Cyber-Versicherung und Netzwerkmodelle

Kerstin Awiszus

Institut für Versicherungs- und Finanzmathematik & House of Insurance

Leibniz Universität Hannover

www.insurance.uni-hannover.de

House of Insurance Day – 05.09.2022

Agenda

1. **Motivation:** Bedeutung und Herausforderungen von Cyber-Versicherungen
2. **Überblick:** Mathematische Modellierung von Cyber-Risiken
3. **Beispiel:** Ein Netzwerkmodell zum Versicherungspricing systemischer Cyber-Risiken

Agenda

1. **Motivation:** Bedeutung und Herausforderungen von Cyber-Versicherungen
2. **Überblick:** Mathematische Modellierung von Cyber-Risiken
3. **Beispiel:** Ein Netzwerkmodell zum Versicherungspricing systemischer Cyber-Risiken

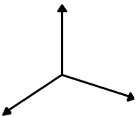
Motivation

- Fortschreitende Digitalisierung und Vernetzung der Wirtschaft
  bei zunehmender Komplexität der IT-Systeme führt zu erhöhter Anfälligkeit
  für Cyber-Kriminalität
- Jährliche Schäden durch Cyber-Risiken weltweit $\approx$ 445 Milliarden USD (2014)
  $\approx$ 600 Milliarden USD (2018)
  $\approx$ 1000 Milliarden USD (2020)[1]

[1] Center for Strategic & International Studies

Motivation

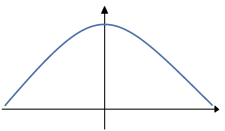
- Fortschreitende Digitalisierung und Vernetzung der Wirtschaft
  bei zunehmender Komplexität der IT-Systeme führt zu erhöhter Anfälligkeit
  für Cyber-Kriminalität
- Jährliche Schäden durch Cyber-Risiken weltweit $\approx$ 445 Milliarden USD (2014)
  $\approx$ 600 Milliarden USD (2018)
  $\approx$ 1000 Milliarden USD (2020)[1]



- **Cyber-Risiko-Dimensionen:**
  - **Ursachen**
    technische Störungen, menschliches Fehlverhalten, Insider/Hacker-Attacken
  - **Schäden**
    Datenverlust oder -diebstahl, Betrug und Erpressung, Reputationsschäden, Betriebsausfälle, Attacken auf kritische Infrastruktur, körperliche Schäden und Todesfälle
  - **Schutzmaßnahmen**
    Systemupdates, Entwicklung von Notfallplänen, Versicherungslösungen

[1] Center for Strategic & International Studies

Motivation (2)



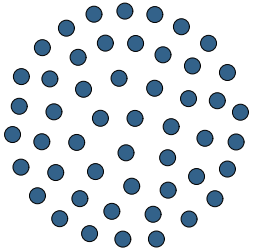
- **Aktuarielle Herausforderungen:**
  - **Datenverfügbarkeit**
    Daten sind bisher weder in geeigneter Menge noch Detailliertheit vorhanden
  - **Technologischer Fortschritt**
    Cyber-Risiken unterliegen einem stetigen Wandel
  - **Kumulschäden**
    keine stochastische Unabhängigkeit der Risiken
    keine geografische Einteilung in Gruppen, wie bspw. bei NatCat-Risiken, möglich
  - **Unterschiedlichkeit der Risiken**
    verschiedenartige Ursachen und resultierende Schäden

Agenda

1. **Motivation:** Bedeutung und Herausforderungen von Cyber-Versicherungen
2. **Überblick:** Mathematische Modellierung von Cyber-Risiken
3. **Beispiel:** Ein Netzwerkmodell zum Versicherungspricing systemischer Cyber-Risiken

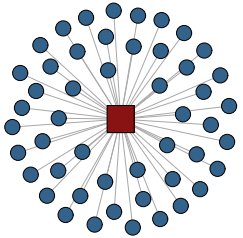
Klassifizierung von Cyber-Risiken

Die Eignung eines Modellierungsansatzes ist abhängig von der Art des Cyber-Risikos:



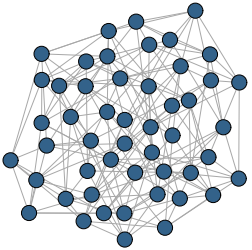
idiosynkratisch

(individuelle Risiken, z.B. gezielte Hacker-Attacken, Fehler, Störungen)



systematisch

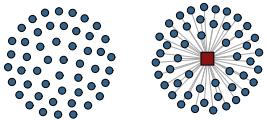
(gemeinsamer Risikofaktor, z.B. Angriffe auf breit genutzte Soft- oder Hardware)



systemisch

(Ausbreitungsrisiken, z.B. Viren, Würmer, Trojaner)

