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

Introductory remarks by Mr Benoît Cœuré, Member of the Executive Board of the European Central Bank, at the second meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures, Frankfurt am Main, 7 December 2018.

* * *

It is a pleasure to welcome you back to Frankfurt. Since our last meeting in March, we have been very busy at the ECB and across the Eurosystem, and we have made considerable progress in our work to enhance the cyber resilience of the financial sector.

The cyber threat facing the financial sector continues to be a challenge. From banking trojans affecting individual customers to systemic threats posed by ransomware and targeted attacks from advanced persistent threat (APT) groups, the landscape is evolving on a daily basis.

At our previous meetings, we shared with you the Eurosystem cyber strategy for financial market infrastructures (FMIs)[1]. This strategy rests on three pillars: individual FMI resilience, sector resilience and strategic regulator-industry collaboration. I am pleased that in the last few months, the ECB and the Eurosystem have made significant progress in putting in place the building blocks for enhancing the cyber resilience of the European financial ecosystem and operationalising the strategy.

We have developed two key tools to improve FMI resilience: the cyber resilience oversight expectations (CROE)[2] and the TIBER-EU Framework[3].

The CROE serves three key purposes: (i) it provides FMIs with detailed steps on how to operationalise the CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures[4], ensuring they are able to make improvements and enhance their cyber resilience over a sustained period of time; (ii) it provides overseers with clear expectations against which to assess FMIs under their responsibility; and (iii) it provides the basis for a meaningful discussion between the FMIs and their respective overseers. The public consultation on the CROE provided some very useful feedback, which we carefully considered, and the final version was published earlier this week. The central banks of the Eurosystem will work closely with the various financial infrastructures to enhance their cyber resilience, with the CROE serving as a good basis for this work.

Enhancing cyber resilience is of crucial importance. Equally important, however, is to test whether the enhancements that have been introduced by individual entities are effective. To that end, we published the TIBER-EU Framework in May and the TIBER-EU Services Procurement Guidelines[5] in August. In due course, we will also be publishing the TIBER-EU White Team Guidance, to further complement the testing framework. The feedback on the testing framework has been very positive, and we are in close dialogue with a number of authorities across the EU that are in the process of adopting it. Our hope is that over time, this sophisticated level of testing will help strengthen our financial infrastructures and raise standards among threat intelligence and red team testing providers.

In terms of sector resilience, we believe that exercises are a key component of building market-wide preparedness for a cyber incident. In March, we told you about our forthcoming market-wide exercise, which we held in June. The exercise, UNITAS, took the form of a facilitated discussion among market participants – many of whom are here today – on a cyber scenario. The scenario involved a cyberattack on a number of financial infrastructures, resulting in a loss of data integrity and a knock-on effect on other financial infrastructures. Today we will discuss how we can proceed in 2019 to follow-up on this exercise.

With regard to strategic regulator-industry collaboration, our third pillar, we formally established the Euro Cyber Resilience Board (ECRB) for pan-European Financial Infrastructures in March 2018, as a forum for strategic discussions between financial infrastructures and authorities. As you know, our objectives are to raise awareness of the topic of cyber resilience; to act as a catalyst for joint initiatives to develop effective solutions for the market; and to provide a place to share best practices and foster trust and collaboration. Today we will discuss what concrete steps we can take as members of the ECRB to develop meaningful solutions and foster this trust and collaboration.

Of course, cyber risk is borderless and it is an international issue. So the Eurosystem's initiatives are part of a growing international effort to combat cyber threats. In October this year, G7 ministers and central bank governors published the "Fundamental Elements for Threat-Led Penetration Testing", which complements the TIBER-EU Framework, and the "Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector". In 2019, the G7 Cyber Expert Group will move ahead with conducting the first global cross-border cyber crisis simulation exercise.

In November, the Financial Stability Board (FSB) published a Cyber Lexicon. Having a common set of definitions in non-technical language will support the work of the FSB, standard-setting bodies, authorities and financial institutions to address cyber security and cyber resilience in the financial sector. The ECB continues to participate in these international fora, ensuring that global initiatives are aligned with our work in Europe.

From an operational perspective, the Market Infrastructure Board, which is in charge of the Eurosystem-operated financial infrastructures, continues to scale up its activities to ensure the continued cyber resilience of its systems and platforms.

At our meeting in March[6], we identified four key areas for further focus: 1) crisis management and incident response; 2) information sharing; 3) awareness and training; and 4) third-party risk. There was general agreement that these key areas warranted further thought and focus. The UNITAS exercise further confirmed that these areas require attention. Today we will reflect on how to address them collectively on the basis of proposals made in close cooperation with the experts at your institutions.

Thank you.

---

1 Eurosystem cyber resilience strategy

2 Cyber resilience oversight expectations

3 TIBER-EU Framework

4 CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures

5 TIBER-EU Services Procurement Guidelines

6 ECRB public summary March 2018