EUROPEAN CENTRAL BANK

EUROSYSTEM

Wiebe Ruttenberg &
Emran Islam
DG Market Infrastructure & Payments

From Cyber Threats via Cyber Security to Cyber Resilience

AMISeCo meeting, 7 March 2017

Cyber threats are not new, but now they are much more harmful and harder to defend against

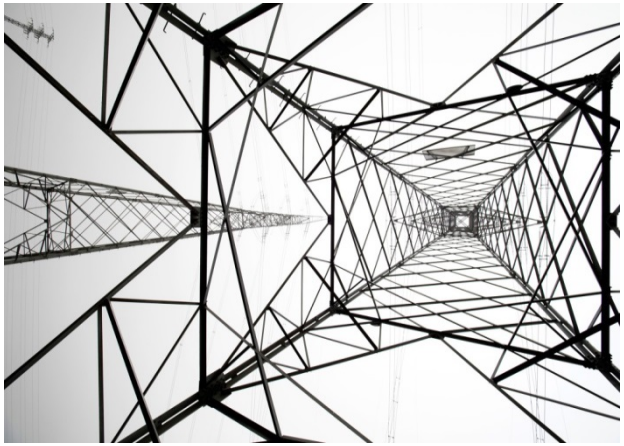
- **Advanced persistent threats**
  Persistent, stealthy, remotely controlled, reconnaissance capabilities
- **Destructive attacks**
  Data availability and data integrity at stake
- **Powerful actors** enter the scene
  States, state-backed initiatives, criminal syndicates, “crime as a service”

High-profile attacks with unprecedented sophistication and destructive impact have radically changed the nature of cyber threats

