DAV/DGVFM
Herbsttagung
2023

Modeling and Pricing Cyber Insurance – Challenges and Perspectives

Stefan Weber

Leibniz Universität Hannover

www.insurance.uni-hannover.de

(joint work with K. Awiszus, M. Scherer, G. Svindland & A. Voß)

ASTIN & DGVFM: *Aus der Wissenschaft* – November 20, 2023

Motivation

- In the context of insurance, **cyber** is an umbrella term for all risks in the context of computer systems, hardware, software, data, the internet or other digital networks, any kind of Information Technology (IT) or Operational Technology (OT)
- While the number of connected devices was estimated at around 30 billion at the end of the last decade, around 125 billion such devices are expected by 2030
- Operational technologies, the Internet of Things, and also the spread of digital work within networks, e.g. in the home office, increase such risks
- The Allianz Risk Barometer 2022 ranks cyber risks as the top global business risk for 2022 (cited by 44% of respondents), ahead of business disruption (42%), natural disasters (25%), pandemics (22%) and legal and political risks (19%)[1]
- Estimated[2] annual damage caused by cyber risks worldwide increases with USD 445 billion in 2014, USD 600 billion in 2018, and USD 1000 billion in 2020
- MunichRe estimates global **insurance premiums** at USD 5 billion in 2018 with an increase to USD 20 billion in 2025, with 50% in the USA and 25% in Europe

[1] The 6th to 10th places are occupied by climate change, fire & explosions, market uncertainty, a shortage of skilled labour and macroeconomic developments.

[2] The above estimates are from the Center for Strategic & International Studies. Depending on the definition and methodology, there are diverging estimates. In some cases, amounts six times higher are given, with up to 10500 billion USD in 2025.

Leibniz Universität Hannover

Motivation

- In the context of insurance, **cyber** is an umbrella term for all risks in the context of computer systems, hardware, software, data, the internet or other digital networks, any kind of Information Technology (IT) or Operational Technology (OT)
- While the number of connected devices was estimated at around 30 billion at the end of the last decade, around 125 billion such devices are expected by 2030
- Operational technologies, the Internet of Things, and also the spread of digital work within networks, e.g. in the home office, increase such risks
- The Allianz Risk Barometer 2022 ranks cyber risks as the top global business risk for 2022 (cited by 44% of respondents), ahead of business disruption (42%), natural disasters (25%), pandemics (22%) and legal and political risks (19%)[1]
- Estimated[2] annual damage caused by cyber risks worldwide increases with USD 445 billion in 2014, USD 600 billion in 2018, and USD 1000 billion in 2020
- MunichRe estimates global **insurance premiums** at USD 5 billion in 2018 with an increase to USD 20 billion in 2025, with 50% in the USA and 25% in Europe

[1] The 6th to 10th places are occupied by climate change, fire & explosions, market uncertainty, a shortage of skilled labour and macroeconomic developments.

[2] The above estimates are from the Center for Strategic & International Studies. Depending on the definition and methodology, there are diverging estimates. In some cases, amounts six times higher are given, with up to 10500 billion USD in 2025.

Motivation

- In the context of insurance, **cyber** is an umbrella term for all risks in the context of computer systems, hardware, software, data, the internet or other digital networks, any kind of Information Technology (IT) or Operational Technology (OT)
- While the number of connected devices was estimated at around 30 billion at the end of the last decade, around 125 billion such devices are expected by 2030
- Operational technologies, the Internet of Things, and also the spread of digital work within networks, e.g. in the home office, increase such risks
- The Allianz Risk Barometer 2022 ranks cyber risks as the top global business risk for 2022 (cited by 44% of respondents), ahead of business disruption (42%), natural disasters (25%), pandemics (22%) and legal and political risks (19%)[1]
- Estimated[2] annual damage caused by cyber risks worldwide increases with USD 445 billion in 2014, USD 600 billion in 2018, and USD 1000 billion in 2020
- MunichRe estimates global **insurance premiums** at USD 5 billion in 2018 with an increase to USD 20 billion in 2025, with 50% in the USA and 25% in Europe

[1] The 6th to 10th places are occupied by climate change, fire & explosions, market uncertainty, a shortage of skilled labour and macroeconomic developments.

[2] The above estimates are from the Center for Strategic & International Studies. Depending on the definition and methodology, there are diverging estimates. In some cases, amounts six times higher are given, with up to 10500 billion USD in 2025.

