Sabine Lautenschläger: Cyber resilience – objectives and tools

In 1903, the Italian inventor Marconi demonstrated his new invention, a wireless telegraph, to a large audience. It didn't go too well for him, though. The machine itself did work in the sense that it transmitted a message. However, it was not the message the audience – or Marconi – had expected. The word "rats" was being sent again and again. The system had been hacked. The culprit in this case was Nevil Maskelyne, a magician. Allegedly, he had been hired by a British wired-telegraph company which was worried that Marconi's invention might ruin its business.

Technology has advanced a lot since 1903. And it has created a deeply interconnected world. The financial system is a case in point. No financial institution can survive, let alone thrive, on its own. No bank can do without the complex web of financial market infrastructures that underpins its day-to-day business. No bank, therefore, must underestimate the associated risks. In particular, no bank must underestimate the IT risks, which include cyber risks. In the worst case, a single hack could compromise the entire system. So cyber resilience is a goal we all share. And anyone who sees it as just another competitive advantage is mistaken; the whole chain is only as strong as its weakest link. And in that sense, many actors in the financial system are parts of the same chain.

ECB Banking Supervision takes cyber resilience very seriously. Naturally, we focus on banks and on the euro area. In doing so, we take into account that banks are not just connected among themselves but also with other market participants and infrastructures. This means that our supervision of IT risks also covers the end-points of payment systems and market infrastructures in the banks directly supervised by us. In short, we aim to ensure the availability, confidentiality and integrity of banks' data and systems.

What have we done so far and what are our plans for the future?

- So far, we have conducted thematic reviews on cyber risk and outsourcing. One result is stating the obvious: there is some concentration in terms of companies to which banks outsource IT functions. Apart from concrete bank-specific findings, the reviews have helped us to get a better idea of the risks. And they have made banks more aware of them.
- We have conducted a stocktake on how IT risks are supervised outside the euro area. This helped us to identify best practices; and it will help us to define our own supervisory expectations. Work is ongoing as part of our contribution to the work programme of the European Banking Authority, the EBA.
- We have conducted quite a few on-site inspections into IT and cyber risks, using state-of-the-art methods. Looking ahead, our aim would be to have such inspections every three or four years for large banks.
- We have set up a reporting framework for cyber incidents. Since

mid-2017, banks have been required to report significant cyber incidents. This will help us to quickly react in a crisis and make us aware of common vulnerabilities.

Drawing on guidelines from the EBA, we have developed comprehensive IT risk self-assessments for the banks we supervise, including an extensive section on IT and cyber security. The results of these assessments will feed into our Supervisory Review and Evaluation Process, in which we will also challenge the information provided by banks. We will do so as a result of our insights from on-site inspections and from reports of cyber incidents. The information collected will then serve as a basis for a thematic review of IT risks. This review will give us a better idea of the overall IT risk landscape in the banking industry. It will allow us to identify blind spots early on and define areas which we need to investigate further; this will eventually feed into our plans for 2019. In addition, the review will also help us to compare banks. Partially anonymised feedback could then be shared with them.

Ladies and gentlemen, there is one thing we need to keep in mind. Right from the start, hacks gained a lot of attention, while preventing them did not. In finance, as in many other fields, it is mostly just mundane work that helps to keep things safe. I wonder whether cyber risk is as unique as we are inclined to believe. I have no doubt that we need to take it seriously and that we need to work towards making banks more resilient. In doing so, we should also welcome new ways of tackling cyber risk, of course. But this I would like to do within the existing framework of banks' risk management. Cyber risk needs to be part of general risk management procedures, of general crisis management, and general business continuity planning. After all, it is an operational risk. And our experience in dealing with operational risks can help us to cope with cyber risk as well.

We must keep in mind that cyber risk does not invariably arise from the technology itself but also from how we use it. It is people who are behind the hacking. And often, it is people who leave doors unlocked and gates wide open for cyber criminals to sneak in. People play a big role when it comes to cyber resilience. Thus, it makes sense to draw on the principles we have established for risk management and governance, and on the experience we have gained in these areas.

Ladies and gentlemen, I am aware that this kind of work is unlikely to capture the public's attention in the same way as Mr Maskelyne did in 1903. But it needs to be done. While cybercrime may have an aura of mystery and power, cyber resilience is quite the opposite: it calls for vigilance and diligence, day in, day out.

