Federal Chancellery

Austrian Presidency of the Council of the European Union

OESTERREICHISCHE NATIONALBANK EUROSYSTEM

Austrian EU-Presidency conference, 16 July 2018, NBB-Auditorium, Brussels

Finance 5.0 – a challenge for cyber security?

Digital transformation is fully under way. All business sectors, and specifically the financial sector, increasingly rely on digital infrastructures. The digital revolution changes the way people, companies and governments interact. Despite its many positive effects, it will also increase vulnerabilities. The number of cyberattacks has risen significantly and the economic damage caused by cybercrime increased by the factor five in the last five years.

The **financial sector** has been a **driver of technological innovation** (upscaling critical market infrastructures like payment systems, developing crypto currencies etc.) while being a frontrunner on **security standards.** Digital disruption affects banks' business models, regulatory and legal frameworks; it also renders the financial sector more vulnerable to cyber risks, thus impacting on economic and financial stability.

Building on the European Commission's Cyber Security Package (2017) and the Fintech Action Plan (2018), **Austria's EU Council Presidency** will concentrate on finalizing the Cybersecurity Act and on agreeing on cyber resilience measures in various sectors. With its conclusions, this conference aims at feeding into EU policy-making balancing innovation and regulation.

Cyber Technology – a challenge for regulation?

- What are the new technologies? Blockchains, algorithms, AI?
- Finance Industry 5.0: What are the challenges for critical market infrastructures and supervision?
- What are the regulatory challenges? Can/should new technologies be regulated – to which extent?

Cyber security – attacks increasingly threaten (financial) businesses and governments?

- How will the EU manage cyber-attacks, given their destabilizing potential for economy, financial systems, societies and democracies?
- How to deal with personal cyber hygiene, social engineering, the "Wild West" of algorithms?
- Distributed ledger technology (blockchains) as a panacea against cybercrime?
- Where are the fault lines between consumer rights, data security, and companies' interests?
- How to enhance cyber intelligence (incident reporting, information exchange) among stakeholders?

Cyber resilience and the financial sector – how to reach an EU policy balancing innovation and regulation?

- Can the EU together with its partners lead an international consensus on norms of cyber security and cyber resilience issues?
- How to strike a balance between the European and national levels regarding the competencies in the event of risk spill-overs, i.e. financial market stability?
- What are the acceptable cyber-risk levels for whom? Who should tackle cybersecurity and cyber resilience issues at which level?
- How to get a coordinated EU-wide emergency response plan (Crisis Emergency Response Teams)?

Target group: EU decision-makers, economic policy actors, business community stakeholders