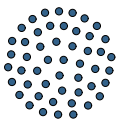
Modellierung idiosynkratischer und systematischer Risiken

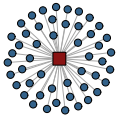


- Zur Modellierung von idiosynkratischen und systematischen Risiken können **klassische aktuarielle Methoden** genutzt werden
- **Typischer Ansatz:** Kollektives Modell (Frequency-Severity-Approach)
  - Zeitintervall $[0, t]$, $t > 0$ (häufig $t = 1$ Jahr)
  - Kollektiv von VN verursacht Schadenzahl $\mathcal{N}_t$ mit entsprechenden Schadenhöhen $\mathcal{Y}_1, \mathcal{Y}_2, \ldots$
  - Gesamtschaden:

$$\mathcal{S}_t = \sum_{j=1}^{\mathcal{N}_t} \mathcal{Y}_j, \quad t > 0.$$

Modellierung idiosynkratischer und systematischer Risiken





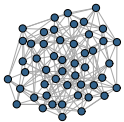
- Zur Modellierung von idiosynkratischen und systematischen Risiken können **klassische aktuarielle Methoden** genutzt werden

- **Typischer Ansatz:** Kollektives Modell (Frequency-Severity-Approach)
  - Zeitintervall $[0, t]$, $t > 0$ (häufig $t = 1$ Jahr)
  - Kollektiv von VN verursacht Schadenzahl $\mathcal{N}_t$ mit entsprechenden Schadenhöhen $\mathcal{Y}_1, \mathcal{Y}_2, \ldots$
  - Gesamtschaden:

$$\mathcal{S}_t = \sum_{j=1}^{\mathcal{N}_t} \mathcal{Y}_j, \quad t > 0.$$

Problem: Die dynamische Interaktion von systemischen Cyber-Risiken kann durch solche klassischen Ansätze nicht vollständig abgebildet werden

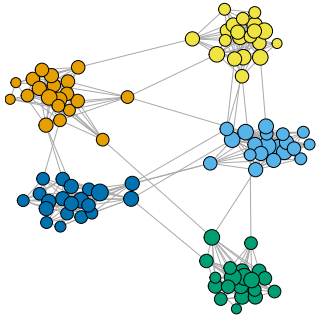
$\rightarrow$ Ein möglicher **Lösungsansatz:** *Epidemische Netzwerkmodelle*



Agenda

1. **Motivation:** Bedeutung und Herausforderungen von Cyber-Versicherungen
2. **Überblick:** Mathematische Modellierung von Cyber-Risiken
3. **Beispiel:** Ein Netzwerkmodell zum Versicherungspricing systemischer Cyber-Risiken

Modellierung systemischer Cyber-Risiken

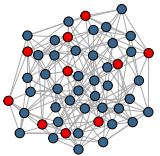


- Fokus auf Risiken, die sich innerhalb eines Netzwerks ausbreiten, z.B. Computerviren, Würmer, Trojaner
- **Beispiel:** Schadprogramm WannaCry infizierte im Mai 2017 mehr als 230.000 Computer in 150 Ländern
- **Unser Modell:**
  - Stochastisches Modell basierend auf IPS und markierten Punktprozessen
  - Versicherungsanwendung: Explizite Prämienberechnung möglich
  - Systemisches Risiko: Analyse des Einflusses der Netzwerkstruktur

Grundidee des Modells

1. **Ausbreitungsprozess der Cyber-Infektion:**
   - Agenten sind verbunden durch ein Netzwerk
   - Cyber-Infektionen können innerhalb des Netzwerks von Nachbar zu Nachbar übertragen werden
   - Heilung erfolgt unabhängig von anderen Agenten

   → Markov-Prozess in stetiger Zeit, genauer: SIS-/Kontaktprozess



2. **Schadensprozesse:**
   - Cyber-Attacken treten zu zufälligen Zeitpunkten auf
   - Hierdurch erleiden infizierte Netzwerkknoten Schäden zufälliger Höhe

   → Markierter Punktprozess

3. **Vertraglich vereinbarte Deckung:**
   - Ein (Rück-)Versicherungsunternehmen (VU) leistet eine vertraglich vereinbarte Zahlung

