# Cyber Risk Management: systemic risk and risk governance

Carsten Liese

**HDI**

# Motivation

- Cyber risk managment based on DAV working group «Cyber als systemisches Risiko» with Nina Kilian, Leonie Ruderer, Mathias Raschke
- Management of cyber risk from a macroprudential perspective
  - Macroprudential : risk management that seeks to respond to system wide factors
- Concretely:
  - Review systemic cyber risk
  - Review suggested/existing macroprudential tools
  - Evaluate using risk governance framework
- Today: review some literature  systemic cyber risk and risk governance

# Systemic Cyber Risk

# Literature

- Malcom Kemp «Systemic risk»
- David Forscey et al «Systemic  cyber risk – a primer»
- ESRB «Systemic cyber risk»
- ECB Financial stability report Nov 22

# Systemic risk: Definition

- Systemic risk
  - «possibility that a single event or development might trigger widespread failures and negative effects spanning multiple organizations, sectors, or nations»
- No universally accepted definition of cyber systemic risk!
  - One problem: what is the relevant *system?* – depends on stakeholder
  - Good reasons for both, broad and narrow definitons
    - Any system typically exhibits fragilites (ecosystem etc) to build on existing research, definition should be broad
    - Not everyone agrees on what constitutes the financial system

# Systemic risk: Definition

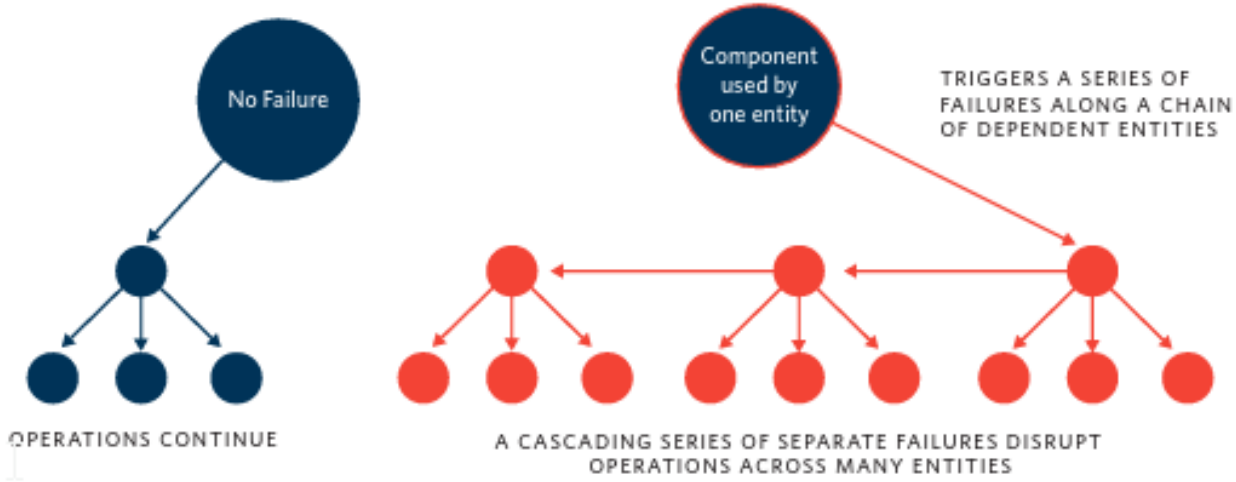
- **European Systemic Risk Board**: «disruption in the financial systems with the potential to have serious negative consequences for the (internal) market and the real economy»
- **Insurance Industry**: «Cyber risk is systemic if uninsurable» – due to scale of potential losses, correlations
- **Legal perspective:** «We know it when we see it» - however, identifying characteristics is crucial for deriving risk managment techniques.