Dimensions of Cyber Risk

1. **Risks**
   - Lost, stolen or corrupted data
   - Disruption of processes / operations / critical infrastructure
   - Physical damage, injury to people and fatalities
2. **Causes**
   - Human errors
   - Technical failures
   - Insider or hacker attacks
3. **Risk Management**
   - Protection of computers and networks
   - Contingency plans
   - Insurance of residual risks

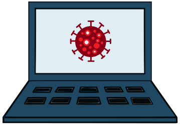
Dimensions of Cyber Risk

1. **Risks**
   - Lost, stolen or corrupted data
   - Disruption of processes / operations / critical infrastructure
   - Physical damage, injury to people and fatalities
2. **Causes**
   - Human errors
   - Technical failures
   - Insider or hacker attacks
3. **Risk Management**
   - Protection of computers and networks
   - Contingency plans
   - Insurance of residual risks

Dimensions of Cyber Risk

1. **Risks**
   - Lost, stolen or corrupted data
   - Disruption of processes / operations / critical infrastructure
   - Physical damage, injury to people and fatalities
2. **Causes**
   - Human errors
   - Technical failures
   - Insider or hacker attacks
3. **Risk Management**
   - Protection of computers and networks
   - Contingency plans
   - Insurance of residual risks

Cyber Insurance



Coverage is offered[3] in the following areas:

1. Loss or theft of data
2. Privacy breach protection
3. Cyber extortion
4. Property damage
5. (Contingent) business interruption
6. Product liability
7. Reputational damage
8. Loss of intellectual property

[3] Source: MunichRe, 2021

Outline

Outline

Actuarial Challenges of Cyber Risk

1. **Data**
   - Data are not yet available in the desired amount or granularity
2. **Non-Stationarity**
   - Technology and cyber threats are evolving fast and are constantly changing
3. **Dependence, Contagion in Networks & Externalities**
   - The classical insurance independence assumption does not hold. Moreover, there is no simple geographical distinction between dependent groups – as, for example, in the case of NatCat
   - In contrast, some forms of cyber risk are contagious and governed by complex interactions in networks
   - Individual investments in cyber security affect the cyber security of the system; for certain risks, these externalities might be substantial
4. **Information Asymmetries**
   - Insurers cannot fully observe investments in cyber security and risk levels
   - In particular, due to moral hazard of policy holders in combination with network externalities, cyber insurance might decrease the overall level of cyber security

Actuarial Challenges of Cyber Risk

1. **Data**
   - Data are not yet available in the desired amount or granularity
2. **Non-Stationarity**
   - Technology and cyber threats are evolving fast and are constantly changing
3. **Dependence, Contagion in Networks & Externalities**
   - The classical insurance independence assumption does not hold. Moreover, there is no simple geographical distinction between dependent groups – as, for example, in the case of NatCat
   - In contrast, some forms of cyber risk are contagious and governed by complex interactions in networks
   - Individual investments in cyber security affect the cyber security of the system; for certain risks, these externalities might be substantial
4. **Information Asymmetries**
   - Insurers cannot fully observe investments in cyber security and risk levels
   - In particular, due to moral hazard of policy holders in combination with network externalities, cyber insurance might decrease the overall level of cyber security

Leibniz Universität Hannover

Actuarial Challenges of Cyber Risk

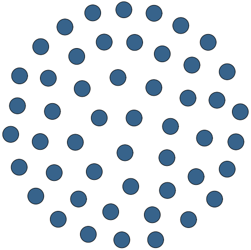
1. **Data**
   - Data are not yet available in the desired amount or granularity
2. **Non-Stationarity**
   - Technology and cyber threats are evolving fast and are constantly changing
3. **Dependence, Contagion in Networks & Externalities**
   - The classical insurance independence assumption does not hold. Moreover, there is no simple geographical distinction between dependent groups – as, for example, in the case of NatCat
   - In contrast, some forms of cyber risk are contagious and governed by complex interactions in networks
   - Individual investments in cyber security affect the cyber security of the system; for certain risks, these externalities might be substantial
4. **Information Asymmetries**
   - Insurers cannot fully observe investments in cyber security and risk levels
   - In particular, due to moral hazard of policy holders in combination with network externalities, cyber insurance might decrease the overall level of cyber security

Actuarial Challenges of Cyber Risk

1. **Data**
   - Data are not yet available in the desired amount or granularity
2. **Non-Stationarity**
   - Technology and cyber threats are evolving fast and are constantly changing
3. **Dependence, Contagion in Networks & Externalities**
   - The classical insurance independence assumption does not hold. Moreover, there is no simple geographical distinction between dependent groups – as, for example, in the case of NatCat
   - In contrast, some forms of cyber risk are contagious and governed by complex interactions in networks
   - Individual investments in cyber security affect the cyber security of the system; for certain risks, these externalities might be substantial
4. **Information Asymmetries**
   - Insurers cannot fully observe investments in cyber security and risk levels
   - In particular, due to moral hazard of policy holders in combination with network externalities, cyber insurance might decrease the overall level of cyber security