   → Funktion der tatsächlich eingetretenen Schäden

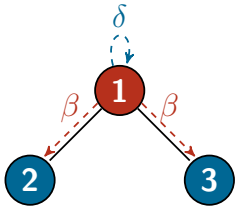
Mathematische Modellierung

N Agenten verbunden durch ein Netzwerk $A = (a_{ij}) \in \{0,1\}^{N \times N}$

Mathematische Modellierung

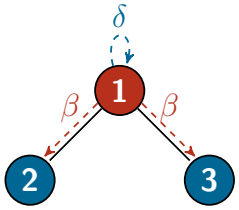
N Agenten verbunden durch ein Netzwerk $A = (a_{ij}) \in \{0,1\}^{N \times N}$

1. **Ausbreitungsprozess der Cyber-Infektion:**
   - $X = (X(t))_{t \geq 0} = (X_1(t), \ldots, X_N(t))_{t \geq 0}$, $X_i(t) \in \{0,1\}$
   - Parameter: $\beta > 0$ (Infektionsrate), $\delta > 0$ (Heilungsrate)
   - Übergangsraten für Agent i:
     - $X_i : 0 \to 1$; $\beta \sum_{j=1}^{N} a_{ij} X_j(t)$ (Infektion),
     - $X_i : 1 \to 0$; δ (Heilung)



Mathematische Modellierung

N Agenten verbunden durch ein Netzwerk $A = (a_{ij}) \in \{0,1\}^{N \times N}$

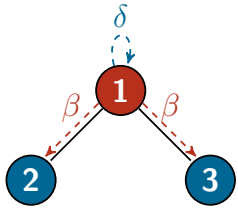


1. **Ausbreitungsprozess der Cyber-Infektion:**
   - $X = (X(t))_{t \geq 0} = (X_1(t), \ldots, X_N(t))_{t \geq 0}$, $X_i(t) \in \{0,1\}$
   - Parameter: $\beta > 0$ (Infektionsrate), $\delta > 0$ (Heilungsrate)
   - Übergangsraten für Agent i:
     - $X_i : 0 \to 1$; $\beta \sum_{j=1}^{N} a_{ij} X_j(t)$ (Infektion),
     - $X_i : 1 \to 0$; δ (Heilung)

2. **Schadensprozesse:**
   - Zählprozess $M = (M(t))_{t \geq 0}$ mit Werten in $\{0, 1, 2, \ldots\}$
   - Schadenhöhenprozess $L = (L(t))_{t \geq 0} = (L_1(t), L_2(t), \ldots, L_N(t))_{t \geq 0}$ mit Werten in $\mathbb{R}^N_{\geq 0}$

Mathematische Modellierung

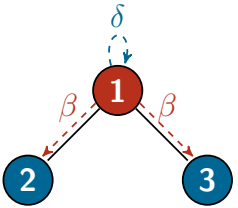
N Agenten verbunden durch ein Netzwerk $A = (a_{ij}) \in \{0,1\}^{N \times N}$



1. **Ausbreitungsprozess der Cyber-Infektion:**
   - $X = (X(t))_{t \geq 0} = (X_1(t), \ldots, X_N(t))_{t \geq 0}$, $X_i(t) \in \{0,1\}$
   - Parameter: $\beta > 0$ (Infektionsrate), $\delta > 0$ (Heilungsrate)
   - Übergangsraten für Agent i:
     - $X_i : 0 \to 1$; $\beta \sum_{j=1}^{N} a_{ij} X_j(t)$ (Infektion),
     - $X_i : 1 \to 0$; δ (Heilung)
2. **Schadensprozesse:**
   - Zählprozess $M = (M(t))_{t \geq 0}$ mit Werten in $\{0, 1, 2, \ldots\}$
   - Schadenhöhenprozess $L = (L(t))_{t \geq 0} = (L_1(t), L_2(t), \ldots, L_N(t))_{t \geq 0}$ mit Werten in $\mathbb{R}_{\geq 0}^N$
3. **Vertraglich vereinbarte Deckung:**
   - $f(\cdot;\cdot) : \mathbb{R}_+ \times \mathbb{R}_+^N \to \mathbb{R}_+$,
   - Das VU zahlt $f(t; L(t) \circ X(t))$, falls eine Cyber-Attacke zum Zeitpunkt $t > 0$ auftritt

