Benoît Cœuré: Cyber resilience for pan-European financial market infrastructures

Introductory remarks by Mr Benoît Cœuré, Member of the Executive Board of the European Central Bank, at the High-Level Meeting on Cyber Resilience, Frankfurt am Main, 19 June 2017.

* * *

Introduction

It is a pleasure to welcome you here today to this strategic high-level meeting on cyber resilience for pan-European financial market infrastructures.

The aim of bringing together high-level representatives from large European market infrastructures, critical service providers and public authorities is threefold:

First we would like to gain a deeper understanding of the cyber threat landscape in Europe.

The European Union Agency for Network and Information Security (ENISA) will make a presentation on the cyber threat landscape and its relevance for the financial sector.

Second, we will share with you the Eurosystem's cyber strategy for financial market infrastructures and also explain ECB Banking Supervision's approach to the issue of bank cyber resilience.

Third, we would like to hear your views on how we can all collaborate in a trusted environment to enhance the cyber resilience of financial market infrastructures.

More specifically, we would like to assess with you how much interest there is in creating a high-level cyber resilience forum for pan-European financial market infrastructures, critical service providers and competent authorities.

Before we start, let me briefly set the scene.

The evolving cyber threat landscape in Europe

Besides the undeniable advantages of information and communication technology, the increase in users and data on digital platforms, in cloud computing and across networks has also created greater opportunities for cybercrime.

There are a variety of agents involved: criminals, hacktivists or nation states.

They may have different motives: financial gain, espionage, disruption and destabilisation.

But what they all have in common is that they are steadily increasing their level of sophistication and exploring ways of attacking.

A sound operational risk management and IT security framework are the first line of defence.

But resilience to cyberattacks means more than that. Unlike critical failures, the likelihood of cyberattacks cannot be mitigated. A paradigm shift is necessary. We have to accept that cyberattacks are inevitable and that attackers are persistent. Consequently, we have to establish how – in case of persistent attacks – we prioritise our operations and resources, protect our key assets and restore functionalities. Cyber resilience goes beyond technology, it also encompasses governance, company culture and business processes.

Given the extensive interlinkages and interdependencies in the financial system, it is obvious that

markets' overall cyber resilience depends not only on the resilience of each individual market actor but also on that of interconnected market infrastructures, participants and service providers.

The Eurosystem cyber strategy for financial market infrastructures

Following the increase in both the frequency and severity of cyberattacks over the last few years, legislators, regulators and standard setters have issued legislation and guidance on cyber security at national and international level and at cross-sectoral as well as sector-specific level.

Let me briefly mention three initiatives.

First, in 2016, the EC adopted the **Directive on security of network and information systems** (the NIS Directive).

Its aim is to bring the cybersecurity capabilities of operators of essential services to the same level of development in all the EU Member States and to ensure an efficient exchange of information and good cooperation on the topic throughout the EU.

Second, at international level, the **G7** countries have drawn up a set of **fundamental elements of cybersecurity for the financial sector**, as well as three further recommendations on the effectiveness of cybersecurity assessments, third-party risks, and coordination with other critical sectors.

Third, with a key focus on financial stability, the CPMI-IOSCO published a principles-based **"Guidance on cyber resilience for financial market infrastructures"** in June 2016.

Supplementing the "Principles for Financial Market Infrastructures", it provides additional detail related to the preparations and measures that financial market infrastructures should undertake to enhance their cyber resilience.

In recognition of the escalating cyber threats, the legislative and regulatory guidance and the required paradigm shift, the Eurosystem's overseers have launched a strategy for cyber resilience in relation to financial market infrastructures. This strategy – which will be explained in more detail at agenda item 3 – is built on three pillars.

- **The first pillar** refers to the cyber resilience of individual financial market infrastructures.
- **The second pillar** refers to the resilience of the financial sector as a whole.
- **The third pillar** highlights the importance of establishing a forum which brings together market actors, competent authorities and the cybersecurity service providers.

This brings me to the third and final objective of today's meeting.

Creation of a high-level cyber resilience forum

Tackling cyber risk is not for regulators or market actors in isolation.

Rather it is a collaborative endeavour that must be undertaken together.

Hence, I invite you to seriously consider the creation of a high-level cyber resilience forum for pan-European financial market infrastructures, critical service providers and competent authorities.

I am convinced that there is cross-fertilisation and collective learning to be gained from such collaboration and I am looking forward to a fruitful meeting today.