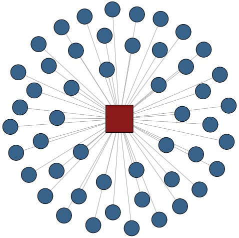
Types of Cyber Risk

The suitability of a modeling approach depends on the type of cyber risk



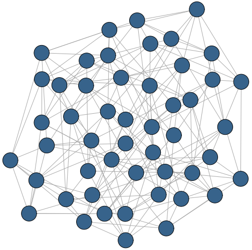
idiosyncratic

(individual risks,
e.g., targeted hacker attacks, errors,
distortions)



systematic

(common risk factor,
e.g., attacks on widely used software or
hardware)



systemic

(propagation risks,
e.g., viruses, worms,
Trojans)

Selected Approaches

1. **Frequency-Severity-Models**
   - Characteristics
     1. Conditional on risk factors, frequency-severity models can also be applied in the area of cyber risks; however, usually not enough data are available
     2. Suitable for idiosyncratic and systematic risks, but not for systemic risks without further modifications

     ★ Zeller, G., Scherer, M. (2022): A comprehensive model for cyber risk based on marked point processes and its application to insurance, *European Actuarial Journal*, 12(1), 33-85

2. **Information Asymmetries**
   - Core topics
     1. Strategies to reduce information asymmetries, for example, by optimizing offerings and contract design (menu of contracts, cyber assistance)
     2. Regulation to strengthen physical cybersecurity in the face of network externalities (see also below)

     ★ A. Marotta et al. (2017): Cyber-insurance survey, *Computer Science Review*, 24, 35-61

Selected Approaches

1. **Frequency-Severity-Models**
   - Characteristics
     1. Conditional on risk factors, frequency-severity models can also be applied in the area of cyber risks; however, usually not enough data are available
     2. Suitable for idiosyncratic and systematic risks, but not for systemic risks without further modifications

     ★ Zeller, G., Scherer, M. (2022): A comprehensive model for cyber risk based on marked point processes and its application to insurance, *European Actuarial Journal*, 12(1), 33-85

2. **Information Asymmetries**
   - Core topics
     1. Strategies to reduce information asymmetries, for example, by optimizing offerings and contract design (menu of contracts, cyber assistance)
     2. Regulation to strengthen physical cybersecurity in the face of network externalities (see also below)

     ★ A. Marotta et al. (2017): Cyber-insurance survey, *Computer Science Review*, 24, 35-61

Selected Approaches (2)

3. **Systemic Cyber Risks**
   - Local interaction
     - M. Fahrenwaldt, S. Weber & K. Weske (2018): Pricing of Cyber Insurance Contracts in a Network Model, *ASTIN Bulletin*, 48(3), 1175-1218
     - K. Awiszus, Y. Bell, J. Lüttringhaus, G. Svindland, A. Voß & S. Weber (2023): Building Resilience in Cybersecurity – An Artificial Lab Approach. To appear in: *Journal of Risk and Insurance*
   - Feedback in point processes
     - Y. Bessy-Roland, A. Boumezoued & C. Hillairet (2020): Multivariate Hawkes process for cyber insurance, *Annals of Actuarial Science*, 15(1), 1-26
     - C. Hillairet, A. Reveillac & M. Rosenbaum (2023): An expansion formula for Hawkes processes and application to cyber-insurance derivatives, *Stochastic Processes and their Applications*, 160, 89-119
   - Interaction on a macroscopic level
     - C. Hillairet & O. Lopez (2021): Propagation of cyber incidents in an insurance portfolio: counting processes combined with compartmental epidemiological models, *Scandinavian Actuarial Journal*, 8, 671-694

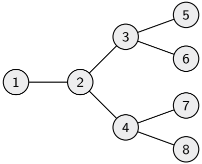
Selected Approaches (2)

