Benoît Cœuré: A Euro Cyber Resilience Board for pan-European Financial Infrastructures

Introductory remarks by Benoît Cœuré, Member of the Executive Board of the ECB, at the first meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures, Frankfurt, 9 March 2018

It is a pleasure to welcome you back to Frankfurt. Our last meeting was in June last year. Today, we will discuss the future course of the high-level cyber resilience forum for pan-European financial market infrastructures, critical service providers and competent authorities.

Establishment of the Euro Cyber Resilience Board for pan-European Financial Infrastructures

Recent technological advances have enabled cybercriminals to conduct ever more sophisticated, precise and powerful attacks. And nobody is immune to cyber risks, including businesses, financial infrastructures and public administrations. So we should avoid a "blame and shame" culture and work together.

The ECB and the Eurosystem are striving to lead by example. At the ECB, overseers, operators, supervisors and IT security services are working together more closely on cyber issues. Within the Eurosystem, there has been close collaboration on implementing the Eurosystem oversight cyber resilience strategy for financial market infrastructures that we presented at our last meeting, in line with CPMI-IOSCO's guidance on this topic.[1] The Market Infrastructure Board, which is in charge of Eurosystem financial market infrastructures, has also scaled up its activities to ensure the continued cyber resilience of its systems and platforms.

Eurosystem initiatives are part of a growing international effort to combat cyber threats. The CPMI-IOSCO guidance is being implemented. In October 2017, the Financial Stability Board (FSB) delivered a stocktake report of relevant regulations and supervisory practices to G20 finance ministers and governors, and G7 ministers and governors published the "Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector".[2] The FSB will produce a common lexicon of important terms, while the G7 Cyber Expert Group continues to work on third-party risks, cross-sector coordination and threat-led penetration testing, and will make proposals for G7 cross-border cyber crisis simulation exercises.

In this context, the Eurosystem aims at coordinating its own activities in

the field of cyber risks with that of market participants and other public authorities to succeed in protecting the financial system from cyber threats. I therefore invite you today to become part of the Euro Cyber Resilience Board (ECRB) for pan-European Financial Infrastructures – a regular forum where we can work together in a trusted environment.

The ECRB's objective is to enhance the cyber resilience of financial market infrastructures and their critical service providers, as well as that of the wider EU financial sector, in line with international standards. This will be achieved by fostering trust and collaboration and facilitating joint initiatives – whether among market players or between market players and authorities. The ECRB will thus contribute to the overall stability of the EU financial system.

The ECRB will have no formal powers to impose binding measures and will not make supervisory judgements. Its legitimacy will stem from the voluntary commitment of its members to abide by its common positions, statements and strategic views.

The ECRB will be chaired by the ECB, which will be closely involved together with national central banks and observers from the relevant European public authorities. This will ensure that the ECRB acts in the interest of Europe as a whole. Its common positions, statements and strategic views will be adopted by consensus.

To kick off the work of the ECRB, we would like to reflect with you on possible work items which we could address collectively. As part of this, we will also report on two of our most recent activities.

First, a cyber resilience survey, developed under the Eurosystem oversight cyber resilience strategy, was conducted across more than 75 payment systems, central securities depositories and central counterparties throughout Europe. As you will see, the survey highlighted a number of very pertinent issues for discussion, such as cyber governance, training and awareness, and cyber incident response.

Second, the Eurosystem is currently finalising the main elements of the European Threat Intelligence-Based Ethical Red-Teaming (TIBER-EU) Framework. This is an interesting concept which we hope will raise the level of cyber resilience in Europe and enable cross-border, cross-authority testing, which has not been done before.

We look forward to hearing your feedback on these two initiatives. We will also update you on the forthcoming market-wide exercise, which will explore the challenges of a specific cyber scenario and see how we can work closer together in times of crisis.

I am confident that we will have a fruitful discussion. I will now hand over to my colleague Sabine Lautenschläger, who will make some introductory remarks from the supervisory perspective.

After that, I would like to invite the European Commission representative to

briefly introduce the very recently published “FinTech Action plan”, which presents some interesting points to be considered with regard to the cyber resilience of the financial sector.

Thank you.