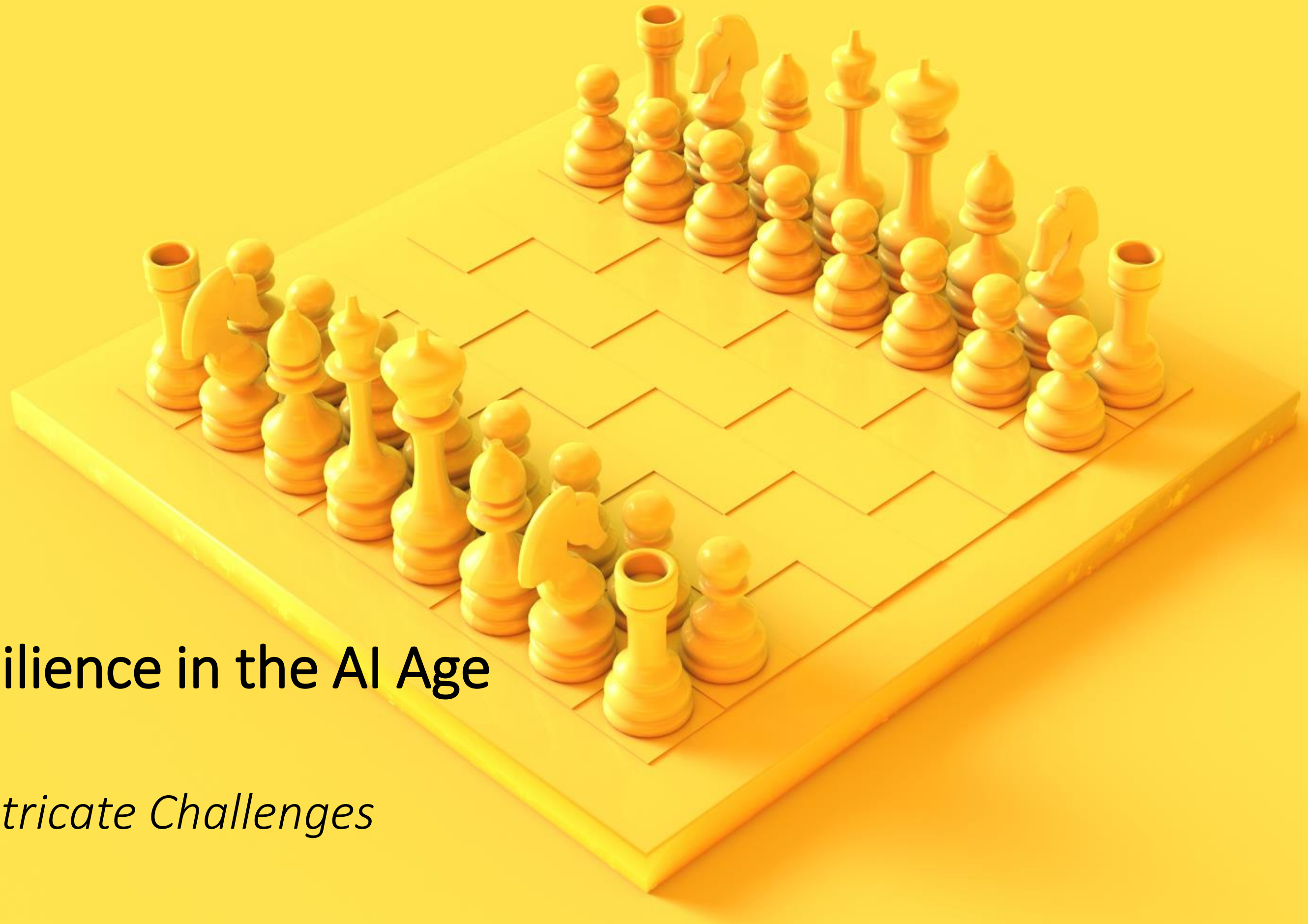
AI & Partners

Amsterdam – London - Singapore



# The EU AI Act

## Traversing Cyber Resilience in the AI Age

*Rounded Solutions for Intricate Challenges*

***November 2024***

# About

AI & Partners

Amsterdam – London - Singapore

For more information on this publication, visit https://www.ai-and-partners.com/.