Stuxnet attack
2010

Tesco Cyber Heist
2016

Sony Entertainment Hack
2014



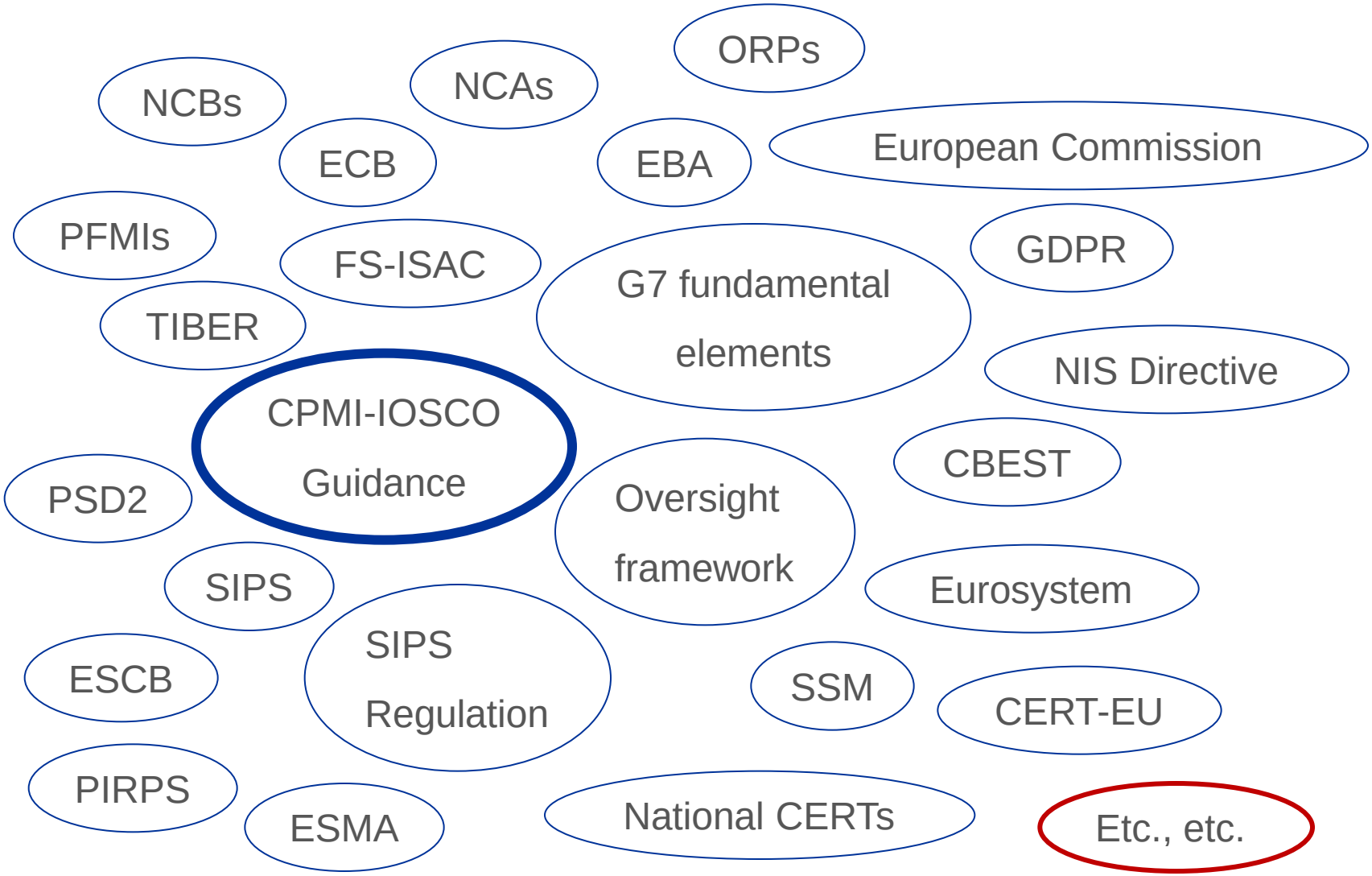
Ukranian electric grid hack
2015

