SPEECH

BY GOVERNOR LARS ROHDE AT THE NORDIC CYBER CONFERENCE

DANMARKS NATIONALBANK

CHECK AGAINST DELIVERY

21 November 2017

On behalf of the Nordic central banks I would like to welcome you all to the *1st Annual Nordic Cyber Conference* here in Copenhagen. I am very pleased to see that so many have chosen to participate today.

I want to give a special warm welcome to all the presenters who have agreed to share their knowledge on cybersecurity with us; it is highly appreciated.

CYBERTHREATS AND FINANCIAL STABILITY

The cyber threat is real. The World Economic Forum has consistently ranked cyberattacks and data theft among the top 10 global risks and cyber is discussed among the world's leaders alongside natural disasters and interstate conflict when they meet in Davos.

In worst case cyberattacks could lead to financial instability. When it comes to securing the financial stability, cyberresilience is a factor alongside ensuring that the credit institutions are robust and that they have sufficient capital and liquidity reserves to draw on in difficult times.

The cyberthreat is here to stay, and to me personally it means that terms like red-team testing, NotPetya and social engineering are becoming part of my everyday vocabulary.

INTERCONNECTED AND BACK-UP

We live in a digitalised world. And the Nordic countries are among the most digitalised countries in the world. Also, the Nordic countries are renowned for having some of the most modern and well-functioning financial infrastructures in the world. One example is the instant retail payments.

These solutions are based on a close collaboration within the financial sector in the Nordic countries. This is something to be proud of and a strength, but in some sense this high level of interconnection is also a liability.

We are not stronger than the weakest link.

It is therefore essential that we take measures to best protect us from cyberattacks, detect them when they occur, respond to them appropriately, and recover from them as fast as possible. Otherwise the very foundation of our digital financial sector could be compromised.

And let us not forget that ultimately the cyberthreat could endanger the trust in the financial sector and also the digitalisation of the society as a whole.

One question that comes to my mind though, is the following:

Do we have a sufficient back up system if our infrastructure systems do not work for a longer period of time?

We need to focus on this in the future.

CYBERATTACKS IN A FINANCIAL CRISIS

The cyberthreat is complex. Attacks are perpetrated by a diverse group of agents, from small-time offenders through hacktivists to nation states. Attacks may spread rapidly through networks, and their impact can reach far beyond their intended targets.

One example is the NotPetya attack on Ukraine in June this year. The malware spread to a large number of global companies and seriously disrupted their operations for days. One victim was the Danish shipping giant Maersk, which has since reported losses between 250 and 300 million dollars due to the incident.

Imagine that such an attack were to hit a bank that was already in financial trouble during the financial crisis in 2008?

Imagine that a major attack hit the entire financial sector with the same consequences as NotPetya?

The consequences for financial stability could be severe.

CORPORATION
Central banks – in close cooperation with the financial sector, public authorities, and the governments – need to play an active role in enhancing the cyberresilience of the critical financial infrastructure.

This cooperation should of course also be supplemented by initiatives in the financial sector. In that regard, I am very pleased that the Nordic banks have decided to establish the Nordic Financial Cert with the main purpose of sharing information and thereby increasing the cyberresilience in the Nordic financial sector.

CONTENT OF THE CONFERENCE
In my view, one of the best ways to ensure higher cyberresilience is through knowledge-sharing, and that is exactly what I hope we can all achieve at the conference today.

We will begin with an overview of the cyberthreat seen from different perspectives.

Next, we will learn how to deal with it, on a national strategic level, both from a governmental and a private sector point of view. We will continue the afternoon with a discussion of cyberregulation as well as cybertesting individual institutions.

Finally, our keynote speaker, Lucas Kello, will give us his view on how the digital future may appear in the light of evolving cyberthreats.

The cyberthreats are here to stay and we must continually adapt to the changing landscape of technology, threats, and actors. Your participation at this conference today is a first step in this adaptive direction. Thank you.

Now, it gives me great pleasure to introduce to you our moderator, Chris Skinner. Chris is known as an independent commentator on the financial markets and is the Chair of the European networking forum The Financial Services Club, and Chair of Nordic Finance Innovation.

We are very pleased that Chris is with us today, so without further ado – Chris, the floor is yours!