Tuomas Välimäki: Opening remarks - Nordic Cyber in Finance Conference

Opening remarks by Mr Tuomas Välimäki, Board Member of the Bank of Finland, at the Nordic Cyber in Finance Conference, Helsinki, 30 October 2024.

* * *

Dear colleagues, dear friends,

A very warm welcome to the seventh Nordic Cyber in Finance conference, hosted by Suomen Pankki, the Bank of Finland. In Finland, we hold resilience and preparedness in high regard, and I am no exception to this. It is a privilege and an honor to open this highly topical event today.

Over the course of the day, we will explore different themes centered on resilience and preparedness. We will deal with hybrid threats in cyber space - critical infrastructure protection, information manipulation and cyber defense tools. These topics will be covered by a distinguished line-up of speakers ranging from cyber security industry to financial institutions as well as authorities. I will now provide you with an overview of what lies ahead and, more importantly, emphasize why these topics matter.

Network Effects, Interconnectedness, and Collaboration

The financial industry prospers on increasing network effects. This creates an inherent drive for growth, where often the largest players dominate the market. As businesses scale, the dependency within the industry deepens, making individual entities critical to the overall network. While this growth may benefit business, it also magnifies the importance of preparedness, as failures can become too large to bear.

This is true not only for payment systems and commercial banks but also for central banks. For instance, over the last two decades, TARGET services have evolved into one of the most efficient settlement systems globally, a testament to the power of scale. Today we will learn how Eurosystem secures Europe's financial backbone, i.e. the TARGET services. Ensuring the security of such a critical infrastructure is a mission that demands relentless efforts. We must maintain and strengthen community wide partnerships to safeguard this backbone.

Critical Infrastructure and Path Dependency

The interdependencies within critical infrastructure extend beyond finance. Consider the electrical grid, which the financial sector heavily relies on. If a major electricity producer or distributor fails, the consequences can be swift and severe for the whole electric system – much like the systemic impact that we've witnessed also in financial crises. These interconnected systems highlight that path dependencies are not industry-specific; they are intertwined across multiple sectors, systems, agreements and customers.

While banks are generally well-prepared for major disruptions, the same cannot always be said for the average citizen or business. For example, large banking institutions are likely to sustain operations during a power outage, but the same cannot be expected for the average citizen or a small firm. The combination of systemic risk and contagion is a central concern for central banks. It underscores the need for a holistic approach to resilience – one that draws lessons also from other sectors. Today, we will hear from a power system network operator on how they as a critical service providers approach disruptions like geopolitics and green transition.

Hearts and Minds

Hybrid warfare isn't limited to physical infrastructure; it also targets our hearts and minds. Some might argue – and I expect some of today's speakers will – that safeguarding our mental processes is even more crucial than securing infrastructure. While I won't take sides, I do believe both are essential.

The way people think and form opinions can have profound impact on societal order. There is ample evidence throughout the history, how minds have been influenced and opinions shaped. Without listing historical nor recent examples, I trust we can all agree on this point. I also believe social media and new technologies have evidenced their capabilities for spreading misinformation at hyper speed and sowing widespread distrust.

The importance of this issue is especially true in the financial sector, where trust is paramount. Lose trust, and customers will leave. Lose trust at the systemic level, and civil order can quickly unravel.

Loss of confidence is central to all systemic crises. Even if not the initial cause, it accelerates crises to new levels. Financial crises have demonstrated how liquidity position of an institution is not only depending on the institution in question but also on the confidence of others. Trust can deteriorate through contagion - even if the crisis begins with another institution.

While technical problems can often be resolved, a coordinated attack on both technology and public trust poses a far greater threat.

Now, imagine a hybrid scenario where critical infrastructure is compromised or even damaged. For this example, the exact location of the damage is irrelevant, as we normally have robust measures in place across sectors to compensate for lost capabilities. We can re-route telecommunications, implement temporary solutions within the power grid, and even deploy backup clearing systems if necessary. Next, imagine that a second or third element in this scenario involves eroding overall trust in the financial system. Suddenly, the issue becomes contagious, escalates rapidly, and becomes much harder to contain – a textbook example of how systemic risks emerge. This is a fascinating topic, and fortunately, we have an entire session dedicated to it today.

Facilitating the Discussion

The financial industry is well-positioned to lead discussions on hybrid threats. Our existence depends on trust, and our interconnectedness means that threats can have a clear and wide-reaching impact. We engage in these conversations not to seek trouble but to emphasize the importance of proactive, coordinated responses in a highly networked world.

While time may be on the attacker's side, we must remain vigilant and learn when and how to respond effectively. In this learning process acting together is vital. Cyber threats don't follow a zero-sum game. If one institution's trust is compromised, the effects ripple industry wide. Indeed, when it comes to fighting cyber-crime or hybrid warfare, two plus two definitely equals much more than four. I am confident that today's event is a step toward building a stronger, more resilient industry and society.

I sincerely hope you find the topics we discuss today both engaging and thought-provoking. With ten presentations and two panel discussions ahead, let's make the most of this opportunity to collaborate and learn from one another.

Thank you for your attention and once again, a warm welcome to this year's Nordic Cyber in Finance conference!