Dutch, French & German elections…?
2017

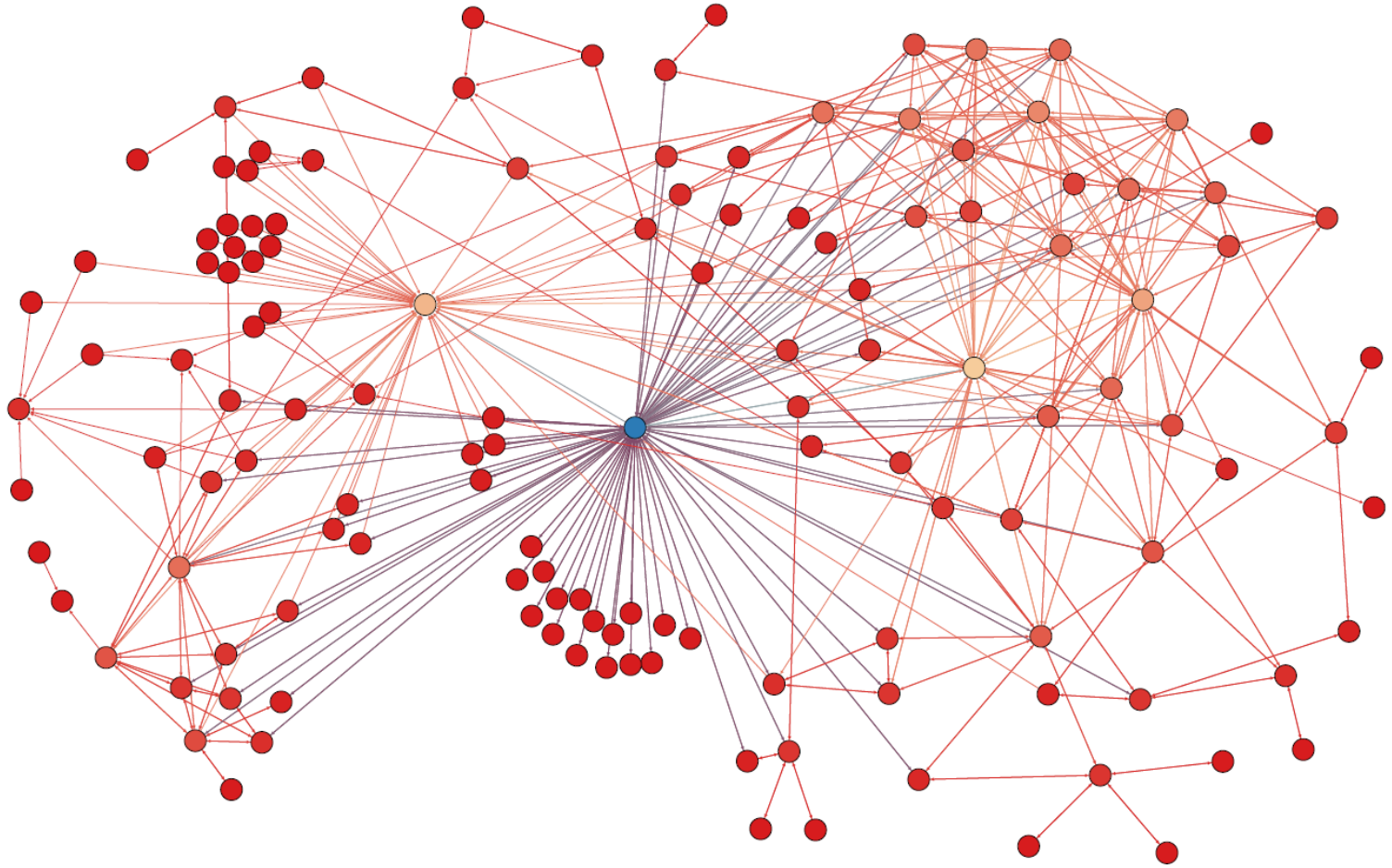
The nature of the emerging threats make conventional cyber security techniques increasingly inadequate