3. **Systemic Cyber Risks**
   - Local interaction
     - M. Fahrenwaldt, S. Weber & K. Weske (2018): Pricing of Cyber Insurance Contracts in a Network Model, *ASTIN Bulletin*, 48(3), 1175-1218
     - K. Awiszus, Y. Bell, J. Lüttringhaus, G. Svindland, A. Voß & S. Weber (2023): Building Resilience in Cybersecurity – An Artificial Lab Approach. To appear in: *Journal of Risk and Insurance*
   - Feedback in point processes
     - Y. Bessy-Roland, A. Boumezoued & C. Hillairet (2020): Multivariate Hawkes process for cyber insurance, *Annals of Actuarial Science*, 15(1), 1-26
     - C. Hillairet, A. Reveillac & M. Rosenbaum (2023): An expansion formula for Hawkes processes and application to cyber-insurance derivatives, *Stochastic Processes and their Applications*, 160, 89-119
   - Interaction on a macroscopic level
     - C. Hillairet & O. Lopez (2021): Propagation of cyber incidents in an insurance portfolio: counting processes combined with compartmental epidemiological models, *Scandinavian Actuarial Journal*, 8, 671-694

Outline

The Role of the Network

- Systemic cyber risk is significantly influenced by the underlying network; important "covariate"
- Examples include cryptoworms like WannaCry
- We take a closer look at the role of security investments in cyber networks and modifications of the network
- Welfare-optimal actions are often not achieved by the rational behavior of individual agents in the presence of externalities
- **Regulatory requirements** or **requirements in insurance contracts** may trigger additional security investments; in our paper, we evaluate and compare — in cooperation with legal experts (Y. Bell, J. Lüttringhaus) — cyber lab case studies to current insurance practice and regulation
- Suitable centrality measures for entities in networks evaluated by questionnaires can also enter insurance pricing



$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

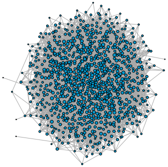
Random Network Models

Random Graphs
Erdős-Rényi Model, 1959

N nodes in which each of the possible $N(N-1)/2$ edges is independently present with the same probability p
$\rightarrow$ Binomial distribution of node degrees K, approximately Poisson for large N in the limit of fixed average degree $(N-1)p \approx Np =: \mathbb{E}[K]$:

$$P(K=k) = e^{-\mathbb{E}[K]} \frac{\mathbb{E}[K]^k}{k!}$$

$\rightarrow$ homogeneous topology with nodes of comparable degrees

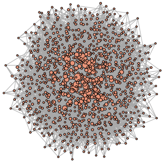


Scale-Free Networks
Barabási-Albert Model, 1999

Modelling growing networks under preferential attachment (world wide web, IT networks, social and biological networks)
$\rightarrow$ Distribution of node degrees K follows a power-law:

$$\mathbb{P}(K=k) \sim k^{-\lambda}, \qquad \lambda \in \mathbb{R}_+$$

Special case $\lambda = 3$ can be modeled using the Barabási-Albert model
$\rightarrow$ heterogeneous topology with few nodes of high degree (called **hubs**), and a vast majority of less connected nodes



Network Contagion: SIS and SIR Model

For a network of N nodes, the spread process at time t can be described by a *state vector*

$$X(t) = (X_1(t), \ldots, X_N(t)) \in E^N$$

- **Node states**: at each point in time, individuals are either *susceptible* (S) to an infection, *infected* (I), or have *recovered* (R)
  $\rightarrow$ **SIS Model**: $E = \{S, I\}$, **SIR Model**: $E = \{S, I, R\}$
- Models differ in terms of immunity: multiple infections for the same node possible for SIS, ruled out in case of SIR
- Markov process with the following rates for infection and recovery of single nodes i:

$$X_i : S \rightarrow I \quad \text{with rate} \quad \tau \sum_{j=1}^{N} a_{ij} \mathbb{1}_{\{X_j(t)=I\}}$$

$$X_i : I \rightarrow Z \quad \text{with rate} \quad \gamma_i,$$

where $Z = S$, for the SIS, and $Z = R$ for the SIR model, respectively

$\rightarrow$ **Modeling parameters:** infection rate τ, recovery rates γ_i

(a) SIS Model **(b) SIR Model**

Security Investments and Strategic Interactions

- We study the interplay of security investment decisions of network agents and the overall systemic risk exposure
  $\rightarrow$ Individual recovery rate γ_i is interpreted as security level of node i
- **Investment decision of network agent** i based on total expenses of node i:

$$\mathcal{E}_i(\gamma_1, \dots, \gamma_N) = C_i(\gamma_i) + L_i(\gamma_1, \dots, \gamma_N)$$

  - $C_i(\gamma_i)$ is the cost of implementing security level $\gamma_i \rightarrow$ choice: $C_i(x) = \exp(kx) - 1$, $x \in (0, \infty)$, $k > 0$ const
  - $L_i(\gamma_1, \dots, \gamma_N) = \mathbb{E}[\int_0^\infty I_i(t)\, dt]$ expected amount of time node i will be infected $\rightarrow$ interdependence