Thank you.

Benoît Cœuré: A Euro Cyber Resilience Board for pan-European Financial Infrastructures

Introductory remarks by Benoît Cœuré, Member of the Executive Board of the ECB, at the first meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures, Frankfurt, 9 March 2018

It is a pleasure to welcome you back to Frankfurt. Our last meeting was in June last year. Today, we will discuss the future course of the high-level cyber resilience forum for pan-European financial market infrastructures, critical service providers and competent authorities.

Establishment of the Euro Cyber Resilience Board for pan-European Financial Infrastructures

Recent technological advances have enabled cybercriminals to conduct ever more sophisticated, precise and powerful attacks. And nobody is immune to cyber risks, including businesses, financial infrastructures and public administrations. So we should avoid a "blame and shame" culture and work together.

The ECB and the Eurosystem are striving to lead by example. At the ECB, overseers, operators, supervisors and IT security services are working together more closely on cyber issues. Within the Eurosystem, there has been close collaboration on implementing the Eurosystem oversight cyber resilience strategy for financial market infrastructures that we presented at our last meeting, in line with CPMI-IOSCO's guidance on this topic.[1] The Market Infrastructure Board, which is in charge of Eurosystem financial market infrastructures, has also scaled up its activities to ensure the continued cyber resilience of its systems and platforms.

Eurosystem initiatives are part of a growing international effort to combat cyber threats. The CPMI-IOSCO guidance is being implemented. In October 2017, the Financial Stability Board (FSB) delivered a stocktake report of relevant regulations and supervisory practices to G20 finance ministers and governors, and G7 ministers and governors published the "Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector".[2] The FSB will produce a common lexicon of important terms, while the G7 Cyber Expert Group continues to work on third-party risks, cross-sector coordination and threat-led penetration testing, and will make proposals for G7 cross-border cyber crisis simulation exercises.

In this context, the Eurosystem aims at coordinating its own activities in

the field of cyber risks with that of market participants and other public authorities to succeed in protecting the financial system from cyber threats. I therefore invite you today to become part of the Euro Cyber Resilience Board (ECRB) for pan-European Financial Infrastructures – a regular forum where we can work together in a trusted environment.

The ECRB's objective is to enhance the cyber resilience of financial market infrastructures and their critical service providers, as well as that of the wider EU financial sector, in line with international standards. This will be achieved by fostering trust and collaboration and facilitating joint initiatives – whether among market players or between market players and authorities. The ECRB will thus contribute to the overall stability of the EU financial system.

The ECRB will have no formal powers to impose binding measures and will not make supervisory judgements. Its legitimacy will stem from the voluntary commitment of its members to abide by its common positions, statements and strategic views.

The ECRB will be chaired by the ECB, which will be closely involved together with national central banks and observers from the relevant European public authorities. This will ensure that the ECRB acts in the interest of Europe as a whole. Its common positions, statements and strategic views will be adopted by consensus.

To kick off the work of the ECRB, we would like to reflect with you on possible work items which we could address collectively. As part of this, we will also report on two of our most recent activities.

First, a cyber resilience survey, developed under the Eurosystem oversight cyber resilience strategy, was conducted across more than 75 payment systems, central securities depositories and central counterparties throughout Europe. As you will see, the survey highlighted a number of very pertinent issues for discussion, such as cyber governance, training and awareness, and cyber incident response.

Second, the Eurosystem is currently finalising the main elements of the European Threat Intelligence-Based Ethical Red-Teaming (TIBER-EU) Framework. This is an interesting concept which we hope will raise the level of cyber resilience in Europe and enable cross-border, cross-authority testing, which has not been done before.

We look forward to hearing your feedback on these two initiatives. We will also update you on the forthcoming market-wide exercise, which will explore the challenges of a specific cyber scenario and see how we can work closer together in times of crisis.

I am confident that we will have a fruitful discussion. I will now hand over to my colleague Sabine Lautenschläger, who will make some introductory remarks from the supervisory perspective.

After that, I would like to invite the European Commission representative to

briefly introduce the very recently published “FinTech Action plan”, which presents some interesting points to be considered with regard to the cyber resilience of the financial sector.

Thank you.

Council adopts conclusions on alternatives to coercive sanctions for drug using offenders

The Justice and Home Affairs Council has adopted today Council conclusions on alternatives to coercive sanctions for drug using offenders.