As consequence, diverging interpretations about the relavance of systemic cyber risk

- Swiss Re Institue (2017) and EastWest Institute(2019): no previous cyber event systemic,no systemic cyber event according to ERSB(2020)
- Cyberhedge: Solar Winds systemic, also AIG(2017) systemic scenarios materialized subsequently

# Domino model of systemic risk

- **Domino model:** systemic risk often associated with propensity of financial system to suffer from interconnectedness («chain reaction»)
  - Problem affecting single component of system triggers chain reaction affecting ever-expanding range of entities
  - E.g., internet exchange point is taken down, disrupting operations of multiple organisations

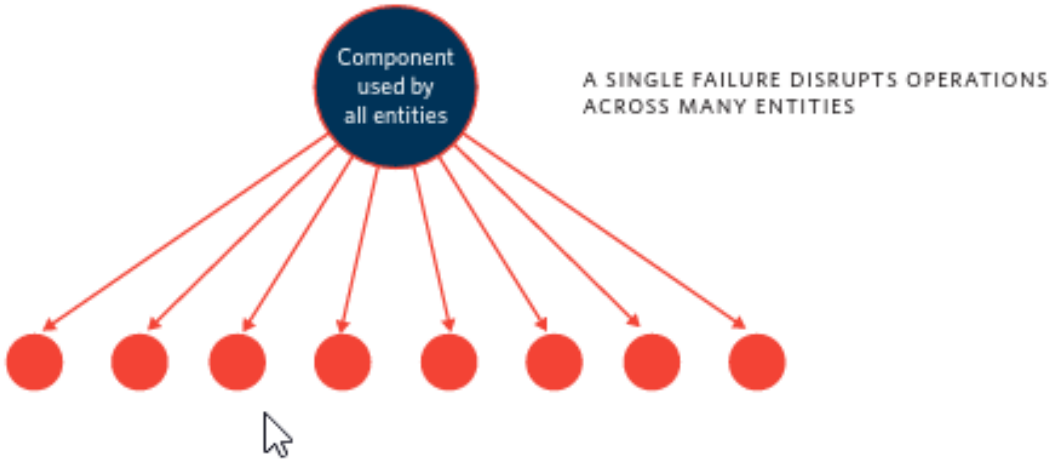


# Domino model: examples

- **Non-Cyber**
  - 2007-2008 Credit Crisis - loss of confidence led to failures
- **Cyber**
  - WannaCry and NotPetya (2017) exploited IT vulnerabilities, impact from interconnectedness
  - Lightning strike Azure data center in Texas triggered a cascading series of ailure in the region and beyond (2018).

# Tsunami model of systemic risk

- **Tsunami model:** modern regulatory thought permits other types of propagation.
  - In this model, entities in system share common exposures
  - E.g., malicious exploit allows attackers to disrupt operations for all users of a given software product



# Tsunami model: examples

- **Non-Cyber:**
  - US Savings and Loan crisis – failure of 1000 US savings and loans associations between 1986 – 1995: reduced regulation led to more risky strategies
- **Cyber:**
  - Nashville suicide bombing caused days-long regional outage of AT&T (2020).
  - Log4j (2021-) security flaw on millions of devices
  - Outage of Amazon(2017), Google(2018) and Microsoft(2019) Cloud services due to human error

# Systemic risk – Indirect Interconnectedness

*Combined model* (Kemp): in most circumstances should expect *both* – domino-like and tsunami-like features  effects to be present simultaneously.

**Model**

- Some often relatively opaque vulnerability to be present across a substantial part of the financial system; and
- Some firms have a level of interconnectedness with other parts of the financial system that is sufficiently high to lead to market reappraisals of plausible vulnerabilities of other firms if one or more of these interconnected firms run into difficulties

In this way, underwriting risks may also become systemic!