γ_i is individually optimal for node i, if it minimizes the total expenses $\mathcal{E}_i$:

$$\gamma_i^{\text{ind}}(\gamma_{-i}) := \underset{\gamma_i \in [0,\infty)}{\operatorname{argmin}} \ \mathcal{E}_i(\gamma_1, \dots, \gamma_N) \qquad \gamma_{-i} := (\gamma_1, \dots, \gamma_{i-1}, \gamma_{i+1}, \dots, \gamma_N)$$

- A steady state *(Nash equilibrium)* of individually optimal security levels is a choice of security levels $\gamma \in (0, \infty)^N$ such that

$$\forall i = 1, \dots, N: \quad \gamma_i^{\text{ind}}(\gamma_{-i}) = \gamma_i$$

Steady states of individually optimal security levels exist

Security Investments and Strategic Interactions

- We study the interplay of security investment decisions of network agents and the overall systemic risk exposure
  $\rightarrow$ Individual recovery rate γ_i is interpreted as security level of node i
- **Investment decision of network agent** i based on total expenses of node i:

$$\mathcal{E}_i(\gamma_1, \ldots, \gamma_N) = C_i(\gamma_i) + L_i(\gamma_1, \ldots, \gamma_N)$$

  - $C_i(\gamma_i)$ is the cost of implementing security level γ_i $\rightarrow$ choice: $C_i(x) = \exp(kx) - 1$, $x \in (0, \infty)$, $k > 0$ const
  - $L_i(\gamma_1, \ldots, \gamma_N) = \mathbb{E}[\int_0^\infty I_i(t)\, dt]$ expected amount of time node i will be infected $\rightarrow$ interdependence

  γ_i is individually optimal for node i, if it minimizes the total expenses $\mathcal{E}_i$:

$$\gamma_i^{\text{ind}}(\gamma_{-i}) := \underset{\gamma_i \in [0,\infty)}{\text{argmin}}\ \mathcal{E}_i(\gamma_1, \ldots, \gamma_N) \qquad \gamma_{-i} := (\gamma_1, \ldots, \gamma_{i-1}, \gamma_{i+1}, \ldots, \gamma_N)$$

- A steady state *(Nash equilibrium)* of individually optimal security levels is a choice of security levels $\gamma \in (0, \infty)^N$ such that

$$\forall i = 1, \ldots, N: \quad \gamma_i^{\text{ind}}(\gamma_{-i}) = \gamma_i$$

  Steady states of individually optimal security levels exist

Security Investments and Strategic Interactions

- We study the interplay of security investment decisions of network agents and the overall systemic risk exposure
  $\rightarrow$ Individual recovery rate γ_i is interpreted as security level of node i
- **Investment decision of network agent** i based on total expenses of node i:

$$\mathcal{E}_i(\gamma_1, \ldots, \gamma_N) = C_i(\gamma_i) + L_i(\gamma_1, \ldots, \gamma_N)$$

  - $C_i(\gamma_i)$ is the cost of implementing security level $\gamma_i \rightarrow$ choice: $C_i(x) = \exp(kx) - 1$, $x \in (0, \infty)$, $k > 0$ const
  - $L_i(\gamma_1, \ldots, \gamma_N) = \mathbb{E}[\int_0^\infty I_i(t)\, dt]$ expected amount of time node i will be infected $\rightarrow$ interdependence

  γ_i is individually optimal for node i, if it minimizes the total expenses $\mathcal{E}_i$:

$$\gamma_i^{\text{ind}}(\gamma_{-i}) := \underset{\gamma_i \in [0,\infty)}{\operatorname{argmin}} \ \mathcal{E}_i(\gamma_1, \ldots, \gamma_N) \qquad \gamma_{-i} := (\gamma_1, \ldots, \gamma_{i-1}, \gamma_{i+1}, \ldots, \gamma_N)$$

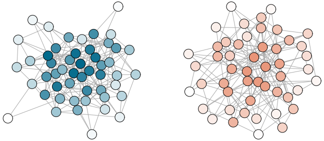
- A steady state *(Nash equilibrium)* of individually optimal security levels is a choice of security levels $\gamma \in (0, \infty)^N$ such that

$$\forall i = 1, \ldots, N: \quad \gamma_i^{\text{ind}}(\gamma_{-i}) = \gamma_i$$

  Steady states of individually optimal security levels exist

Leibniz Universität Hannover

Public and Private Regulation



Visualization of steady states for exemplary networks drawn from the Erdős-Rényi (left) and Barabási-Albert (right) classes. Nodes are colored according to their chosen level of security after round 50 of the security investment game: the darker the color, the higher the chosen security level (*for Erdős-Rényi*: minimum: 0.3780, maximum: 0.6526; *for Barabási-Albert*: minimum: 0.4719, maximum: 0.7598).