## About AI & Partners

**'AI That You Can Trust'** - Your trusted advisor for EU AI Act Compliance. Unlock the full potential of artificial intelligence while ensuring compliance with the EU AI Act by partnering with AI & Partners, a leading professional services firm. We specialise in providing comprehensive and tailored software solutions for companies subject to the EU AI Act, guiding them through the intricacies of regulatory requirements and enabling responsible and accountable AI practices. At AI & Partners, we understand the challenges and opportunities that the EU AI Act presents for organisations leveraging AI technologies. Our team of seasoned experts combines in-depth knowledge of AI systems, regulatory frameworks, and industry specific requirements to deliver strategic guidance and practical solutions that align with your business objectives.

To find out how we can help you, email contact@ai-and-partners.com or visit https://www.ai-and-partners.com.

## Business Integrity

AI & Partners defends and extends the digital rights of users at risk around the world.  By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots professional services, regulatory interventions, and participating in industry groups such as AI Commons, we fight for fundamental rights in the artificial intelligence age.

AI & Partners' publications do not necessarily reflect the opinions of its clients, partners and/or stakeholders.

This document is published by AI & Partners as part of its ongoing contributions to EU AI Act preparations, insight areas or interactions. The findings, interpretations and conclusions expressed herein are a result of a collaborative process facilitated and endorsed by AI & Partners but whose results do not necessarily represent the views of the AI & Partners, nor the entirety of its Partners or other stakeholders. This was prepared using research produced by the World Economic Forum (WEF).

## Contents

| | |
|---|---|
| Executive Summary | (Slide 4) |
| Introduction | (Slide 5) |
| Cybersecurity Concerns | (Slide 6) |
| Calculating the Impact | (Slide 7 – 8) |
| Conclusion | (Slide 9) |

# Adopt a ‘resilient-by-design’ approach for high-risk AI systems

## As the digital era unfolds, AI brings unparalleled possibilities for economic advancement, operational improvements, and societal progress.

