29 November 2018

Deputy Governor Rannveig Sigurðardóttir. Introductory remarks at the 2nd Annual Nordic Cyber in Finance Conference, Helsinki, 29 November 2018

Let me begin by saying that this conference is both timely and interesting for me, as I have only been in office for five months. Given that I come from the monetary policy department at the Central Bank of Iceland, cybersecurity has not been much on my agenda until now. It is, nonetheless, a very important topic. The Central Bank of Iceland, and other central banks are facing several new challenges in this area, both in the financial sector generally and central banking more specifically.

Last week I attended an interesting macroprudential policy conference at Danmarks Nationalbank. The discussion paper prepared for that conference was called *While the sun is shining, prepare for a rainy day*. Sitting there, I pondered what the discussion paper for this conference today might be called. Perhaps something like *The snowstorm is here – what do we wear?*

Cybercrime is now the world's fastest-growing type of crime. It has shot up to second place on the list of the top ten business risks worldwide, after not even making the list five years ago. The financial sector is particularly important because it greases the wheels of our economies, and cyber risks pose mounting threats to the financial system.

Developments since the emergence of the internet show that new technologies have brought with them new challenges. We only need to think of robotics, artificial intelligence, blockchains, and smart phones with 5G Wi-Fi to realize the extent of the changes that lie ahead for financial services.

New technologies also bring opportunities. The Austrian economist, Finance Minister, and banker Joseph Schumpeter demonstrated in the 1920s that successive waves of technological change raise productivity, income, and living standards. However, we know from long experience that technological change often results in costs involving new risks that must be addressed in order to optimise the net benefit. So while FinTech

will broaden consumers' range of choices in financial intermediation, it also brings new risks, both to the security of transactions and to privacy.

To maintain financial stability and real economic activity, we need payment and settlement systems that are secure. As a result, cybersecurity has moved from being a technical issue to a central bank issue. That is why the Nordic central banks have set up this forum for discussion and cooperation so as to foster closer cooperation on cyber resilience and cybersecurity. Today the focus is on financial market infrastructure.

One of the questions being asked in this section of the conference is, "What challenges are likely to emerge with new operating models and new actors in the financial sector?" As I said before, the FinTech snowstorm is already here. The newest challenge with respect to cybersecurity is the emergence of new players offering financial services, some of whom have not provided financial services before. The question therefore becomes: What technology are they using? Is it established, or is it new and unknown technology?

We also know that attitudes towards security and operational risk are important. But with tech firms rushing to offer new products to the market, there is the risk of insufficient emphasis on security. This is a risk that must be monitored – not only for new products or for new players, but also for incumbent businesses.

Tech giants like Google, Apple, and Alibaba look set to become dominant players. Their advantage comes from providing cross-border services and having already gathered significant information about users. They are already present in the Nordic marketplace. This development may lean towards monopolies, as it can create entry barriers for new and smaller players in the market. If that proves to be the case, it could have a negative impact on competition and go against the aims of the PSD2 (the recent EU Directive on payment services in the internal market (2015/2366). This risk is greater when the payment mechanisms are outside the jurisdiction of the relevant state.

Then there is the question of supervision. Will the new solutions be supervised, and if so, how? The challenge here is that many new solutions are global, and thus outside the European Economic Area or the European Single Market. Such supervision thus requires cross-border cooperation among supervisors.

The challenge for the supervisor is also to maintain a comprehensive overview of the market. For the legislator, it is a challenge to stay on top of rapid technological developments, as rules tend to lag behind technological changes. Financial market participants must commit fully to guarding the system. Cybersecurity needs to be promoted at all levels.

With respect to this fast-changing technology, keeping one step ahead of antisocial elements is a constant challenge. As I see it, cooperation is the only way forward. It is vital that all financial system entities work together on all fronts – within and between countries – to identify and address vulnerabilities. We need to share both our successes and our mishaps. We must do as mountain-climbers do – tie ourselves together

– because we are all in this together: central banks, financial service providers, FinTech firms, consumers, regulators, and politicians. And our success in combining forces will determine whether we reach the mountain peak or have to go back to base camp again.

All systems can break. This is why some of us still use paper banknotes, even though they are not the most sophisticated technology. But their security has been improved upon over recent centuries. Try imagining what would have been the main topic at a conference in Florence at the time of the first Medici's. As with paper money, the technologies we are discussing here today will become more secure, although we will encounter blizzards. Our role is to prevent or reduce the likelihood that those blizzards will create systemic risk.