Mathematische Modellierung

N Agenten verbunden durch ein Netzwerk $A = (a_{ij}) \in \{0,1\}^{N \times N}$



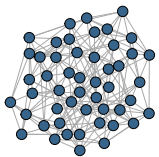
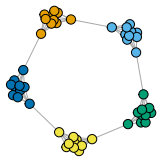
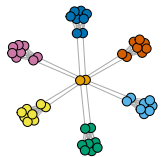
1. **Ausbreitungsprozess der Cyber-Infektion:**
   - $X = (X(t))_{t \geq 0} = (X_1(t), \ldots, X_N(t))_{t \geq 0}$, $X_i(t) \in \{0,1\}$
   - Parameter: $\beta > 0$ (Infektionsrate), $\delta > 0$ (Heilungsrate)
   - Übergangsraten für Agent i:
     - $X_i : 0 \to 1$; $\beta \sum_{j=1}^{N} a_{ij} X_j(t)$ (Infektion),
     - $X_i : 1 \to 0$; δ (Heilung)
2. **Schadensprozesse:**
   - Zählprozess $M = (M(t))_{t \geq 0}$ mit Werten in $\{0, 1, 2, \ldots\}$
   - Schadenhöhenprozess $L = (L(t))_{t \geq 0} = (L_1(t), L_2(t), \ldots, L_N(t))_{t \geq 0}$ mit Werten in $\mathbb{R}^N_{\geq 0}$
3. **Vertraglich vereinbarte Deckung:**
   - $f(\cdot;\cdot) : \mathbb{R}_+ \times \mathbb{R}_+^N \to \mathbb{R}_+$,
   - Das VU zahlt $f(t; L(t) \circ X(t))$, falls eine Cyber-Attacke zum Zeitpunkt $t > 0$ auftritt
4. **Erwarteter Gesamtschaden des VU in** $[0, T]$**:** $\mathbb{E}\left[\int_0^T f(t; L(t) \circ X(t)) dM(t)\right]$

Zusammenfassung der Ergebnisse

- In unserem Modell:
  Explizite Berechnung des erwarteten Gesamtschadens für allgemeine Vertragsfunktionen möglich

- Berechnung führt zu numerischen Schwierigkeiten
  → Entwicklung geeigneter Approximationsmethoden, z.B.:
  - Nichtlineare Vertragsfunktionen → Polynomapproximation
  - 2^N Zustände des Ausbreitungsprozesses → Mean-Field-Approximation zur Berechnung der Momente
  - Alternativ: Monte-Carlo Simulation

- Analyse numerischer Fallstudien:
  → Netzwerktopologie besitzt erheblichen Einfluss auf die erwartete Gesamtschadenhöhe

Fazit

- Cyber-Risiken unterscheiden sich von anderen versicherten Risiken auf vielfältige Art und Weise, was VU – und insbesondere ihre Aktuare – vor große Herausforderungen stellt
- Insbesondere sind Daten bisher weder in geeigneter Menge noch Detailliertheit vorhanden
- Bei der Modellierung von Cyber-Risiken lassen sich drei Klassen von Cyber-Risiken unterscheiden: idiosynkratische, systematische und systemische Risiken
- Während für idiosynkratische und systematische Cyber-Risiken klassische aktuarielle Methoden weitgehend passend erscheinen, benötigen systemische Risiken neuartige Ansätze – zum Beispiel basierend auf epidemischen Netzwerkmodellen
- Die Topologie des Netzwerks besitzt dabei erheblichen Einfluss auf das resultierende Risiko

Forschungsagenda und Ausblick

1. Datenverfügbarkeit & Top-Down-Ansätze
   - Die Kalibrierung von Cyber-Risikomodellen stellt aufgrund der begrenzten Datenverfügbarkeit derzeit noch eine enorme Herausforderung dar
   - **Fernziel:** Aufbau von (wissenschaftlich zugänglichen) Pools für relevante Cyber-(Infektions-)Daten
   - **Approximation:** Top-Down-Ansätze, z.B. populationsbasierte Epidemiemodelle

2. Strategische Interaktion & Netzwerkmodelle
   - **Ziel:** Integration strategischer Interaktionsaspekte in Netzwerkmodelle

3. Pricing von Cyber-Risiken & systemische Risikomaße
   - **Idee:** Pricing von systemischen Cyber-Risiken mithilfe systemischer Risikomaße, welche die dynamische Interaktion innerhalb der Risikomessung berücksichtigen können

Vielen Dank!

Literatur:

1. **Überblick:** 'Modeling and Pricing Cyber Insurance – A Survey'
   (mit T. Knispel, I. Penner, G. Svindland, A. Voß & S. Weber)
   Working Paper, 2022.
2. **Beispiel:** 'Pricing of Cyber Insurance Contracts in a Network Model'
   (mit M.A. Fahrenwaldt & S. Weber)
   ASTIN Bulletin: The Journal of the IAA, 48(3):1175–1218, 2018.