This agreement represents the political will of the 28 EU Member States to apply, in each legal system, alternative measures to coercive sanctions in order to: prevent crime; reduce recidivism; enhance the efficiency and effectiveness of the criminal justice system and look at reducing health-related harms and minimising social risks.

Alternative measures can include: education; suspension of investigation or prosecution; suspension of sentence with treatment; rehabilitation and recovery, aftercare and social reintegration.

This initiative, started under the Maltese Presidency in 2017, was promoted by the Estonian Presidency and concluded under the current Bulgarian Presidency of the Council. It responds to Action 22 of the EU Action Plan on Drugs 2017–2020 which requests Member States and working parties of the Council to provide and apply alternatives to coercive sanctions for drug using offenders (where appropriate, and in accordance with their legal frameworks). The Action Plan also requests concerned parties to increase monitoring, implementation and evaluation of alternatives to coercive sanctions.

This political agreement calls on the EU Member States to: implement effectively alternative measures and monitor and evaluate their implementation; develop and share best practice in the field; and raise awareness (e.g. through training among national policy makers, law enforcement, criminal justice, public health, social and education professionals and persons providing support to drug-using offenders).

The text: ‘Invites the EMCDDA to continue to monitor the measures and to exchange information and best practices on implementation, development of these measures, their effectiveness and cost-effectiveness’. It also: ‘Invites the European Commission ‘to support this work’.

Tackling terrorism: local leaders welcome EU plans to invest in cities to protect communities

The President of the European Committee of the Regions (CoR) has welcomed a European Union plan to provide funding to build urban defences against terrorist attacks, stressing the role of local authorities in both the prevention and fight against violent radicalisation. Speaking in Brussels, he said that strengthening public protection must go hand-in-hand with tackling social exclusion and warned that proposals to cut EU cohesion policy would therefore undermine these efforts.

President Lambertz was speaking during a conference, ' **Building urban defences against terrorism: lessons learned from recent attacks** ', that took place just 300 metres from the site of one of the terrorist attacks in Brussels on 22 March 2016, the Maalbeek metro station in the heart of the Belgian capital's EU quarter. The conference is one element of the EU's effort to put in place counter-terrorism measures, which includes an initiative to increase the protection of public spaces **launched at the end** of last year, led by **Julian King**, the European Commissioner for the Security Union.

Karl-Heinz Lambertz (BE/PES), the President of the EU's assembly of local and regional politicians, welcomed the decision by the European Commission to dedicate specific measures and EU funds for cities to increase protection of public spaces against terrorism. "Community safety is a priority and, by bringing together every level of government, the EU is taking the right steps to counter terrorism," he said. "We need to cooperate across borders, invest locally to promote social cohesion and ensure that our security services are ready to prevent future attacks. This work starts in our communities."

The fund for cities was promoted by the European Commission at the conference, which was co-organised with and hosted by the CoR. Commissioner King, **Dimitris Avramopoulos**, European Commissioner for Migration, Home Affairs and Citizenship, Corina Creţu, European Commissioner for Regional Policy, as well as French Interior Minister **Gérard Collomb** also took the floor.

President Lambertz said: "It is welcome that the EU is taking action by working together with our cities to protect our streets. Nevertheless, if we want to prevent future tragedies we need to tackle the root causes of radicalism: social exclusion and a lack of community integration. Cutting EU cohesion policy or diverting precious EU funds away from local authorities' pockets would be dangerous and counterproductive. Cohesion policy is not a cash cow, or a cow to be slaughtered to feed other objectives. It is about

investing in shared local problems that need European solutions."

Corina Creţu , the European Commissioner for Regional Policy, also addressed the conference. "There is far more to security than security measures," she said. "Security in our cities has a social dimension: access to quality basic services such as education and healthcare, urban regeneration, community empowerment. Also, I truly believe that solutions will be found by working together at all levels, local, national and European, by exchanging experience and good ideas, and by making our cities truly more inclusive in order to tackle extremism and violence before they take roots in our streets."

Bart Somers (BE/ALDE), Mayor of Mechelen, winner of the World Mayors Prize in 2017 for his work on social integration, and the CoR's rapporteur on **counter-radicalisation** efforts, said: "To counter radicalisation, our Committee advocates a strong line on respecting the rule of law. But local and regional governments also deeply believe in the importance of integration and of upholding fundamental European values. Extremists share a common trait – a sense of alienation. While many others who face social exclusion never become terrorists, they often express their alienation in other ways that harm society, such as rejecting shared values of democracy and the rule of law. A lack of integration is bad for society and potentially dangerous, which is why the EU must act together to invest in social infrastructure."