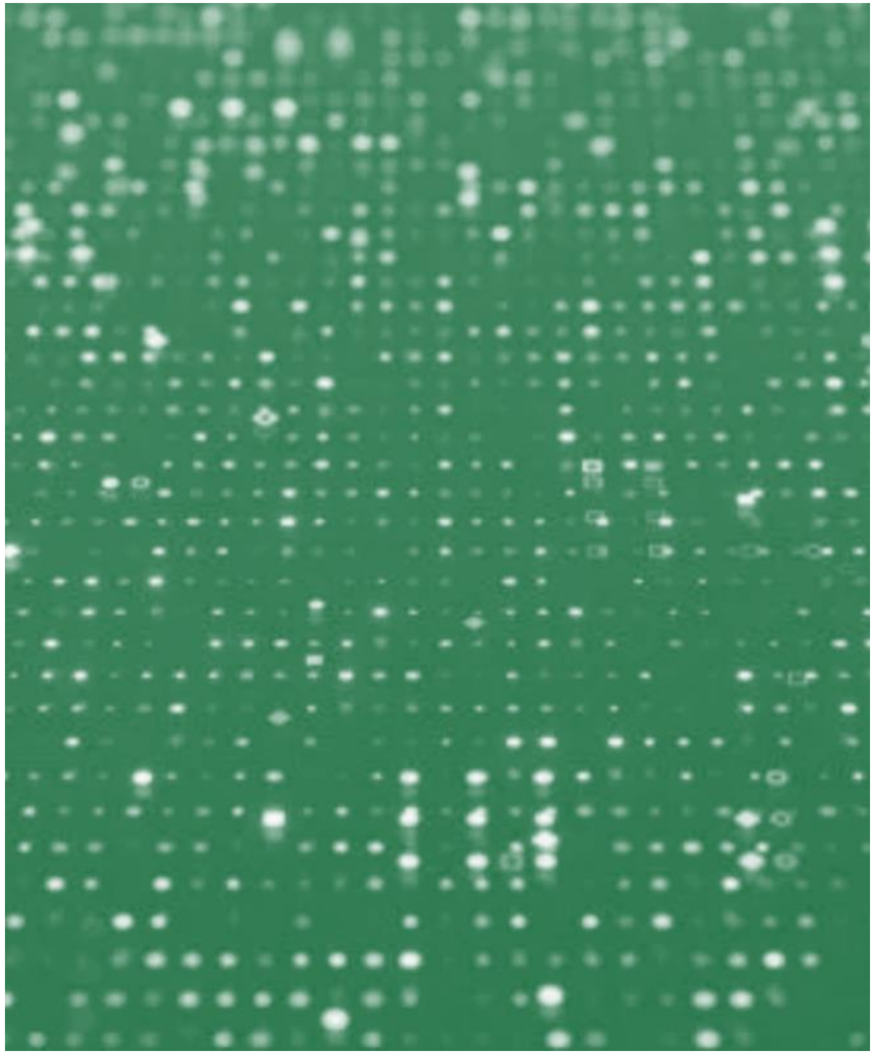
Evolving innovations in the field of artificial intelligence (AI) reshape industries and redefining societal standards. AI enhances decision-making and automates intricate processes, Yet, these advancements come with increased cybersecurity risks, signalling the need for a shift in technology development strategies.

The traditional “security by design” approach, which embeds security features at the technology’s inception, is no longer sufficient given today’s complex and evolving threat landscape. Instead, a “resilience-by-design” mindset for high-risk AI systems is essential, focusing not only on protection but on ensuring systems can endure and recover from inevitable cyberattacks as technology advances. Key findings include:

**AI-specific threats**: AI systems introduce new vulnerabilities such as data poisoning, model manipulation and adversarial attacks. The dual nature of AI as both a cybersecurity tool and potential weapon requires advanced defence strategies and continuous innovation.

**Regulatory challenges**: The speed of technological advances often outpaces existing regulatory frameworks, such as the EU AI Act, creating governance gaps. There is a need for flexible, adaptive regulations that balance innovation and security.

**Skills gap**: A significant shortage of cybersecurity professionals with expertise in AI presents challenges for organizations attempting to secure new systems and respond to evolving threats.



# AI-driven technologies introduce complexities to enterprises’ cyber-resilience frameworks

## New AI innovations are supported by a menacing threat landscape that requires support for a wide-ranging, innovative cyber-resilience ecosystem

AI is rapidly expanding the digital attack surface, introducing new vulnerabilities that traditional security measures struggle to manage effectively. Integrating AI into critical infrastructure offers transformative capabilities but also presents significant risks, such as data poisoning, adversarial attacks, and deepfakes, which can cause AI systems to operate unpredictably or maliciously. This increased reliance on AI within interconnected systems creates a complex threat landscape. A security breach in one AI system can lead to cascading effects, impacting multiple connected networks and potentially disrupting essential services on a large scale. This interconnectedness enhances operational capabilities but requires an adaptable and robust cybersecurity approach—one that not only defends against threats but also includes strong recovery mechanisms to ensure continuity and maintain trust in digital systems.

Rapid advancements in AI often outpace regulatory and cybersecurity developments, leaving governance gaps that hinder consistent security practices. Compounding these issues is the shortage of cybersecurity professionals skilled in AI-specific threats, highlighting an urgent need for targeted training to build a resilient workforce capable of managing next-generation cyberthreats. The shift from “security by design” to “resilience by design” is essential, embedding resilience throughout AI development and deployment. This approach acknowledges that preventing all cyberattacks is unrealistic; instead, systems should be designed to absorb attacks, maintain critical functions, and recover swiftly with minimal disruption. AI-driven predictive analytics, for example, can help organizations pre-emptively identify and respond to potential vulnerabilities, enhancing system resilience.