# Systemic cyber risk – What are its causes?

**Cyberspace: highly interconnected nature, standardized technologies naturally amplify systemic risk.**

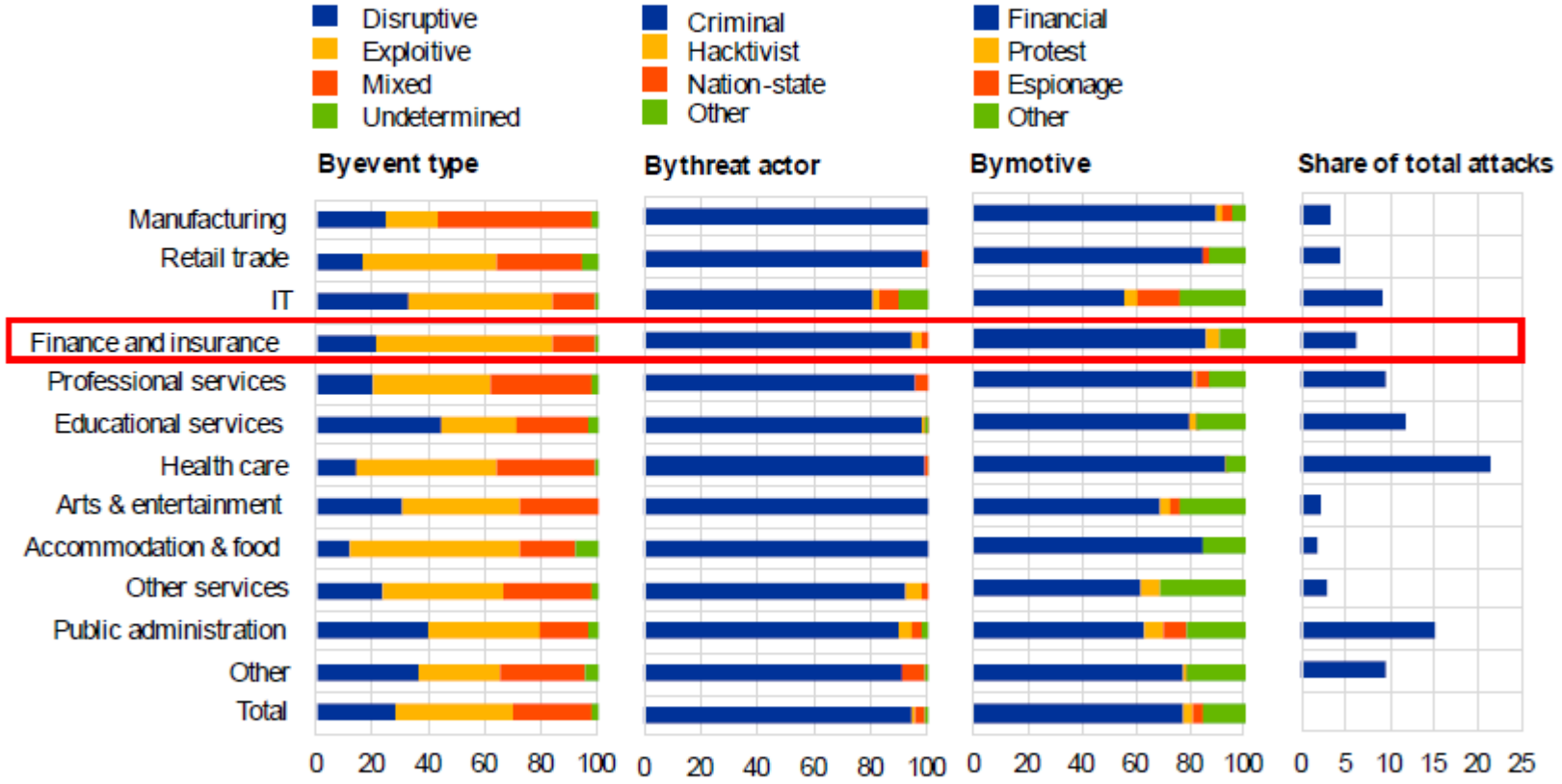
- Risk concentration
  - Consolidation around common technologies, software products, third-party providers creates **common vulnerabilites** and **single points of system failure**
- Complexity
  - Increasing complexity of computer networks ensures hidden levels of mutual dependence
- Opacity
  - Understanding systemic relationships requires specialized knowledge of and access to sensitive parts of privately owned technology systems.
- Scale
  - Many machines that ofte share identical, remotely exploitable vulnerabilities.
- Strategic threat actors
  - Threat actors act strategically and with purpose, which complicates the task of understanding and managing systemic risk.