- A Nash equilibrium is not necessarily Pareto optimal
- System perspective: total network expenses given by

$$\mathcal{E}(\gamma_1,\dots,\gamma_N) = \sum_{i=1}^N \mathcal{E}_i(\gamma_1,\dots,\gamma_N) = \underbrace{\sum_{i=1}^N C_i(\gamma_i)}_{\text{total cost of sec.}} + \underbrace{\sum_{i=1}^N L_i(\gamma_1,\dots,\gamma_N)}_{\text{total exp. infection time}}$$

- **Question**: Given a steady state of individually optimal security levels, is it possible to reduce the total expenses by increasing the total security investments $\sum_{i=1}^N C_i(\gamma_i)$, and thus in particular the total expected infection time?
- Answer: In the considered case, yes!

Allocation of Additional Security

- **Idea**: Given a steady state $(\gamma_1^{stead}, \dots, \gamma_N^{stead})$ of individually optimal security levels, distribute additional security $\beta > 0$ among the nodes
- Untargeted allocation new security levels $\gamma_i^{stead} + \beta/N$
- Targeted allocation: importance of node i corresponds to centrality of node i, e.g.,
  - Degree centrality: Nodes are ranked by the number $\mathcal{C}^{\text{deg}}(i)$ of neighbors
  - Betweenness centrality: Node as "bridge" between different network regions:

$$\mathcal{C}^{\text{bet}}(i) = \sum_{j,h} \frac{\sigma_{jh}(i)}{\sigma_{jh}}, \qquad i = 1, \dots, N,$$

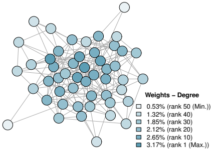
  where σ_{jh} denotes the total number of shortest paths between nodes j and h, and $\sigma_{jh}(i)$ is the cardinality of the subset of those paths that go through node i

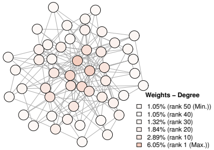
Choose a centrality measure $\mathcal{C}$ and determine the allocation weights

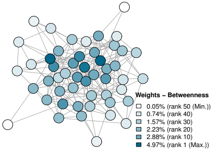
$$w_i := \frac{\mathcal{C}(i)}{\sum_{j=1}^{N} \mathcal{C}(j)}, \qquad i = 1, \dots, N$$

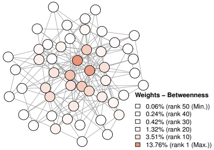
Budget β is allocated proportionally to the centrality, i.e., $\gamma_i^{\text{all}} := \beta \cdot w_i$

Allocation of Additional Security (2)









c^{deg}	c^{bet}	untargeted
10.6% 11.3%	10.8% 12.3%	9.9% 9.0%

Percental reduction of accumulated total expenses $\mathcal{E}$ after the allocation of the additional budget $\beta = 5$ among all network nodes. Erdős-Rényi network is colored in blue, Barabási-Albert network in red.

Cyber Pandemic Risk in Large-Scale Systems

- In large-scale networks, the frequency distribution of epidemic outbreak sizes in the SIR model can typically be characterized by the presence of two peaks (see, e.g., Kiss et al. (2017): *Mathematics of Epidemics on Networks*):
  - small outbreaks, affecting only a very small fraction of network nodes, and
  - epidemic outbreaks or pandemics, where a large number of nodes becomes infected
- The network topology has a major effect on the occurrence of pandemic outbreaks

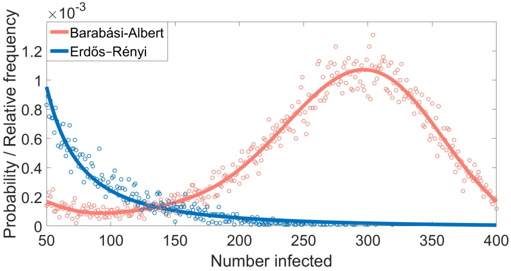


Figure: Final outbreak size frequencies given an infection of a single network node for Barabási-Albert and Erdős-Rényi networks with $N = 1,000$ and other parameters such that a similar number of total edges is generated.
Epidemic parameters are chosen as $\tau = 0.1$ for the infection rate, and $\gamma_i = 1$ for all recovery rates.

