Fabio Panetta: Keeping cyber risk at bay - our individual and joint responsibility

Introductory remarks by Mr Fabio Panetta, Member of the Executive Board of the European Central Bank, at the fifth meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures, Frankfurt am Main, 16 December 2020.

* * *

At the last meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB), we were all in the same room at the ECB premises in Frankfurt am Main. That was on 27 February 2020, when we launched the Cyber Information and Intelligence Sharing Initiative (CIISI-EU)[1]. We already knew this was a critical step in addressing cyber threats. But we did not know just how timely it was.

Shortly after that meeting, the first wave of the coronavirus (COVID-19) pandemic led to strict containment measures across Europe. While the upcoming vaccine roll-outs are a light at the end of the tunnel, mobility restrictions are likely to remain in place for some time.

These restrictions have confronted us all with unparalleled challenges in our personal and professional lives. In response, the world has taken a giant leap forward in terms of digitalisation.

And when the public health situation finally improves, we will not go back to the old normal. Working from home has become the norm for many of us. We have adjusted our way of life. And while we will certainly enjoy regaining our ability to move and interact freely, we will also learn lessons from the pandemic and see benefits from how we adapted to it. The digital transformation is here to stay.

But for digitalisation to contribute to economic resilience beyond the pandemic, cyber resilience will be paramount. Otherwise, digitalisation may increase risks rather than reduce them. Today I will argue that this applies to the financial sector in particular and I will discuss the necessary policy response.

Digitalisation and the resilience of the financial sector: lessons from the pandemic

Digitalisation is transforming financial services and consumers' behaviour[2]. As our recently published study on the payment attitudes of consumers in the euro area (SPACE)[3] shows, almost half of euro area adults now prefer to pay digitally.

And the more Europe's citizens rely on digital payment initiation – be it by card, credit transfer or direct debit – the more Europe's businesses rely on the underlying financial infrastructures or the clearing and final settlement of these transactions. The resilience of these infrastructures is of key importance to the functioning of Europe's economy, especially during troubled times.

Well-functioning financial infrastructures are also crucial to enabling the unprecedented measures that have been taken to stimulate Europe's economy in response to the devastating effects of COVID-19. This applies to emergency aid and recovery packages implemented at national level as well as to the ground-breaking decision to use EU borrowing to support the crisis response and stimulate the recovery. The related financial flows can only be channelled to their beneficiaries through stable and reliable trading, clearing and settlement infrastructures.

One thing is clear: the *operational* resilience – and with it the *cyber* resilience – of financial entities and of our financial system as a whole is just as important as their *financial* resilience.

Safeguarding the cyber resilience of financial services: building the European lines of

defence

To safeguard the cyber resilience of financial services, the EU can build on three lines of defence: regulation and oversight, cyber resilience testing, and intelligence sharing.

The European Commission's proposal for a Digital Operational Resilience Act (DORA)

In September this year, the European Commission launched its proposal for a Digital Operational Resilience Act[4] now commonly referred to as DORA. As indicated by the Commission, EU financial services legislation since the financial crisis has focused to a large extent on financial risks associated with financial services, while it has not fully addressed the digital operational resilience of the entities offering these services. DORA is therefore a welcome initiative: it provides a unique opportunity to address the current fragmentation in financial legislation and supervisory approaches in the field of digital operational resilience, including cyber resilience.

DORA incorporates the lessons that have been learned from the Eurosystem's cyber resilience strategy for financial market infrastructures. It covers – implicitly or explicitly – the Eurosystem's cyber resilience oversight expectations, the European programme to test and improve the resilience of the financial sector against sophisticated cyber-attacks (TIBER-EU), and the Cyber Information and Intelligence Sharing Initiative created by the ECRB (CIISI-EU). We will hear more from the European Commission today on DORA, including how it contributes to the Commission's wider digital finance package[5].

Testing cyber resilience: the TIBER-EU framework

While cyber risk is a form of operational risk, it has its own unique characteristics, namely the speed and scale at which it can spread and the intent and perseverance of threat actors. The best way to demonstrate cyber resilience is to test it in a way that mimics a real-life attack. That is what the TIBER-EU framework is about. TIBER-EU is currently implemented in ten European countries. Some of the participants in this meeting have already gone through a TIBER-EU test. The Netherlands and Denmark have drawn the main findings from the first wave of tests performed on Dutch and Danish core financial entities and I look forward to learning more about them today.

Sharing intelligence: the Cyber Information and Intelligence Sharing Initiative

The objective of the ECRB is to foster trust and collaboration between pan-European financial market infrastructures and critical service providers on the one hand, and between both of these groups and the relevant authorities on the other. The ECRB also aims to encourage joint initiatives whose goal is to increase the cyber resilience capabilities of the financial sector and to reinforce its operational resilience more generally.

Trust, collaboration and joint initiatives form the bedrock of the ECRB's Cyber Information and Intelligence Sharing Initiative (CIISI-EU)[6]. In February this year, we launched this initiative and committed to implementing it. Today we will hear about the progress achieved so far. For the CIISI-EU to be a success and contribute to the stability of Europe's financial system, we need to make sure not only that all building blocks are in place, but also that we actively share cyber information and intelligence.

Conclusion

We want to avoid a situation where a cyber incident affecting financial infrastructures could evolve into a systemic financial crisis. Assessing whether or not this will happen hinges on identifying whether a cyber incident will escalate from the operational level to the financial level, and ultimately start damaging confidence.

So we must continue our efforts to prevent cyber incidents. And if they do occur in spite of our individual and collective efforts, we must make sure they do not escalate. The work of the ECRB is instrumental here, as it encourages trust, cooperation and joint initiatives. Cyber resilience is not a *state*, it is an *ever-shifting aspiration.* Improving our cyber resilience and staying ahead of our adversaries requires ceaseless efforts from all of us. We are all individually responsible, but we are all in it together.

---

1 See the related press release and F. Panetta (2020), "Protecting the European financial sector: the Cyber Information and Intelligence Sharing Initiative", Introductory remarks at the fourth meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures, 27 February 2020.

2 See F. Panetta (2020), "On the edge of a new frontier: European payments in the digital age", Keynote speech at the ECB Conference "A new horizon for pan-European payments and digital euro", 22 October 2020; and F. Panetta (2020), "From the payments revolution to the reinvention of money", Speech at the Deutsche Bundesbank conference on the "Future of Payments in Europe", 27 November 2020.

3 See the press release on the topic, as well as the full report.

4 Proposal for a Regulation of the European Parliament and the Council on digital operational resilience for the financial sector, 24 September 2020.

5 See the European Commission's website for details.

6 For more details on CIISI-EU, see "Combating cybercrime: sharing information and intelligence as the first line of defence", September 2020.