Sabine Lautenschläger: Euro Cyber Resilience Board for pan-European Financial Infrastructures

Introductory remarks by Sabine Lautenschläger, Member of the Executive Board of the ECB, at the third meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures, Frankfurt am Main, 28 June 2019

It is a pleasure to welcome you back to Frankfurt. As you may know, I recently became responsible for market infrastructures and payments at the ECB. As this includes the ECB's work on the cyber resilience of financial market infrastructures (FMIs), I have taken over Benoît Cœuré's chairmanship of the Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB). I would first like to thank Benoît for his contribution in establishing the ECRB and for this opportunity to continue the excellent work on cyber resilience at European level which he has personally driven forward.

Six months have passed since our last meeting in December, during which time, all of us – whether on behalf of a public or private financial infrastructure, a supervisor or an overseer – have been busy enhancing the cyber resilience of our respective financial infrastructures and of the financial sector as a whole. But cybercriminals have been making progress too, and they remain persistent and relentless in their pursuits. As widely reported in the press, a major cyber incident occurred at a significant bank earlier this year, seriously affecting the real economy in a specific

European country. This publicly known incident reminds us of the debilitating impact a cyberattack can have on our financial system. So the need for continued vigilance, work and collaboration in this field is imperative.

You will recall that – in December 2018 – the ECB published its cyber resilience oversight expectations[1], a tool meant for both FMIs and overseers. These expectations contain detailed best practices for implementing the CPMI-IOSCO Cyber Guidance[2] and are now being followed by FMI operators at national and European level. Overseers are working with their respective FMIs to ensure that they do what is necessary to enhance their cyber resilience. I am also pleased that the World Bank has recently embraced our cyber resilience oversight expectations with a view to boosting the cyber resilience of FMIs in developing and emerging countries under its mandate, and consequently promoting global harmonisation.

Last year, the Eurosystem also developed the European Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU)[3]. Red teaming helps entities assess, by means of controlled "ethical hacking", if and how they are capable of withstanding a cyberattack. And because TIBER-EU involves high-end testing on live production systems, we are currently reflecting on how to foster an accreditation and certification capability in the EU. This would allow cybersecurity service providers to raise standards around threat intelligence and red team testing and to have their capabilities in this field validated.

I am pleased to say that, since its publication, TIBER-EU has been implemented – or is currently being implemented – in Belgium, Denmark, Germany, Ireland, the Netherlands, Romania and Sweden, and by the ECB in its oversight capacity. The ECB is also in close dialogue with other EU and non-EU jurisdictions that are considering TIBER-EU as a tool for their respective financial sectors. The gradual roll-out of TIBER-EU will ensure that threat-led penetration testing is conducted in a harmonised way across the EU, avoiding duplication of work for financial entities and authorities alike.

Already in March 2018, at the first ECRB meeting, we presented the results of a cyber resilience survey that had been developed under the Eurosystem oversight cyber resilience strategy. The survey had been conducted across more than 75 payment systems, central securities depositories and central counterparties throughout Europe. You will recall that the survey highlighted a number of weaknesses prevailing at the time, such as cyber governance, training and awareness, and cyber incident response. Today we will update you on the second round of the cyber resilience survey, which we conducted again across mostly the same population of FMIs throughout Europe. The results have given us an insight into how the sector has progressed, and indeed, while we see improvement in some areas, there is still much to be done.

When we established the ECRB, the aim was essentially to create a forum for strategic discussions at board level, to raise awareness of the topic of cyber resilience, to catalyse joint initiatives to develop effective solutions for the market and to share best practices and foster trust and collaboration. In this context, I am very pleased that the spirit of the ECRB is living up to expectations. As you will recall from the UNITAS crisis

communication exercise last year[4], we identified two key areas in which the ECRB could drive improvements forward: *information sharing* and *crisis management*. This year, thanks to your commitment and contribution, we have set up two working groups of experts drawn from your institutions and we have made significant progress in these areas. I would like to sincerely thank you for your contributions and for sustaining our spirit of trust and collaboration.

The ECRB working group on information sharing will tell us about their proposed model, which sets out the building blocks for sharing information and intelligence. It is clear that, among other things, financial infrastructures should have effective cyber threat intelligence processes; they should actively participate in information-sharing arrangements and collaborate with trusted stakeholders within the industry. The working group's proposal seeks to address this by facilitating information and intelligence sharing, enabling you to better protect yourselves and the wider ecosystem. As discussed at our last meeting, regulatory reporting on cyber incidents is intentionally not part of this work.

We will also receive an update on the work of the ECRB working group on crisis management, and we will touch upon third-party risk and ecosystem recovery and coordinated reconciliation.

As you may guess from my brief remarks today, we have a great deal of work ahead of us. I believe that sharing information, knowledge and expertise among financial infrastructures and authorities in a non-regulatory context remains essential for tackling the cyber challenge we all face. I am convinced that we can only do this by joining forces. I want to thank you for being here today and I look forward to a fruitful discussion.