# Systemic cyber risk – threat environment

## The characteristics of cyberattacks differ across economic sectors

**Breakdown of global cyberattacks by sector, event type, threat actor and motive**

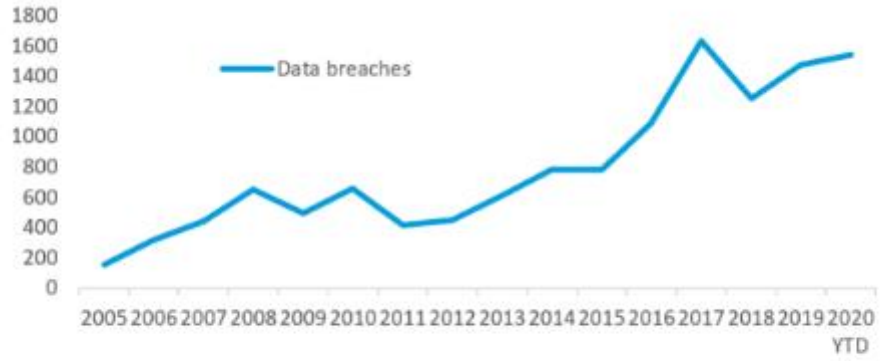
(2021, percentages)



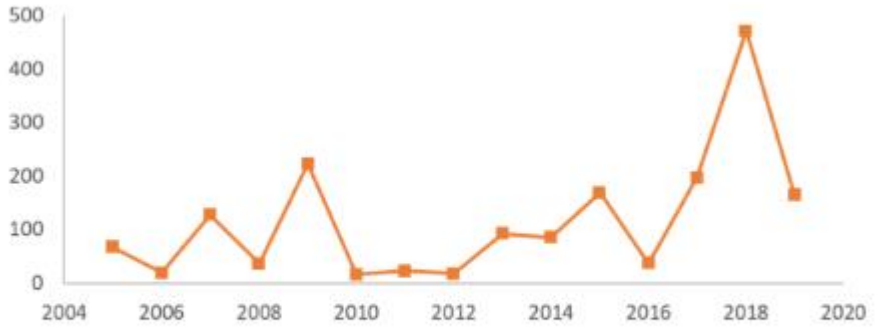

Sources: University of Maryland CISSM Cyber Attacks Database and ECB calculations.

- Public administration, health care and education are most frequently targeted economic sectors.
- Attacks on the financial sector are more moderate, accounting for around 5 to 10% of the total
- . On aggregate, most attacks are carried out by criminals, and this is also the case for the financial sector where more than 90% of cases involved criminals. Other actors who have primarily targeted the financial sector, IT and public administration, include hacktivists and nation-states.
- While financial motives – accounting for over 75% – are the dominant driver of attacks on the financial sector, protests also play a role

# Systemic cyber risk – threat environment




Source: Identity Theft Resource Center.




Source: Identity Theft Resource Center.

- Explosion in cyber attack incidents
- Attacks are exposing more data

# Systemic cyber risk - take aways

- Cyber risk has several characteristics that – in theory – amplify systemic risks from cyber incidents.
- A notable share of cyber incidents happens in sectors that appear to be relevant for systemic risk
- Numer of incidents and severity increasing over time
- ERSB shows that catastrophic systemic cyber events are also possible under plausible parametrizations but requires a severe shock, alignment of amplifiers and a lack of systemic mitigants.

