SPEECH

Macroprudential policy in Europe – the future depends on what we do today

Welcome remarks by Christine Lagarde, President of the ECB and Chair of the European Systemic Risk Board, at the fifth annual conference of the ESRB

Frankfurt am Main, 8 December 2021

It is my pleasure to welcome you to the fifth annual conference of the European Systemic Risk Board (ESRB).

Today's conference marks the first decade of the ESRB – although the pandemic has delayed our celebration by one year.

That decade has been one of important achievements. Most notably, macroprudential policy for banks has developed from an idea into a reality. But this morning I would like to look forward and ask: how can we prepare for the next decade?

There are known threats to financial stability which have always been on the ESRB's radar, such as unbridled risk-taking, stretched asset valuations and excessive credit growth. But today we are also facing new types of threats which could affect financial stability profoundly.

Two such threats stand out: climate change and cyber incidents. And both have common patterns. Both are global phenomena that do not stop at borders. Both are cross-sectoral, potentially affecting banks, insurers, investment funds and the markets that connect them. And both are complex, depending on many factors and actors.

Tackling these threats is challenging, but as Steve Jobs said, "if you define the problem correctly, you almost have the solution". So, in my remarks today I would like to explore the nature of these threats, the type of responses we need to address them, and where the ESRB can add value in the decade to come.

Threats from climate change

Climate change has become the defining challenge for our generation. Rising to this challenge requires a collective effort in which the financial sector has a key role to play. We need the sector to channel resources to finance the transition to a more sustainable economy.

However, to be able to play this role, the financial system needs to be resilient. And climate change itself poses a threat to that resilience in two main ways.[1]

The first is through physical risks. Environmental disasters like floods, droughts and heat stress can lead to direct and indirect losses for financial institutions – and the intensity and likelihood of those disasters is clearly linked to climate change.[2] The flooding catastrophe this summer is estimated to have caused financial damages exceeding €29 billion in Germany alone.[3]

The second threat to resilience is through transition risk. A disorderly transition to a greener economy could also create losses for the financial sector, insofar as the business models of polluting industries become unviable and their assets end up being stranded. If assets lose value ahead of their expected economic lifespan and reprice abruptly, it could lead to systemic tremors.

Such tipping points in financial markets are far from unrealistic. ESRB analysis finds that financial markets are not yet meaningfully differentiating their pricing on the basis of climate risks.[4] Since physical and transition risks are clustered in individual banks, the effects of reaching a tipping point

would be concentrated and might have stronger effects than would otherwise be the case. That could in turn spill over to the financial system more broadly.

For example, 70% of banking system credit exposures to firms subject to high or increasing physical risks are concentrated in the portfolios of only 25 euro area banks. For seven of these banks, these exposures account for more than 10% of their total assets.

However, the financial stability impact of climate change is highly path-dependent: it depends on whether we avoid the most extreme climate scenarios, and whether we are able to carry out an orderly transition. Which path we follow is, for now, still in our own hands.

If we are to contain the most harmful effects, the first line of defence requires governments to rescale their climate policies to the magnitude of the challenge. Effective climate policies would also benefit the financial sector.

But macroprudential policymakers have a part to play, too, in identifying and mitigating the financial aspects of climate-related risks. We should not fall into the false logic of trade-offs, believing that policies which make the financial system more resilient will hold it back from funding the transformation of our economies. Stronger banks are banks that lend more.[5]

Threats from cyber incidents

Let me now move to the second threat: cyber incidents.

The financial sector relies on robust information and communications technology. People's confidence in the sector in turn depends on the confidentiality, integrity and availability of the data and systems it uses. Cyber incidents, however, can corrupt information and destroy confidence. They therefore pose a systemic risk.

To date, we have not seen a systemic cyber incident affecting the financial system. But the cyberattacks on hospitals in Europe during the COVID-19 crisis[6] and the attack on the Colonial Pipeline in the United States[7] have given us a taste of what could happen in the future. Such an attack is probably now a question of when, not if. There are three reasons why.

First, digitalisation means that individual firms have become more exposed to cyberattacks – and COVID-19 has only accelerated this trend. Financial institutions have had to adapt their technological infrastructure to a sudden increase in remote working and remote customer relationships, which increases efficiency but also vulnerability.