- **Traditional prevention techniques are insufficient**
  Blacklisting / whitelisting does not work any more: everything has to be verified
- **The network perimeter is dissolving**
  Mobility, remote access, cloud, extended enterprises etc.
- **IT security skills are scarce**
  Supply of skilled security professionals is far below the market demand
- **Security of the supply chain is a difficult problem**
  Both service and technology supply chains are hard to control and trust
- **The Internet of Things is bound to introduce unprecedented security hazards**
  Physical objects are becoming increasingly networked
  Security is low on the agenda of manufacturers

Legislation, Guidance, authorities and initiatives....

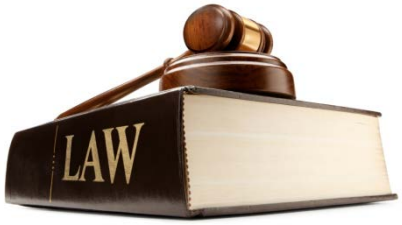


Cyber resilience of individual FMIs is key, but it is the resilience of the total financial ecosystem which needs to be ensured



Regulatory initiatives – next to regular supervision and oversight – are legislative and/or "guiding"

Legislative



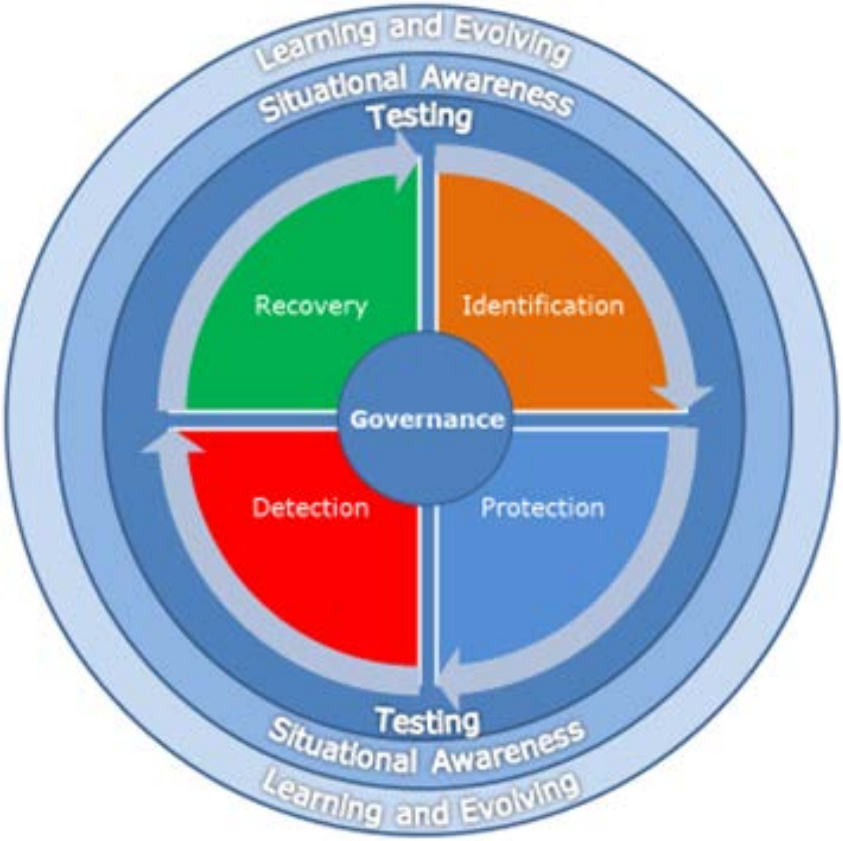
- **Payment Services Directive 2**: *mandatory access to payment accounts by 3rd parties!*
  Dir (EU) 2015/2366, Nov 2015
- **Network & Information System Security Directive**: *covers credit institutions, trading venues and CCPs, but not payment systems CSDs, trade repositories, etc.* Dir (EU) 2016/1148, July 2016
- **General Data Protection Regulation**: *rules to protect personal data / mandatory reporting of data breaches (fines up to EUR 10 million or 2% of the total worldwide annual turnover…)*
  Reg (EU) 2016/679, May 2016
- **Systemically Important Payment Systems Regulation:** *ensuring efficient risk management and sound governance for TARGET2, EURO1, STEP2-T and CORE(FR); being updated, public consultation closed* Reg ECB/2014/28

Regulatory initiatives – next to regular supervision and oversight – are legislative and/or "guiding"

Guidance

- **G7 Fundamental elements of Cyber Security for the Financial Sector**: *joint call by highest policy level to private entities and public authorities to address – individually and jointly – cyber security risks (Oct 2016)*
- **CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures**: *Governance, Identification, Protection, Detection, Response & Recovery (June 2016)*

Structure of the CPMI-IOSCO Guidance



5 risk management categories
3 overarching components

"FMIs should immediately take necessary steps (….) to improve their cyber resilience, taking into account this Guidance."
CPMI-IOSCO Guidance on Cyber Resilience for FMIs (June 2016)

"FMIs should also, within 12 months of the publication of this Guidance, have developed concrete plans to improve their capabilities in order to meet the two-hour RTO."
CPMI-IOSCO Guidance on Cyber Resilience for FMIs (June 2016)

Eurosystem in its oversight and catalyst role

Three strategic pillars

1. **FMI Readiness**
   Strategic objective: Overseers to work with FMIs to enhance their cyber resilience to ensure their safety and soundness.
2. **Sectoral Resilience**
   Strategic objective: Enhance collective cyber resilience capability of the financial sector, through cross-border / cross-authority collaboration, information sharing and exercises.
3. **Strategic Regulator – industry engagement** ("social" dialogue)
   Strategic objective: Establish trust and collaboration amongst participants, catalyse joint initiatives to enhance sector capabilities and capacities, and increase cyber awareness

The pillars – and underlying objectives and deliverables – are derived from the CPMI-IOSCO Guidance and interconnected!

- **Cyber resilience of financial ecosystem is a joint effort of institutions, infrastructures and regulators**
- **Banking supervisors and financial market infrastructure overseers will increasingly focus on ensuring cyber resilience, *but***
- **First responsibility is and stays with the financial institutions and infrastructures**