# Risk Governance

# Risk Governance

- Merges two fields: risk analysis & governance
- Key characteristics:
  - Focus on process of risk characterization and evaluation as core of legitimate risk decision making
  - Focus on institutions and processes
  - Focus on «democratic foundations»
- «More comprehensive, adaptive and socially sensitive»
- Literature:
  - Klinke/Renn: «Risk governance and resilience»
  - Klinke Renn: «Coming of Age of Risk Governance»
  - Renn «Risk Governance – coping with an uncertain world»

# Risk knowledge

Risk governance should address the challenges raised by three risk characteristics that result from a lack of knowledge about the risk problem.

- **Complexity**
  - The difficulty of identifying and quantifying causal links between a multitude of candidates and special adverse effects, the complexity of the cause-and-effect relationship
- **Uncertainy**
  - Lack of knowledge about fundamental phenomena (epistemic uncertainty)
  - Other uncertainty, e.g. uncertainty from restricted models and limited amount of parameters
- **Ambiguity**
  - «Giving rise to several meaningful and legitimate interpretations of accepted assessment results»
  - Interpretative ambiguity: effects are adverse or not
  - Normative ambiguity: different concepts of what can be regarded tolerable

# Risk knowledge: Drug example (Renn 2008)

- Simple case is a drug that treats a serious disease effectively. Metabolic pathway well understood.
- Complexity is determined by the degree of complity of the assumed causal relationship. Age, health status, dietary factos might all play a promoting or inhibiting role in mediating the efficacy of the drug in treating the disease. So long as this network of effects is known, decison on use of drug can still be made, but may require more tests (increased *complexity*)
- If clinical trials for the drug were conducted predominantly in one population with a particular age, health and dietary profile and then the use of the drug is extended to another population which differs from the first population in critical ways there may be greater *uncertainty* of the amount of disease reduction and severerity of side effects. Similarly, there may be interactions with other lifestyle factors.
- If drug has serious side effects but is most affordable option for a serious disease in a new population, then health authorities and drug manufacturers may be reluctant to authorize the drug while individuals may be willing to risk the side effects (*normative ambiguity*).

# Risk knowledge – Cyber risk

Evaluating cyber risk

- **Complexity**
  - Dependence structure
- **Uncertainy**
  - Limited data, strategic threat actors
- **Ambiguity**
  - no unified view on what constitutes a systemic event

Cyber risk is a complex risk, with high uncertainty and (some) ambiguity!

# From risk characteristics to risk managment

- **Linear risk problems**
  - Routine based
    - Instruments include Risk-benefit analysis, technical standards, trial and error
- **Complexity-induced risk problems**
  - Risk-informed
    - Characterize the available evidence: Expert consensus, Scenario construction
  - Robustness-focused
    - Improving buffer capacity of risk target: inserting conservatism and safety factors, redundancy and diversity to improve structures against multiple stresses, improving organizational capacity to initiate, enforce and monitor risk managment actions

# From risk characteristics to risk managment

- **Uncertainty-induced risk problems**
  - Precaution-based
    - Close monitoring, small steps of impementation, avoiding irreversibility managment options for worst-case scenarios
  - Resilience-focused
    - Reduction of catastrophic potential, improvment of conditions for emergency managment and systemic adaption
- **Ambiguity-induced risk problems**
  - Discourse-based
    - Application of conflict-resolution for reaching consensus
    - Participary discourse with stakeholders

# Examples: cyber risk

Recommended and actual cyber risk measures can be subsumed under the sketched categories. E.g. the macroprudential toolkit ESRB:

- Developing capacity to analyse cyber risk
  - Scale and criticality
  - Network topology
- Monitoring for systemic risks
  - Collective vulnerabilities, e.g. inadequate cyber hygiene
- Sector-wide collective action
  - Cyber incident response
- Macroprudential tools
  - Cyber stress testing
  - Scenario setting