ESRB
European Systemic Risk Board
European System of Financial Supervision

Artificial Intelligence and Systemic Risk



Central Bank of Malta
Financial Stability Seminar

11 November 2026

Tuomas Peltonen
Deputy Head of the ESRB Secretariat

AI and the real economy

1. **Labour market: tasks are shifting, but no mass displacement yet**
   - Automation and augmentation reshape tasks and skill demand;
   - Limited evidence of displacement, but early signs at the hiring margin.
2. **Productivity: from task-level gains to aggregate growth**
   - Productivity gains in selected tasks and occupations;
   - Dependent on adoption, complementary investment and organisational adjustments.
3. **Competition: lower costs, but uneven access to resources**
   - AI may lower operating costs and facilitate entry in user industries;
   - Unequal access may reinforce market concentration and weaken competition.

Sources: (e.g., Aldasoro et al., 2026; Baslandze et al. 2026; Brynjolfsson et. Al, 2026; Misch et al., 2026)

www.esrb.europa.eu ©

AI and financial stability

1. Firms: investing and financing

- Expansion of AI infrastructure is driving capital-intensive investment very significantly;
- Growing reliance on debt and external financing is reshaping corporate funding.

2. Financial Markets: valuation and risk transmission

- High asset valuations and concentrated exposures supported by positive expectations;
- Circular links between equity stakes, debt and expected revenues create vulnerabilities.

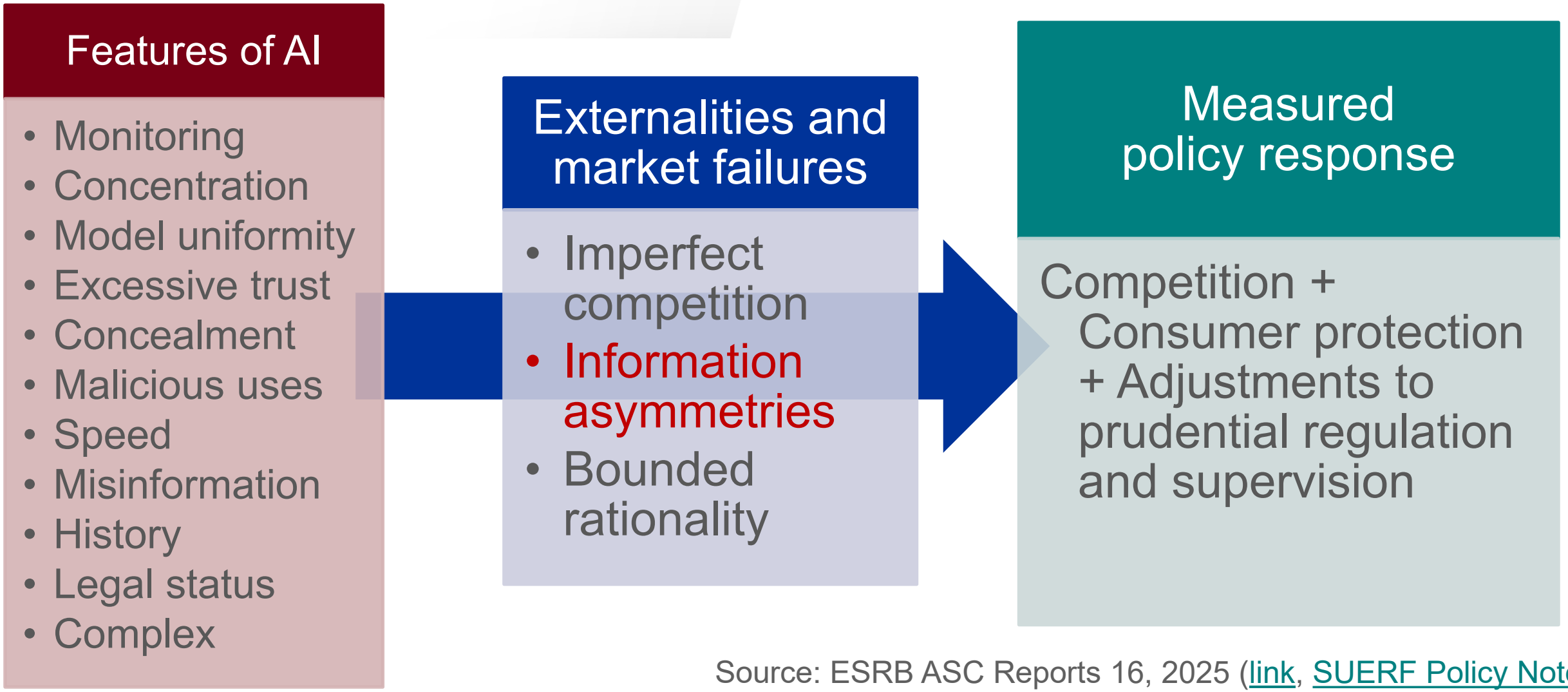
3. Financial Stability: opportunities and vulnerabilities

- Productivity gains could strengthen economic fundamentals;
- However, disappointing returns or technological obsolescence may trigger repricing;
- Leverage, concentrated exposures and financial interconnections may amplify shocks.