### ‘Resilience-by-Design’

Organizations must prioritize cyber resilience, embedding adaptability into AI systems to respond effectively to new threats. This approach involves continuous monitoring, rapid response, and learning from incidents to strengthen defences.

### ‘Collaborative Security’

To tackle AI’s complex risks, collaboration among governments, industries, academia, and civil society is essential. Developing adaptable frameworks and fostering international cooperation ensures a coordinated response to global cyberthreats.

### ‘Balanced Innovation’

Balancing AI’s benefits with security safeguards allows innovation to thrive without compromising societal values. By investing in both AI advancements and human capabilities, organizations can create robust, flexible systems prepared for future challenges.

This paper examines the risks and opportunities associated with AI, offering data-driven insights and recommendations to strengthen cyber resilience. By understanding AI's evolving landscape and the security challenges it introduces, organizations can better navigate the digital era, advancing innovation and security together. This approach not only safeguards current systems but also ensures a secure, resilient, and prosperous future as AI technology continues to grow.

# Understanding cyber concerns involves a range of diverse, interconnected risk factors

## Cybersecurity threats specific to AI include vulnerabilities in data privacy, manipulation, and risks from compromised supply chains.

Addressing cybersecurity concerns in AI requires tackling a range of complex, interconnected risks. Rapid AI advancements bring opportunities to strengthen cyber resilience but also introduce challenges that could heighten vulnerabilities. Understanding these dynamics is critical for developing strategies to protect against emerging AI threats while harnessing its potential.

1

### Technological Arms Race

AI is accelerating a technological arms race in cybersecurity, with defenders and attackers constantly innovating to outmanoeuvre each other. As defenders create new AI-powered security tools, attackers adapt, advancing techniques to bypass these measures. This cyclical escalation is a driving factor in cybersecurity growth as organizations seek advanced solutions to counter evolving AI-driven threats.

2

### Ethical and Legal Challenges

AI poses significant ethical and legal challenges, especially around data privacy, accountability, and transparency. Current legal frameworks often lag behind AI advancements, resulting in fragmented regulations. A globally harmonized set of laws and ethical standards is essential to guide AI's responsible use, balancing innovation with societal safeguards.

3

### Privacy Concerns

AI, particularly as it integrates into daily life, intensifies privacy concerns. The vast data AI collects can yield deep insights but also risks misuse if not managed securely. Balancing data use with individual privacy is essential to maintain public trust, especially as AI's role in sectors like critical infrastructure grows.

4

### Skills Gap and Educational Needs

AI's rapid evolution has created a significant skills gap in the cybersecurity workforce. Specialized AI knowledge is scarce, posing challenges for organizations that need to secure AI-driven systems. Addressing this gap will require significant investment in AI-specific education and training programs.

5

### Regulatory Challenges

AI's fast-paced development outpaces many regulatory frameworks. Policymakers must balance the need for innovation with robust protections against evolving AI threats. Flexible, adaptive regulation is necessary to keep pace with AI advancements, ensuring cybersecurity without stifling progress.

6

### Interdisciplinary Collaboration

Addressing AI-related cybersecurity challenges requires collaboration across disciplines. Technologists, policymakers, and ethicists must jointly develop AI cybersecurity strategies that consider technical, social, and ethical implications.

7

### Trust and Confidence in the Digital System

As AI becomes integral to infrastructure and daily life, maintaining public trust is vital. Misuse of AI, data breaches, and operational failures can erode confidence. Building trust demands transparency, robust security measures, and clear communication about AI's risks and benefits.

8

### Increased Attack Surface

AI systems, by their nature, increase the potential attack surface. The proliferation of connected AI systems represents numerous potential entry points for cyberattacks, necessitating robust security measures and comprehensive monitoring to mitigate risks effectively.