Topological Interventions and Network Functionality

- **Topological Interventions**
  - edge removal
    - *physical deletion of certain connections*, or if not possible,
    - *edge hardening*, which corresponds to strong protection of network connections via firewalls, the closing of open ports, or the monitoring of data flows using specific detection systems
  - node splitting to separate critical contagion channels replacing them by multiple nodes with the same operational task

  $\rightarrow$ Topological interventions affect both the risk exposure and the functionality of the network

- **Network Functionality** could be measured by the average shortest path length:

$$\langle l \rangle = \sum_{i \neq j} \frac{1}{N(N-1)} l_{ij}$$

where l_{ij} is the minimum number of edges connecting i and j $\rightarrow$ small $\langle l \rangle$ corresponds to fast and efficient data flow

Leibniz Universität Hannover

Effect of Edge Removal

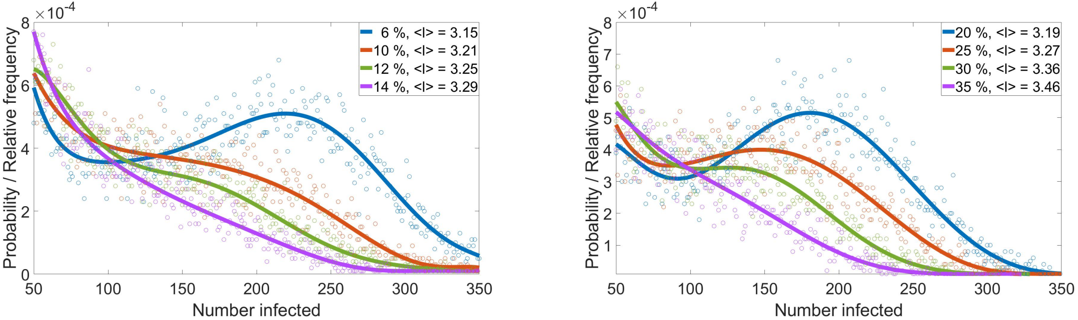
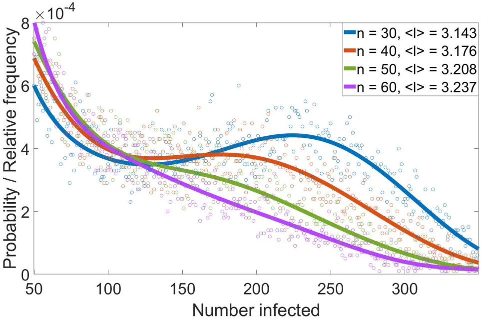
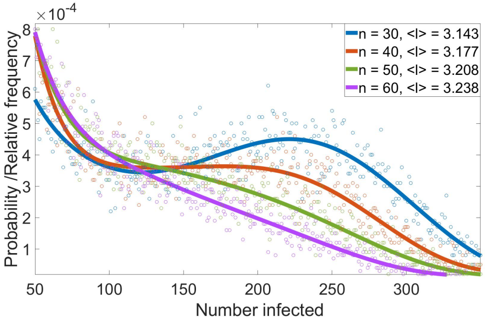


Figure: Final outbreak size frequencies given an initial infection of a single node in a Barabási-Albert network with $N = 1,000$, over 100,000 simulations for different percentages of deleted edges. The results for **edge centrality-based** removals are depicted in the **left figure**, and the percentage of critical links is found to be about 14%. In contrast, **random edge removals** are shown in the **right figure**, and this procedure is clearly less effective: Approximately 30-35% of edges need to be removed here to eliminate the risk of cyber pandemics. The initial $< l >$ was 2.95.

Effect of Node Splitting



degree-based



betweenness-based

Figure: Final outbreak size frequencies given an initial infection of a single network node in the previously considered Barabási-Albert network, over 100,000 simulations for different numbers of splitted nodes. For degree-based splittings, the number of critical splits is found to be about $n = 60$ which corresponds to 6% of the nodes. Similar results in case of betweenness centrality based splits. The initial $< l >$ was 2.95.