Second, the interconnectedness of information systems enables cyber incidents to spread quickly. There are approximately 22,000 financial entities in the EU[8], and digitalisation has deepened the linkages between them and with third-party infrastructure and service providers. As a result, a cyber incident can quickly grow from an operational disruption into a systemic event.[9]

Third, cyber incidents are becoming more frequent and sophisticated. For example, between 2019 and 2020 the number of cyber incidents reported to the ECB increased by 54%, and many of them were malicious.[10] The SolarWinds incident, which affected Microsoft email servers globally, highlights the sophistication with which attackers can now exploit operational vulnerabilities.[11]

Collectively, we need to be prepared to manage the financial stability consequences of a major cyber incident. If such an event happens, a coordinated and swift response will be essential to preserve confidence and re-establish reliable information. This might require new forms and mechanisms of cooperation and communication. Financial authorities have to adapt to this new environment, as the cyber threat landscape is also evolving continuously.

The role of the ESRB

So where can the ESRB add value?

When threats are global, cross-sectoral and complex, no institution can understand and tackle them alone. We need to see the whole picture, connecting data and diverse perspectives.

This is where the ESRB comes in. It comprises around 80 member institutions, including the ECB and all national central banks in the EU. It includes banking, insurance and market supervisors, as well as the three European Supervisory Authorities and the European Commission. And it benefits from the expertise of academia through its Advisory Scientific Committee.

This diversity of perspectives helps find solutions to complex problems – and this is already happening for both climate change and cyber threats.

Five years ago, the ESRB's Advisory Scientific Committee provided a conceptual framework for addressing systemic risks related to climate change. This called for enhanced information collection and disclosure, as well as climate stress tests.[12] Since then, the ESRB has worked to develop the analytical toolkit needed for evidence-based policymaking.

With this toolkit, the ESRB can map how climate risk impacts millions of firms and what this means for the exposures of our most important financial institutions. It can also assess the system-wide impacts from different paths that climate change or the transition might take.[13] Based on this evidence, we now need to work on policy options.

For cyber incidents, the ESRB will soon present steps for a framework to ensure a coordinated and rapid response from public financial authorities. Such a framework is already foreseen in the European Commission's proposal on digital operational resilience for the financial sector.[14] The ESRB wants to ensure that it is fully operational and ready to be used in the near future.

In particular, the ESRB is seeking to create communication channels and a classification of cyber incidents to ensure situational awareness and a swift response by authorities. This includes coordination on impact assessments and the exchange of information on planning and execution.

We know that threats from climate change and cyber incidents will materialise. This means that we need to prepare now. As Mahatma Gandhi said: "The future depends on what you do today."

In this spirit, I now open the fifth ESRB conference.

1. ESRB (2021), "Climate-related risk and financial stability" and ESRB (2020), "Positively green: Measuring climate change risks to financial stability", reports of the Advisory Technical Committee.

2. World Weather Attribution (2021), Rapid attribution of heavy rainfall events leading to the severe flooding in Western Europe during July 2021.

3. See, for example, Tageschau, 7 November 2021.

4. ESRB (2021), op. cit.

5. Gambacorta, L. and Shin, H.S. (2018), "Why bank capital matters for monetary policy", *Journal of Financial Intermediation*, pp. 17-29.

6. "Patients fall victim to health ransomware", Financial Times, 26 January 2021.

7. "Colonial Pipeline: cyber attack draws attention to besieged US energy system", Financial Times, 11 May 2021.

8. Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector.

9. For more detail on the propagation channels of cyber incidents, see ESRB (2020), "Systemic cyber risk".

10. ECB Banking Supervision (2021), "IT and cyber risk: a constant challenge", *Supervision Newsletter*, 18 August.

11. Cybersecurity & Infrastructure Security Agency (2021), "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations", 15 April.
12. ESRB (2016), "Too late, too sudden: Transition to a low-carbon economy and systemic risk", report of the Advisory Scientific Committee.
13. ESRB (2021), op. cit. and ESRB (2020), op. cit.
14. Article 43 of the Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector.

CONTACT

European Central Bank

Directorate General Communications

- Sonnemannstrasse 20
- 60314 Frankfurt am Main, Germany
- +49 69 1344 7455
- media@ecb.europa.eu

Media contacts