Blog

Working together against new AI-enhanced cyber threats

Financial stability, Digitalisation | 08 July 2026 | Olli Rehn

AUTHOR



Olli Rehn
Governor

The frontier artificial intelligence models are changing the nature of cyber threats. At the same time, they are also changing our understanding of where serious disruptions and systemic risks in the financial system may originate.

On 7 July 2026, the European Systemic Risk Board (ESRB) issued a warning about systemic cyber risks stemming from frontier AI models. The warning message is clear: cyber threats enhanced by AI are no longer just a security issue. They can pose a significant risk to the stability of the entire financial system.

This is a new phase in financial stability thinking. Traditionally, attention has focused on the capital adequacy of banks, indebtedness and the functioning of financial markets. These remain the bedrock of financial stability. But the world around banks has changed.

The financial system increasingly relies on digital services, cloud services, software, data and AI. Payments, securities trading, lending and many other services rely on shared digital systems. When everything functions well, this dependency is barely noticeable. When a critical system is disrupted, the effects may quickly spread throughout the economy.

This is precisely the essence of modern-day systemic risk. A crisis no longer necessarily starts with a bank's balance sheet. It may start with a software bug, a cyberattack, a cloud service outage or a vulnerability discovered by an AI model. If many financial institutions use the same technology platforms or the same AI models, a local problem may quickly escalate into a system-wide disruption.

The financial system is a global network. Money, information and risks move quickly across

borders. AI, digital infrastructure or cybersecurity incidents are therefore not just a problem for one country. They are not just a European or an American issue. They are a global issue.

This also leads to a clear conclusion. New systemic risks cannot be managed solely at a national level. This requires international cooperation, common ground rules and continuous exchange of information between authorities and the financial sector.

This is precisely the kind of European cooperation we are seeing now. The ESRB is examining the issue from the perspective of the stability of the entire financial system. At the same time, ECB Banking Supervision (SSM) has asked large banks to prepare action plans by autumn on how they will strengthen their own systems and manage AI-related risks. The European Commission has also launched measures to strengthen the security assessment of frontier AI models and Europe's preparedness to respond to new cyber threats. When the ESRB assesses systemic risk, Banking Supervision strengthens the operational capacity of banks, and the Commission develops a common regulatory and operational framework, the whole is greater than the sum of its parts.

AI, naturally, can also strengthen defence, helping to detect anomalies, identify attacks and uncover vulnerabilities more efficiently. But the same technology also provides attackers with new tools. Frontier AI models can find software weaknesses, build effective attack methods and significantly shorten the time between finding and exploiting a vulnerability.

Defensive capabilities, moreover, are not the same everywhere. The leading AI developers are largely located outside Europe. Not all European actors have equally rapid access to the latest tools. At the same time, banks and other financial sector entities must follow strict testing, change management and monitoring procedures. Attackers have no such restrictions.

This does not mean, however, that the old lessons have lost their relevance. On the contrary.

Former Goldman Sachs CEO Lloyd Blankfein stated after the financial crisis that too many financial institutions had, effectively, outsourced their own risk management. His message is still relevant today. External expertise and AI can be used in risk analysis, but responsibility cannot be outsourced. Every bank, technology company and authority must understand what its operations are based on and what consequences system disruptions may have.

The critical observation of contrarian economist Hyman Minsky still holds true. Long periods of stability can create an excessive sense of security. As belief in the functionality of systems increases, caution easily decreases. In the age of AI, this lesson becomes increasingly important. The more society is built on shared digital systems, the more essential it is to identify their common vulnerabilities.

The ESRB has paid special attention to frontier AI models. If a large part of the financial system relies on the same foundation models, the same cloud services and the same technology suppliers, vulnerabilities may also be shared. In that case, a single cyber attack could, at worst, spread via payment, settlement or securities systems to the entire financial system.

From a financial stability perspective, the conclusion is clear. Innovation is needed, and Europe cannot remain a bystander in technological development. But it is equally important to ensure that our ability to manage new risks grows at the same rate as our ability to adopt new technology.

Ultimately, it's a question of trust. The financial system only works as long as people can trust that payments will be made, savings will be safe and markets will remain functional even in times of disruption. Trust is easy to lose, but difficult to rebuild.

Effective international and European cooperation is therefore needed, above all to combat the new cyber threats posed by AI. Systemic risk is increasingly rarely the risk of one bank, one market or one country. It is the risk of networks. That is precisely why managing such risk is also a shared responsibility.

The author is the Governor of the Bank of Finland and First Vice-Chair of the European Systemic Risk Board (ESRB).

Keywords

artifical intelligence, cyber risks