Lessons Learnt from the Toy Examples

- Cyber security and resilience is significantly influenced by contagious transmission channels in digital networks
- Substantial externalities are observable in cyber network toy models
- Besides governments, also insurance companies might act as private regulators
- Centrality measures are important covariates for cyber pricing
- Qualitative implications are:
  - Cybersecurity measures can mitigate cyber losses:
    - GOV: size-cap rule (in good agreement with EU-NIS2), supply chain protection (beyond most central entities)
    - INS: assistance services (identification when important, effective resource allocation), patch management and backup (centrality captures when to invest more than individually rational amount)
  - Topological cyber resilience measures can reduce the risk of contagious scenarios:
    - GOV: incident response and reporting (focus on central entities, early warning systems), critical supply chains (risk of contagion, improving resilience)
    - INS: contact liability premiums, insurance backstop mechanism (incentives for more resilient network structures)

Outline

Research Challenges and Perspectives for Cyber Insurance

Challenges in Cyber Risk and Cyber Insurance:

Models, Methods, and Data

Matthias Scherer[1] and Stefan Weber[2]

Report for ENISA, September 2022

Final Version, October 4, 2022

Abstract: This report offers an introduction to cyber risk and cyber insurance. It provides an overview of the cyber insurance industry's functions and discusses challenges and implications. An in-depth perspective on available data, modeling approaches, and statistical methods is presented, including machine learning and artificial intelligence. Finally, a list of important research questions, to be explored in the future, is given.

Keywords:
Cyber insurance; cyber risk; cyber security; machine learning; artificial intelligence; systemic risk

[1] Technical University of Munich, Parkring 11, 85748 Garching-Hochbrück, Germany, scherer@tum.de
[2] House of Insurance, Leibniz Universität Hannover, Welfengarten 1, 30167 Hannover, Germany, stefan.weber@insurance.uni-hannover.de

The following research opportunities are detailed in Chapter 8 of the ENISA report mentioned above

Research Challenges and Perspectives for Cyber Insurance

1. Improving the process of cyber risk assessment
2. Identifying relevant covariates
3. Modeling & estimating loss frequency & severity
4. Modeling of systemic risk in network models
5. Modeling dynamic strategic interaction
6. Understanding multilayer networks
7. Pricing idiosyncratic, systematic, & systemic risk
8. Data for systemic cyber risk
9. Adapting existing ML methods to the specific stylized facts of cyber
10. Estimation of models for cyber risk (e.g. combining statistical estimation and expert opinion)
11. Cyber assistance
12. Hedging accumulation risks
13. Cyber risk as an asset class
14. Closing the cyber-insurance gap
15. Optimal contract design
16. Behavioral challenges
17. Cyber insurance for private customer segment
18. Resilience of systems
19. Robustness of models
20. Data collection
21. Welfare and regulatory implications
22. Explainable AI for cyber risk
23. Vision: Autonomous cyber risk management

Selected Challenges

Data

- To date, only limited amounts of data are accessible for research, and their quality also has to be enhanced
- We advocate government incentives and regulatory interventions to enable a database that can allow Europe to be competitive in cybersecurity

Models

- Innovative models need to be developed – both pragmatic models that can be used as proxies in practice and models that capture the main classes of cyber risk, idiosyncratic, systematic and systemic risks

Insurance products and markets

- Coupling cyber insurance with cyber assistance and optimal contract design are important topics, as are strategies to close the cyber insurance gap
- How to design standardised cyber insurance for private customers is an open question

Societal and regulatory implications

- The impact on welfare needs to be explored in more detail
- Guided by research results, governmental actors should select the guardrails in a manner that strengthens both the functionality and security of cyber networks and establish resilient structures; insurance companies can in addition function as private regulators

Leibniz Universität Hannover

References

This qualitative cyber network analysis is based on

1. K. Awiszus, Y. Bell, J. Lüttringhaus, G. Svindland, A. Voß & S. Weber (2023): Building Resilience in Cybersecurity – An Artificial Lab Approach. To appear in: *Journal of Risk and Insurance*
2. Auxiliary references
   - M. Fahrenwaldt, S. Weber & K. Weske (2018): Pricing of Cyber Insurance Contracts in a Network Model, *ASTIN Bulletin*, 48(3), 1175-1218
   - A. Barabási & M. Pósfai (2016): *Network Science*, Cambridge University Press
   - I.Z. Kiss, J.C. Miller & P.L. Simon (2017): *Mathematics of Epidemics on Networks*, Springer
   - M. Newman (2018): *Networks*, 2nd ed., Oxford University Press

Survey Papers

1. K. Awiszus, T. Knispel, I. Penner, G. Svindland, A. Voß & S. Weber (2023): Modeling and Pricing Cyber Insurance – Idiosyncratic, Systematic, and Systemic Risks, *European Actuarial Journal*, 13(1), 1 - 53
2. M. Dacorogna, & M. Kratz (2023): Managing cyber risk, a science in the making. *Scandinavian Actuarial Journal*
3. M. Scherer & S. Weber (2023): Challenges in Cyber Risk and Cyber Insurance: Models, Methods and Data. To appear in: *Annual Research and Innovations Briefs*, ENISA

Thank you for your attention!