The CoR is currently drafting a response to the European Commission's action plan to reduce the vulnerability of public spaces. The CoR's rapporteur, **Jean-François Barnier** (FR/ALDE), mayor of Chambon-Feugerolles, said: "In its action plan, the European Commission recognises that we need cooperation between local, regional, national and European authorities to protect public spaces better. That is very welcome. The plan is an invitation to politicians and officials to learn from each other. I believe the plan will not just help reduce the number of terrorist attacks, but will also help to prevent radicalisation and promote more inclusive communities."

In a joint statement, the European Committee of the Regions and European Commission welcomed the initiative of EU local leaders to work together to share knowledge, increase cooperation and the improve security of their public spaces. The statement complements a declaration adopted in **Nice** in September 2017.

Speakers at the conference included the mayors of Nice,**Christian Estrosi**, and of Manchester, **Andrew Burnham**. Both cities have been the targets of major attacks in the past two years.

Notes to editors:

- The conference on 'Building urban defences against terrorism: lessons learned from recent attacks' was organised by the European Commission and hosted by the European Committee of the Regions. Over 100 local and regional politicians and municipal officials attended, with speakers from Barcelona, Berlin, London, Nice, Manchester, Marseille, and

Stockholm and – from the United States – New York.

- The European Committee of the Regions adopted proposals for counter-radicalisation efforts at the local and regional level in June 2016. The opinion – entitled ” **Combatting Radicalisation and Violent Extremism: Prevention mechanisms at local and regional level** ” – was drafted by Bart Somers (BE/ALDE). The CoR decided to present proposals two days after the terrorist attacks in Paris in November 2015.

- The CoR is currently drafting recommendations for an ” **Action Plan to support the protection of public spaces** ” drawn up by the European Commission. The opinion, whose rapporteur is Jean-François Barnier (FR/ALDE), will be adopted in July 2018.

Contact:

Andrew Gardner

Tel. +32 473 843 981

andrew.gardner@cor.europa.eu

Joint operation against drug trafficking in Finland and the Netherlands

The Hague, 8 March 2018

Since October 2017, Eurojust has been supporting the Finnish authorities in one of the largest investigations of drug trafficking in Finland, and especially in the region of Pirkanmaa, from which most of the Finnish suspects originate.

A larger organised crime group (OCG) established both in Finland and the Netherlands, which has been trafficking drugs, mainly amphetamine, in those countries, was dismantled by the Finnish and Dutch authorities. The estimated value of the drugs (approximately 50 kg) amounts to EUR 2.8 million.

Eurojust facilitated the simultaneous execution of European Investigation Orders and European Arrest Warrants and assisted in the development of coordinated strategies for the joint operations of the Finnish, Dutch, German and Swedish national authorities, which were facilitated through a coordination centre established at Eurojust. Without Eurojust’s intervention,

cross-border actions would have been very difficult to perform.

The German and Swedish national authorities supported the Finnish authorities' investigation and cooperated on the basis of mutual legal assistance requests. In the Netherlands, suspects were arrested and house searches were conducted by the International Legal Assistance Centre (IRC) of Limburg. During these actions, important evidence was obtained for the Finnish authorities. Through the close and active cooperation of the national authorities with Eurojust and Europol, 19 members of the OCG were detained in Finland. A total of 37 individuals (23 in Finland, 14 in the Netherlands) are suspected of five aggravated drug offences.

In addition to drug trafficking, the investigation focused on seven suspected money laundering offences related to the trafficking of drugs between Finland and the Netherlands.

The National Member for Finland at Eurojust, Piia Vottonen, stated: '*The active cooperation between Eurojust and the national authorities at the Eurojust coordination centre enabled the success in the case. Eurojust dealt with the judicial aspects within its competence, organised a coordination meeting to discuss the details of the case and set up a coordination centre to support the coordinated actions.*

Our core task at Eurojust is to assist judicial authorities in dealing with cross-border criminal cases. In this case, as in so many others, the Finnish authorities took on-the-spot investigative measures during the action day at the coordination centre, which provided the necessary judicial support to the investigation.'