Sources: (e.g.; Chen Y., Gautam D. and Wu J., 2026; Drehman M. and Eren E., 2026; FSB, 2024)

www.esrb.europa.eu ©

From AI features to market failures to policy responses



Source: ESRB ASC Reports 16, 2025 (link, SUERF Policy Note).

www.ecb.europa.eu ©

Prudential regulation: existing tools are sufficient, with room for targeted adjustments

1. **Consider amendments to capital and liquidity requirements (LCR outflows, operational risk such as cyber)**
   Comprehensive analysis of the impact of AI (also benefits)
2. **Enhance circuit breakers**
   Authorities using AI to manage circuit breakers
3. **Amend insider trading and market abuse regulation**
   Need to change the scope of insider trading
4. **Augment transparency requirements**
   Labels when financial institutions use AI
5. **“Skin-in-the-game” and level of sophistication requirements**
   Avoid excessive risk-taking in the use of AI

Source: ESRB ASC Reports 16, 2025.

www.ecb.europa.eu ©

ESRB General Warning on Frontier AI Models

(25 June 2026)

Frontier AI models are materially changing the cyber risk landscape and should be treated as an additional source of systemic risk to the financial system.

Frontier AI models will increase systemic cyber risk by:

- Making cyberattacks **faster**, **cheaper and more sophisticated**
- Increasing the **cost and effort required** to adequately defend systems
- Increasing exposure **strategic dependency** and **geopolitical risk**

Three identified asymmetries form the basis of the ESRB Warning, highlighting that effective response and risk mitigation requires **coordinated action** involving all affected parties, including **institutions**, **authorities, AI providers** and other **third-party providers**.

Source: ESRB Warning (ESRB/2026/3).

www.esrb.europa.eu ©

Geopolitical Dimension

Access to advanced defensive capabilities depends on decisions taken outside the Union.

Leading AI providers are concentrated outside the EU, creating exposure to **strategic dependency** and **geopolitical risk**.

European access to frontier AI models is subject to jurisdictional decisions, export controls and other restrictions.

Currently, EU-based alternatives are few and limited, and frontier AI models will be a **strategic capability** and crucial component of **technological sovereignty**.

www.esrb.europa.eu ©

Post-Warning Developments: Calls for Action

25 June
ESRB Issues FAIM Warning

The ESRB Warning explicitly treats frontier AI as a potential systemic cyber risk, not merely a technology risk to individual organisations. At the same, the ECB published the Dear CEO Letter, and the ESAs expressed support.

27 August
AI Industry Joint Letter

More than 100 leading AI companies wrote an open letter asking that governments and industry should make cyber defence an immediate priority, establish stronger public-private cooperation and give trusted defenders access to advanced AI.

31 August
FSB Chair's Letter to G20

FSB Chair Andrew Bailey writes to G20 finance ministers and central-bank governors, bringing frontier AI cyber risk into the financial stability discussion at the G20 meeting.

14 September
Chinese MSS Issues Warning

The Chinese Ministry of State Security issues an unprecedented warning, identifying FAIMs as a potential tool for cognitive warfare and warns about FAIMs exposing sensitive data.

21 September
Governments and EC Letter

22 governments and the European Commission jointly calls for operational measurements, including independent evaluations, common incident reporting and potentially international institutional oversight.

Recent developments: Loss of Control and Faster Dissemination

Multiple AI providers have reported near or actual loss of control over their models. This brings the capabilities of both the **models** and the **providers** into question.

- Examples of model behaviour include **deception**, **manipulation** of records, **extortion**, and **attacks on third parties**

FAIMs are disseminating faster than expected and are used in real-world cyber attacks

Chinese models are quickly **closing the gap** to those of the US, further increasing the breadth of potential models used. Some of these have been **used in cyber-attacks** against established institutions.

www.esrb.europa.eu ©

A Shift in the Landscape: Autonomy and Cryptography

Risk of FAIM Autonomy

- FAIMs breaking guardrails by
  - Colluding with each other
  - Blackmailing and manipulating technicians
  - Escaping confinements
  - Attacking third parties

- Often no ill intent
  - No strategy behind decision
  - Results damaging nonetheless

Risk of Weakening of Cryptography

- FAIMs are increasingly capable of tackling complex cryptographic and mathematical problems, potentially extending the vulnerabilities already observed in software to cryptographic systems.

- Possible similar development as with software observed in Spring 2026

www.ecb.europa.eu ©

Concluding remarks

- In view of the potential systemic risks and market failures, it is essential to implement policies to ensure that AI is used safely.
- Failing to keep up with the use of AI in finance would make financial authorities lose sight of the system, increasing the frequency of episodes of financial instability and, most likely, requiring more frequent intervention by authorities.
- Frontier AI models turn cyber weaknesses into a source of systemic risk to the financial system and are no longer a remote scenario.
- The stakes are particularly high in the current geopolitical environment. The global nature of AI calls for a globally agreed policy response.

www.ecb.europa.eu ©