Steven Maijoor: A race we cannot afford to lose - cybersecurity in an age of geopolitical tensions

Speech by Mr Steven Maijoor, Executive Director of Supervision of De Nederlandsche Bank, at the International Swaps and Derivatives Association (ISDA) Annual General Meeting, Amsterdam, 14 May 2025.

* * *

On April 22 the Dutch Military Intelligence and Security Service reported that it had detected a Russian cyberattack targeted at a Dutch critical public service. It was the first time a state-sponsored cyberattack was reported in the Netherlands. Which is not the same as saying that it happened for the first time.

Geopolitical tensions have been rising for more than a decade, but over the past few years they have accelerated. Needless to say this is bad news for the world economy and the financial sector. But perhaps in no area is the geopolitical threat so real and acute as in the digital domain.

State-sponsored cyberattacks are often very well concealed, so we do not have reliable numbers on how often they occur. But anecdotal information from intelligence agencies suggest their number is increasing.

Traditionally, the financial sector has been targeted by cyber criminals with financial motives. But with the changing geopolitical climate, nation-state cyberattacks on financial institutions have become a realistic possibility. The aim of nation-state actors is usually not financial gain, but disruption. For them, the financial sector is an attractive target. The sector is crucial to the functioning of the economy. Also, many financial firms depend on the same third-party service providers. If one of these suppliers is attacked, large chunks of the financial sector may experience the knock-on effects. As we showed in our latest Financial Stability overview, a quarter of all reported global cyberattacks – so including energy and telecom - can potentially affect the financial sector through this channel.

Artificial Intelligence is likely to reinforce the cybersecurity threat. AI makes cyber-attacks more sophisticated. At least some of them, like phishing. Also, the scale, access and speed of cyber-attacks will probably go up.

Recently, we have seen this very clearly in the context of cyber-crime. For example, by enabling very advanced deepfakes. We had the rather spectacular case of a finance worker in Hong Kong, who was tricked into paying out $ 25 million. The fraudsters used deepfakes to pose as the company's CFO in a videoconference call. Although nation-state actors use AI, we have not yet observed them using these techniques to create large scale disruptions. But what if nation-state actors fully exploit the potential of AI, and use it to disrupt vital processes on a larger scale?

When we talk about financial institutions in this context, most people will first of all think of banks. But for you, I think Central Counterparty Clearing Houses and other market infrastructures are perhaps just as important. Many of you depend on them for the

trading, clearing and settlement of transactions in foreign exchange, securities, options and derivatives.

Market infrastructures occupy a unique position in the cyberthreat landscape. They seem to be targeted less, but if, for example, CCPs are attacked successfully, the impact could be very high. This is partly because there are relatively few of them. If party A goes down, it can be difficult for party B to compensate. Their attack surface is also relatively smaller because they offer fewer types of services compared to banks. Also, they have fewer public-facing web applications, and fewer customers than banks. However, the systems they do operate are highly advanced and very important for the functioning of the financial system.

All of these features make them an attractive target for nation-state actors who want to cause maximum disruption. This does not mean that market infrastructure parties are currently being attacked. But given the geopolitical situation, tomorrow's reality could be different.

What makes CCPs potentially more vulnerable than banks is that most of them have outsourced part of their cybersecurity. That is understandable. If you are a large bank, having a few hundred cybersecurity experts is an affordable investment. CCPs do not have the resources for this. To them, outsourcing provides access to expertise and higher standards for cyber and information security. But the drawback of course is that it makes CCPs dependent on external parties, and it makes their cyber defence more complex.

All this means CCPs need to stay alert. Cyber resilience is at least as important for CCPs as it is for other financials.

Many financial institutions have taken big steps in recent years to boost their cyber resilience. But given the size, urgency and evolving nature of the threat, we need to do even more to keep financial services safe. It seems more and more that we are involved in a digital arms race. A race with a sophisticated and cunning opponent. A race in which we want to be roadrunner, and not the coyote.

This is why cyber resilience will absolutely be a key focus area in our supervision of the financial industry in the coming years. Our aim as a supervisor is to make financial services and the financial system safer against cyber threats. Not only by increasing the resilience of the financial sector itself, but also by stepping up the robustness of the entire chain of ICT service providers. DORA, the European Digital Operational Resilience Act, that came into effect at the beginning of this year, gives us additional tools to accomplish this aim.

To start with, under DORA, threat-led penetration tests are mandatory for the largest financial institutions in Europe. In the Netherlands we have been conducting these kinds of tests voluntarily for over eight years with good results, and we are very pleased that it is now becoming the norm at the European level. The largest CCPs within the EU will be part of the group of financial institutions for which the penetration tests will be mandatory.

But DORA also imposes stricter requirements for managing cyber risks in outsourcing chains. For example, financial firms face stricter rules for conducting due diligence on potential ICT providers. And very importantly, under DORA, European supervisors can conduct inspections of critical third-party ICT service providers in tandem with national supervisory authorities. We expect big techs like Google and Microsoft to be placed under EU-wide supervision. And, just as with the banks, we are going to test their readiness to detect and withstand cyberattacks.

Despite all efforts, there is no such thing as perfect cyber security. It is therefore vital that financial institutions take measures to recover quickly after cyber incidents. This is crucial to ensure that services can continue and people don't lose trust in financial firms or the financial sector as a whole.

The results of the ECB's 2024 cyber stress test of a group of banks show that there is room for improvement on the recovery front. So it's a very good thing that DORA also imposes new requirements on institutions' continuity plans and backup policies. They need to develop a culture where cyber incidents are quickly detected and reported. They need to have their playbooks in place. And they need to have clearly defined management roles and responsibilities. And this includes good crisis communication, which is absolutely essential. These are all key ingredients for an effective response after a cyberattack.

But even if we all have our own house in order, that is not enough. Because on a digital level the financial sector is so interconnected, and connected to other vital sectors of the economy as well, that some degree of overall coordination and cooperation is necessary.

Governments should take the lead to improve cross-sectoral cooperation and coordination. They must continue to conduct large-scale cyber-drills and practice activating crisis plans. The insights gained should be used to enhance resilience.

Under the new legislation supervisors also have an obligation to cooperate closely with other sectors. DNB is putting this into practice by working with sectors that are most critical to the financial sector, such as energy and telecommunications. Within our mandate, we support these sectors with information, cooperation and ethical hacking experience.

To keep financial institutions and the financial system safe, resilience against cyberattacks has become just as important as holding sufficient capital and liquidity. So we need to do whatever we can to further boost it. Both in terms of detection and recovery. And we need to work together. Governments, banks, market infrastructures, supervisors, telecom, energy and other vital players in the outsourcing chain. Because this is a race we cannot afford to lose.