Fabio Panetta: Protecting the European financial sector - the Cyber Information and Intelligence Sharing Initiative

Introductory remarks by Mr Fabio Panetta, Member of the Executive Board of the European Central Bank, at the fourth meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures, Frankfurt am Main, 27 February 2020.

* * *

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, I have taken over chairmanship of the Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB). I would like to take this opportunity to thank my predecessors for their efforts in taking forward the work of the ECRB. I look forward to following in their footsteps and contributing to the excellent work being undertaken on cyber resilience at the European level.

Protecting the integrity of the financial system, and maintaining confidence in it, is critical. Specifically, financial market infrastructures are crucial for intermediation between market participants and end users. They are critical for the everyday livelihood of European citizens, for instance by transmitting salary and pension payments. They are also vital for the functioning of the financial system and the financing of the real economy, as they settle market transactions through a web of settlement banks, clearing houses, settlement systems and custodians.

Cyberattacks are already used to harm companies and to interfere with national and international politics. Cyberattacks against financial market infrastructures would undermine confidence in the financial system, with repercussions on the economy as a whole. Fending off these attacks is therefore a matter of European security.

The range of motivations for compromising the financial sector includes financial gain, a desire to create havoc and disruption, and meticulously planned espionage. In any of the given scenarios, the impact can be severe. Cyberattacks can threaten financial stability by disrupting the interconnected and interdependent operational network and its critical nodes. Cyberattacks can result in the corruption or loss of data or the outright loss of systems and critical infrastructure.

Cyber risk is a danger which has the potential to trigger a systemic crisis.[1] In financial terms, while the total costs of cyber incidents are hard to establish, industry estimates range from USD 45 billion to USD 654 billion for the global economy in 2018.[2] According to some estimates, the average cost of cyber incidents had increased by 72% in the last five years[3] and businesses will fall victim to a ransomware attack every 11 seconds by 2021[4].

All of the financial infrastructures represented around the table today are at the forefront of providing safe and innovative solutions to the European market. Your collective activity and collaboration in this sphere of cyber resilience is critical for the financial stability of Europe.

Given the unconventional nature of cyber risk, we need to be agile and sophisticated in our approach. I am pleased to say that, over the past few years, we have made significant progress at the European level.

The cyber resilience oversight expectations (CROE)[5] published by the ECB in 2018 are now being followed by financial infrastructure operators across Europe. They are even gaining global traction: for example, the World Bank has formally adopted the CROE[6] to help boost the cyber resilience of financial market infrastructures in emerging market economies under its mandate, as well as to promote global harmonisation.

The European Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU)[7] was introduced in 2018 to help entities test and improve their resilience against sophisticated cyberattacks. Since its publication, the TIBER-EU Framework has been adopted by the ECB in its oversight capacity and, at national level, by Belgium, Denmark, Germany, Ireland, Italy, the Netherlands, Romania and Sweden. It is close to adoption in Norway and Finland and more countries are to follow. This means that we are well on the way to ensuring that threat-led penetration testing is conducted in a harmonised way across the EU, avoiding duplication of work for financial entities and authorities alike.

And, of course, setting up the ECRB itself as a forum for strategic discussions on cyber resilience has been an important step. Building on what we have achieved so far, we today wish to launch the Cyber Information and Intelligence Sharing Initiative (CIISI-EU), which members overwhelmingly backed at our meeting in June 2019. This initiative would support our aim of catalysing joint initiatives to develop effective market solutions, working together for the public good and fostering trust.

By addressing cyber risks that can be systemic and highly costly in an increasingly sophisticated threat landscape, CIISI-EU will contribute to protecting the European economy and security. The initiative will allow the most important financial infrastructures to share vital technical information among themselves using an automated platform. Members will create a trusted community where they will meet to discuss cybersecurity threats and share related intelligence and best practices. The ECRB members will receive bi-annual threat reports informing them of strategic issues pertinent to their businesses.

Exchanging cyber information and intelligence among peers within a trusted community allows financial infrastructures to leverage the collective knowledge, experience and capabilities of that community to address the threats they may face. It enables them to make informed decisions about their defensive capabilities, threat detection techniques and mitigation strategies. By sharing cyber information and intelligence, financial infrastructures act in the public interest to support the safe and sound operation of the financial system as a whole.

We should not underestimate the significance of taking this step. Never before have the largest pan-European financial infrastructures, in close liaison with Europol and the European Union Agency for Cyber Security, come together and agreed to share information and intelligence. For years, the industry has talked about sharing information and intelligence, but few have actually done it.

The ECRB working group on information sharing, comprised of ECRB members and authorities, has worked very hard over the last year to push forward this unique and ground-breaking model of cooperation. The CIISI-EU operating model has the potential to serve as an example to other communities and jurisdictions on how to work together, share information and catalyse new initiatives.

The work we do within the ECRB also supports the ambitions set by the European Commission as part of its Digital Single Market strategy. Strengthening trust and security is a key element of that strategy, and the Commission has recently launched a public consultation on a potential legal initiative to improve the resilience of financial services against cyberattacks[8]. We look forward to hearing more about this today from the European Commission.

I want to thank you for being here today. I look forward to a frank, open and fruitful discussion and to continuing the good cooperation between pan-European financial infrastructures, central banks and other authorities.

---

[1] European Systemic Risk Board (2020), *Systemic cyber risk*.

[2] *ibid.*

[3] *ibid.*

[4] Cybersecurity Ventures, *2019 Official Annual Cybercrime Report*

[5] European Central Bank (2018), *Cyber resilience oversight expectations for financial market infrastructures*

[6] ECB press release of 6 January 2020, World Bank adopts ECB's cyber resilience oversight expectations

[7] European Central Bank (2018), TIBER-EU Framework

[8] European Commission, *Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure*, Consultation document.