# Meaningful calculation involves several key considerations

## Calculating AI's impact matters in today's fast moving technological landscape

Effective measurement of AI's impact involves several key considerations:

### Developing Comprehensive Metrics

Balanced metrics are needed to measure AI's impact accurately. These should include quantitative measures like economic impact and incident numbers, as well as qualitative metrics assessing societal, ethical, and regulatory impacts, such as how AI affects employment, privacy, and decision-making autonomy.

### Holistic Risk Assessment

Evaluating AI demands a holistic risk assessment that considers factors like the expanded attack surface, complexity of threat analysis, and potential skills gaps. Establishing a structured approach to risk identification, assessment, and mitigation is vital for resilience.

### Standardised Measurement Approaches

Industry-wide standards for assessing AI readiness, security, and performance are necessary for consistent, comparable impact analysis across sectors.

### Contextual Analysis

AI's impact varies depending on the context in which it is deployed. Measurement should consider factors like organizational roles, critical business processes, and broader regional contexts to provide an accurate assessment.

### Interdisciplinary Approach

Quantifying AI's impact requires input from technology experts, economists, social scientists, and ethicists. This interdisciplinary approach ensures a well-rounded assessment that includes broader societal, economic, and ethical implications.

### Continuous Monitoring and Adaptation

Given AI's rapid evolution, impact measurement should be continuous. Regularly updating metrics and analysis methods ensures that approaches remain relevant and effective.

### Developing Comprehensive Metrics

Making data and analysis results accessible promotes transparency and fosters further research, enhancing understanding of AI's impact and aiding the development of inclusive policies.

# Focus enables development of a robust approach that facilitates informed decision making

## Addressing cyber risks means adopting comprehensive solutions and mitigation strategies

**Building a resilient digital environment**

Creating a secure environment requires security by design and default, layered security approaches, and incentive frameworks for distributing security responsibilities. This ensures security integration at every stage of AI development and deployment.

**Promoting cyber equity**

Bridging the cybersecurity skills gap is essential. Increasing access to cybersecurity resources and training programs, specifically tailored for AI security, can empower individuals and organizations to manage AI-driven threats more effectively.

**Enhancing data exchange and collaboration**

Breaking down information barriers and promoting data exchange within and across countries is critical. Harmonizing standards and reporting frameworks facilitates collaboration and enables coordinated responses to global AI-related cyberthreats.

## Maintaining robust cyber resilience in the face of emerging AI threats drives enterprises' prioritisation

**Investment in research & development**

Continued investment in R&D is essential for developing innovative AI security solutions, advancing AI-driven cybersecurity tools, and building secure frameworks for data and model protection.

**Collaboration and capacity building**

Strengthening partnerships among government, industry, and academia is crucial for addressing AI-related cybersecurity challenges. Capacity-building initiatives can enhance AI-focused cyber skills and expertise.

**Regulatory reform and standardisation**

Developing frameworks that promote security by design and support international cooperation is essential for a resilient AI ecosystem. Standardizing AI cybersecurity practices streamlines compliance and improves interoperability across sectors.

**Cyber-resilience planning**

Developing and testing incident response plans that account for AI-related threats ensures rapid recovery. Regular updates to these plans are essential to reflect the evolving AI threat landscape.

# Practical suggestions for creating a resilient, long-term AI-enabled cyber ecosystem

## A pre-emptive, cooperation-based approach drives cyber resilience in the AI age

As society progresses deeper into the digital era, AI is rapidly transforming industries and reshaping societal norms. The immense potential of AI offers significant opportunities for economic growth, enhanced operational efficiency, and societal advancements. However, the swift development and integration of AI technologies bring increased cybersecurity risks, highlighting the need to shift from traditional "security by design" to a more robust "resilience by design" approach. This new strategy acknowledges that it is unrealistic to prevent all cyberthreats in our interconnected world. Instead, the focus must shift to creating systems and infrastructures that can endure attacks, maintain essential functions, and recover swiftly from disruptions.

