Received: 7 November 2022 | Revised: 20 May 2023 | Accepted: 15 August 2023

DOI: 10.1111/jori.12450

ORIGINAL ARTICLE

Journal of Risk and Insurance

Building resilience in cybersecurity: An artificial lab approach

Kerstin Awiszus[1] | **Yannick Bell**[2] | **Jan Lüttringhaus**[2] | **Gregor Svindland**[2] | **Alexander Voß**[2] | **Stefan Weber**[2]

[1]University of Applied Sciences and Arts, Hannover, Germany

[2]House of Insurance, Leibniz Universität Hannover, Hannover, Germany

Correspondence
Stefan Weber, House of Insurance, Leibniz Universität Hannover, Hannover, Germany.
Email: stefan.weber@insurance.uni-hannover.de

Abstract

Based on classical contagion models we introduce an *artificial cyber lab*: the digital twin of a complex cyber system in which possible cyber resilience measures may be implemented and tested. Using the lab, in numerical case studies, we identify two classes of measures to control systemic cyber risks: security- and topology-based interventions. We discuss the implications of our findings on selected real-world cybersecurity measures currently applied in the insurance and regulation practice or under discussion for future cyber risk control. To this end, we provide a brief overview of the current cybersecurity regulation and emphasize the role of insurance companies as private regulators. Moreover, from an insurance point of view, we provide first attempts to design systemic cyber risk obligations and to measure the systemic risk contribution of individual policyholders.

KEYWORDS

complex systems, complexity economics, cyber insurance, cyber resilience, cybersecurity, economics of networks, systemic cyber risks

1 | INTRODUCTION

Cyber risks pose a major threat to societies, governments, businesses, and individuals worldwide. For example, the annually published Allianz Risk Barometer, see Allianz (2022), recently identified cyber incidents as the most important global business risks, ahead of business interruptions, natural disasters, and pandemic outbreaks. In addition, cyber risk continues to increase, first due to the continued digitization of business processes, second due to the COVID-19 pandemic and the associated increase in teleworking, see for example, Lallie et al. (2021), and third in the context of the current political conflicts and wars.

Regulatory and macroprudential leaders are increasingly aware of the potentially catastrophic consequences of cyber risks. In particular, the systemic relevance of certain types of cyber threats, so-called systemic cyber risks, is highlighted, see for example, Lagarde (2021). Two illustrative systemic cyber incidents from the past are the WannaCry and NotPetya attacks[1]:

- In May 2017, the WannaCry ransomware infected around 230,000 computer devices in more than 150 countries. It encrypted data on the infected systems and demanded a ransom payment of USD 300. The encryption resulted in data loss and rendered IT systems unusable in healthcare services and in industry. It is estimated that the damage caused ranges from hundreds of millions to four billion US dollars. The discovery of a "kill switch" helped contain the incident.
- In June 2017, the NotPetya malware was used for a global cyberattack that mainly targeted Ukraine. This version of the Petya malware was disguised as ransomware, but with the intention of causing maximum damage by encrypting data and disrupting IT systems. The encryption of data resulted in a permanent loss of its availability with immediate impact on institutions such as the Ukrainian Central Bank and a disruption of the country's major stock markets. In addition, the malware was able to infect other organizations outside the Ukrainian financial sector with offices in Ukraine, compromising machines also elsewhere. For example, the global shipping company Maersk experienced widespread business disruptions at other locations around the world, which nearly destroyed the company.

This paper, in view of the previous examples, focuses on systemic cyber risks which are characterized by contagion effects in interconnected systems. Other instances of cyber accumulation scenarios are attacks based on a common risk factor such as the dependence on joint IT architecture or service providers, see for instance the infamous SolarWinds attack.[2] For insurance stress testing of accumulation scenarios which may not follow a contagion pattern, like DoS attacks or cloud outage, see the discussion in EIOPA (2022).

In light of the rapidly growing and evolving cyber threat landscape, cybersecurity approaches that focus solely on preventing attacks may be insufficient to manage and mitigate this class of systemic cyber risks. Therefore, building *cyber resilience* requires taking a more expansive approach that targets the "ability to *anticipate*, *withstand*, *recover from*, and *adapt to* adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources."[3]

[1]An in-depth risk analysis of these two incidents can be found, for example, in ESRB (2020).

[2]Awiszus et al. (2023) propose to classify aggregate cyber risks which depend on a common risk factor as *systematic* while reserving the notion *systemic* for cyber risks caused by local or global contagion effects.

[3]See the definition of "cyber resiliency" in NIST (2022).

