Introduction

DeNederlandscheBank
EUROSYSTEEM

Opening

Good morning everyone. Let me also extend a warm welcome to this press conference on our Financial Stability Report.

Risk landscape – Confluence of risks



Let me start with the good news. Economic growth in the Netherlands is still robust, and our financial institutions have solid buffers. That said, cyber risks and operational risks are on the rise and can affect financial stability through a loss of confidence or lower revenues.

In the FSR, we therefore conclude that the risks to financial stability have increased. And they were already quite significant; as you know, I mentioned code amber earlier. What is now a further cause for concern – even more so than before – is the possibility that various shocks and vulnerabilities may occur simultaneously and thereby reinforce one another. And cyber threats are no longer just a risk; they are already happening. However, no cyber attack has yet been found to be systemic.

The scope for absorbing shocks is shrinking

In addition, the scope for absorbing setbacks has diminished, meaning that new shocks can spread more quickly and more widely throughout the financial system. There are several causes for this. For example, higher interest rates and high levels of public debt mean that governments have less fiscal scope for absorbing shocks.

There is also less wriggle room in monetary terms. After all, in an uncertain geopolitical world, supply shocks can keep inflation – and therefore interest rates – elevated for longer. Furthermore, the financial system's resilience to shocks has been reduced by the increasing use of leveraged financing. In addition, banking buffers are falling in some parts of the world, although fortunately this is not the case in the Netherlands.

Cyber risk

Let me now address the most pressing risk to financial stability, which is cyber risk and its relationship to AI.

Cyber risk is nothing new. What is new, however, is that we currently regard cyber risk as the main threat to Dutch financial stability. Other institutions – such as the ECB and the AFM – have also recently highlighted the elevated cyber risk.

Cyber attacks have now become an almost daily reality. And we are seeing more and more successful attacks, both within and outside the financial sector. Take, for example, the crypto trading platform Binance, the French bank Crédit Mutuel Arkea and, most recently, the European Commission, Visa, Mastercard and JP Morgan.

So far, these cyber attacks have not caused widespread disruption in the financial sector, but this could well happen. In fact, we simply have to take it into account. This is because financial institutions are dependent on a small group of technology firms. Furthermore, cyber threats are increasing as new AI models are being developed.

AI and cyber risk

Powerful and autonomous AI models make cyber attacks faster, more powerful and therefore more damaging. Attackers need less specialist knowledge to carry out an attack. This works to the attackers' advantage. A single vulnerability can be enough to enable a successful attack, while defenders need to secure the entire system.

The need to quickly patch digital vulnerabilities is therefore increasing. And with that comes the risk that financial services may temporarily be disrupted or need to be suspended to prevent further damage. We have seen this most recently at Ahold. In the event of a cyber incident in the financial sector, too, it may be necessary and advisable to disconnect systems from the internet for a few hours or days.

Policy recommendation: the operational bar has been raised, demanding a greater focus on crisis preparedness

Although cyber resilience is already a high priority for financial institutions, the bar is being set ever higher due to the rapid AI advances. Financial institutions are therefore required to invest continuously in their operational defences. The same applies to us at DNB. We have, for example, significantly scaled up our capacity to address digital vulnerabilities.

At the same time, it can no longer be ruled out that a potentially system-wide disruption may occur. As a society, we will therefore need to prepare ourselves as best we can for such situations. That calls for closer collaboration and more operational drills.

In the Netherlands, contingency planning for payment and capital market transactions is well organised. Public and private sector organisations are working well together. However, the financial sector is also dependent on other vital infrastructure, such as energy supply and telecoms. We simply need to practise together more.

Furthermore, many cyber threats are cross-border in nature, so we must also carry out more drills at European level and involve the sector more closely in this.

Society, too, must prepare itself. The 24-hour economy will not be able to keep running continously. By keeping an emergency kit and sufficient cash to hand, we can minimise the social impact of a disruption.

AI and financial risks

The risks associated with AI are not just of an operational nature; they can also be financial. In the FSR, we have set out two possible scenarios for this. In the first one, we examine the risks should the high earnings expectation of AI-related firms prove to be unsustainable.

Tech and AI firms have been very dominant in the stock markets for some time now. This is accompanied by relatively high valuations and a significant weighting in many stock indices. In recent weeks, investors appear to have become more critical about the high expectations surrounding AI. This is also reflected in the volatile prices of technology and AI stocks.

At the same time, we are seeing AI play an increasingly important role in bond markets as well. After all, ramped-up investment in AI is increasingly being financed through debt. Debt is growing rapidly, increasing the use of leveraged financing within the system. Furthermore, complex structures and interconnections make it more difficult to gain a clear picture of exposures within the financial sector.

Policy recommendation: maintaining buffers in the financial sector is increasingly important

In this risky and uncertain world, it is essential that financial institutions maintain their buffers. Robust buffers ensure financial resilience and instil confidence. I therefore believe it is important that we do not lose this resilience, and as far as I am concerned, that is a key condition when simplifying regulations. And it is against this backdrop that we will assess the European Commission's proposals to strengthen the competitiveness of the banking sector.

DeNederlandscheBank
EUROSYSTEEM

Conclusion

In conclusion, let me summarise as follows. Like a medicine, AI can have real benefits: it can drive productivity growth and economic growth. But don't skip the leaflet: be aware of financial and operational vulnerabilities and be prepared in case things *do* go wrong.