To foster a secure and resilient digital environment that fully capitalizes on AI while managing risks, leaders in government, industry, and academia should consider the following practical recommendations:

| | |
|---|---|
| Invest in AI Research | Continuously fund research in AI to develop stronger systems that can detect and respond to cyber threats effectively. |
| Foster Global Partnerships | Collaborate internationally to share knowledge and create shared cybersecurity standards, ensuring secure integration of AI worldwide. |
| Create Data-Driven Governance | Develop clear metrics and standards for assessing AI technologies to manage risks and ensure safety across industries. |
| Build a Skilled Workforce | Establish training programs to develop skills in AI security, ensuring a knowledgeable workforce to tackle emerging challenges. |
| Establish Ethical Guidelines | Create clear ethical rules for AI development to protect human rights and build trust in digital systems. |
| Design for Resilience | Build security into every step of AI development so systems can withstand and recover from cyber threats. |
| Establish Monitoring Systems | Set up continuous monitoring and incident response plans to detect and address cyber threats quickly. |
| Promote Transparency | Communicate openly about cybersecurity practices and risks to build trust and encourage responsible AI adoption. |

Creating a resilient and sustainable digital environment amidst the evolving landscape of AI requires a multifaceted approach that integrates security, resilience, sustainability, and quantifiable risk measurements into all aspects of technology development and deployment. By embracing these recommendations, leaders can enhance cyber resilience, encourage responsible innovation, and secure a digital future. This strategy underscores the significance of international collaboration, ethical governance, data-driven frameworks, and continuous improvement as essential elements for navigating the complexities of the digital realm. Prioritizing resilience by design, investing in workforce development, and supporting local innovation ecosystems are key to ensuring that AI technologies contribute positively to global cybersecurity efforts while minimizing the associated risks.

# Thank you!

AI & Partners

Amsterdam – London - Singapore

## Email

contact@ai-and-partners.com

## Phone

+44(0)7535 994 132

## Website

https://www.ai-and-partners.com/

## Social Media

LinkedIn: https://www.linkedin.com/company/ai-&-partners/
Twitter: https://twitter.com/AI_and_Partners

## Disclaimer

This Presentation may contain information, text, data, graphics, photographs, videos, sound recordings, illustrations, artwork, names, logos, trade marks, service marks, and information about us, our lines of services, and general information may be provided in the form of documents, podcasts or via an RSS feed (“the Information”).

Except where it is otherwise expressly stated, the Information is not intended to, nor does it, constitute legal, accounting, business, financial, tax or other professional advice or services. The Information is provided on an information basis only and should not be relied upon. If you need advice or services on a specific matter, please contact us using the contact details for the relevant consultant or fee earner found on the Presentation.

The Presentation and Information is provided “AS IS” and on an “AS AVAILABLE” basis and we do not guarantee the accuracy, timeliness, completeness, performance or fitness for a particular purpose of the Presentation or any of the Information. We have tried to ensure that all Information provided on the Presentation is correct at the time of publication. No responsibility is accepted by or on behalf of us for any errors, omissions, or inaccurate information on the Presentation. Further, we do not warrant that the Presentation or any of the Information will be uninterrupted or error-free or that any defects will be corrected.

Although we attempt to ensure that the Information contained in this Presentation is accurate and up-to-date, we accept no liability for the results of any action taken on the basis of the Information it contains and all implied warranties, including, but not limited to, the implied warranties of satisfactory quality, fitness for a particular purpose, non-infringement, compatibility, security, and accuracy are excluded from these Terms to the extent that they may be excluded as a matter of law.

In no event will we be liable for any loss, including, without limitation, indirect or consequential loss, or any damages arising from loss of use, data or profits, whether in contract, tort or otherwise, arising out of, or in connection with the use of this Presentation or any of the Information.