Steven Maijoor: Cyber resilience in an age of geopolitical tensions

Speech by Mr Steven Maijoor, Executive Director of Supervision of De Nederlandsche Bank, at the Annual FinTech and Regulation Conference, Brussels, 4 February 2025.

* * *

On December 12th 2023, Kyivstar, Ukraine's largest telecom provider, suffered a cyberattack that disrupted services for millions of users. The attack, attributed to the Russian state-sponsored group Sandworm, was one of the biggest cyber incidents in Ukraine since the onset of the Russian invasion. The hackers had infiltrated Kyivstar's infrastructure months earlier. They deployed malware that erased thousands of virtual servers and personal computers, crippling the company's network for managing communication services.

The attack had several immediate effects. First of all, approximately half of Kyivstar's network was disabled, leaving millions without mobile and internet connection. But the damage wasn't limited to the telecom sector. The attack also disrupted banking operations, payment processing, and online banking services. Some ATMs and point-of-sale terminals didn't work. Financial transactions were in disarray across the country.

Amazingly, the Ukrainians were quickly able to restore services. Over the past three years they have become quite proficient in dealing with large-scale disruption. Many critical processes in Ukraine are equipped with redundancy measures. Many people even have two sim cards in their phones. That enabled the other Ukrainian telecom providers to circumvent the outage. Services at Kyivstar were gradually reinstated, with almost full restoration achieved eight days after the attack.

This episode raises some inconvenient questions. What if this would happen to us? What if a large scale Russian or Chinese cyberattack is launched on the telecoms sector of an EU member state? Would it be possible? How much damage could such an attack cause? Would it affect financial services? And would we be able to recover as quickly as the Ukrainians did?

A few years ago, most people would have found these questions to be rather hypothetical, but today, unfortunately, they have become quite urgent. Geopolitical tensions have been rising for more than a decade, but over the past few years they have accelerated. Countries are re-arming, they are protecting their strategic economic infrastructures, they are imposing trade restrictions and sanctions on each other, and they are weaponising access to international financial infrastructures and services. 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.

Apart from the Kyivstar case, there are many other examples to back this up. In late 2023, a Russian hacker breached Microsoft's corporate network by exploiting a legacy account. As a result, the security and confidentiality of the email accounts of many organisations around the world were potentially compromised. Last year, the FBI discovered a dormant network of Chinese hackers in the United States that had compromised hundreds of routers and that was on standby to launch an attack if called on. And recently, Russian and Chinese vessels were suspected of damaging subsea data cables. Since state-sponsored cyberattacks are often very well concealed, we do not have reliable numbers on how often they occur. But anecdotal information from intelligence agencies, like the Dutch General Intelligence and Security Service, suggest their number is increasing.

Traditionally, the financial sector has been an attractive target for cyber criminals with financial motives. But with the changing geopolitical climate, nation-state cyberattacks have become a very real possibility. Their main aim is to cause disruption and to steal sensitive information. Nation-state actors possess more resources, sophistication, and endurance than other hackers. And many sectors of the economy have become more vulnerable to large-scale disruption due to increased complexity and digitalisation. This is certainly true of financial services, with their long outsourcing chains and interconnectedness. And many financial firms depend on the same third-party service providers, so 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 can potentially affect the financial sector through a vital process run by a third party on which the financial system depends.

So, to answer the questions I posed at the start: yes, I think a major state-sponsored cyberattack on the financial sector or one of its supporting sectors could happen. And frankly, I hope we would be able to recover as quickly as the Ukrainians did.

That is not because financial institutions haven't prepared. Many financial institutions have taken big steps in recent years to boost their cyber resilience. I think it is fair to say the financial industry is one of the better digitally defended sectors in the economy. As it should be. But given the size and urgency of the threat, we need to do even more to keep financial services safe. This is why cyber resilience will absolutely be a key focus area in our supervision of the financial industry in the coming years. This goes both for De Nederlandsche Bank, and for the European Central Bank.

Our aim is to make financial services 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.

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. As a result, Fintechs may also experience more stringent due diligence from financial sector customers. 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 bigtechs 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 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. These are key ingredients for an effective response after a cyberattack.

An important principle of our supervision has always been that financial institutions are responsible for putting their own house in order. And that is also the case with cybersecurity. But if we only focus on individual institutions, we miss something. As I mentioned, 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 to arrive at an optimal level of resilience. Notably, recent assessments, derived from nationwide contingency exercises in the Netherlands, reveal various weaknesses. These weaknesses relate to the exchange of information between critical infrastructure providers, the distribution of roles and responsibilities, and the mobilisation of scarce cyber security knowledge and expertise in the event of major cyber incidents.

So the message here is: we need to work together. 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.

But there is also a role for financial supervisors like DNB. Under the new legislation, we do not only need to check whether financial firms are compliant, but we also have an obligation ourselves to look over the fence and cooperate closely with other sectors. DNB is putting this into practice by working with vital 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 sum up, the threat of major disruptions to our financial system from nation-state cyberattacks has become more urgent. Financial firms, and the entire outsourcing chain on which they depend, therefore need to do whatever they can to further boost their cyber resilience. Both in terms of detection and recovery. Cyber resilience is a top priority for European financial supervisors and there are new European laws in place. And we are going to use these laws to make sure that financial institutions under our supervision are as secure and well defended as possible. Enhancing resilience also means we need to work together. Governments, financial firms, supervisors, telecom, energy and other vital players in the outsourcing chain. Because in cyberspace, we are all linked together. And after all, a chain is only as strong as its weakest link.

Thank you.