Legislators and regulators have enacted a variety of laws and policies governing cybersecurity and identified the need to enhance the resilience of cyber systems. In addition, private actors may also take a leading role in shaping and guiding cybersecurity standards. In particular, the idea of (re)insurance companies acting as *private regulators* to fill existing regulatory gaps and mitigate residual risks has emerged.

But how can private and government regulators ensure an adequate level of protection against cyber threats and implement appropriate measures to build cyber resilience? What characteristics of networked cyber systems are critical to managing and controlling cyber threats and, in particular, to preventing, managing, and responding to the onset of a systemic cyber risk event? And is regulatory intervention even necessary to build effective levels of cyber resilience? In this paper, we address these questions. Our key contributions are:

1. We design the *artificial cyber lab*, the digital twin of a complex cyber system, to evaluate different types of cyber resilience measures. Digital twins consist of a "physical entity, a virtual counterpart, and the data links between them," cf. Jones et al. (2020). The virtual counterpart of interconnected cyber-physical systems is based on network contagion models and is therefore tailored to the analysis of *systemic cyber risks* such as the aforementioned WannaCry and NotPetya attacks.
2. In *two exemplary case studies*, we leverage the lab to generate artificial data from virtual counterparts of real-world cyber systems to analyze specific types of cyber resilience interventions.
   a) *Security-related interventions*: Interconnected actors in a cyber network use security investments to protect themselves from cyber risk contagion. We
      - study a *security investment game* modeling network interaction and interdependence effects related to IT security standards; unlike the vast majority of game-theoretic models in the cyber insurance literature, our game is based on the underlying *dynamic contagion* captured by stochastic Monte-Carlo simulations,
      - rigorously *prove* that there exists a steady state (Nash equilibrium) of security investment decisions which, however, generally does not minimize the overall cyber risk losses of the network,
      - develop and evaluate different *regulatory allocation strategies* to further improve the overall system security in a steady state of security investment choices,
      - and analyze centrality measures to identify *systemically relevant nodes* for the targeted allocation of cybersecurity obligations.
   b) *Topology-based interventions*: Network topology is important for both network functionality and the risk of cyber epidemic contagion. Therefore, we
      - characterize the cyber contagion risk exposure of large-scale networks,
      - study the effect of network heterogeneity on risk amplification,
      - discuss possible *efficient intervention strategies* that minimize the negative impact on network functionality,
      - present a *novel approach* to quantify contagious cyber risks and effectively allocate associated surcharges or insurance premiums based on the identification of critical network connections.

   Our digital twin approach provides an experimental framework for testing and evaluating different regulatory intervention strategies. This is particularly important due to the lack of data on historical cyber incidents and the nonstationarity of the cyber environment. Our results clearly indicate a *need for regulation* to build an appropriate level of cyber resilience.

3. Based on the findings from the case studies, selected regulatory measures that are currently in use or under debate to strengthen resilience in real-world networked cyber systems are discussed.
4. To this end, we provide a brief overview of the current regulatory framework for cybersecurity in the European Union and the United States. In addition, we also discuss the role of private actors, particularly cyber insurance companies, in shaping security standards.

1.1 | Literature

In the following, we will only briefly review the relevant literature. For a comprehensive overview of the various modeling and pricing approaches in the field of cyber risk and insurance, we refer the interested reader to the most recent survey Awiszus et al. (2023). Dacorogna and Kratz (2023) provides another recent discussion on characteristics, models, and the management of cyber risks.

In the actuarial literature, cyber loss models are often based on classical frequency-severity approaches; see, for example, Zeller and Scherer (2022) for an exemplary loss model and a comprehensive literature overview, and Eling (2020) for a recent review of research in business and actuarial science. While at first glance such approaches appear to be the most feasible from an insurer's perspective, they suffer from insufficient or inadequate data, see also Zeller and Scherer (2023). Furthermore, in the case of systemic cyber risks such as WannaCry or NotPetya, the structural importance of network effects for risk emergence and amplification cannot be adequately captured by these classical approaches. The dynamics of incidents are similar to feedback mechanisms in financial systems such as the propagation of economic distress in a network of creditors or business partners. Interaction mechanisms of this type were, for example, studied in Giesecke and Weber (2004) and Giesecke and Weber (2006) using results from the theory of interacting particle systems. A similar approach was first introduced in microeconomics in the seminal work Föllmer (1974), in which actors interact on a grid.

Regulatory aspects are also not considered in frequency-severity models for cyber claims. In a game-theoretic framework, by contrast, regulatory issues as well as network interdependence of policyholders can be taken into consideration. The existing literature on strategic interactions in cyber networks has focused mainly on the impact of cyber insurance on the self-protection efforts of interconnected actors, see, for example, Ogut et al. (2005), Bolot and Lelarge (2009), Schwartz and Sastry (2014), and Yang and Lui (2014). In most cases, market inefficiencies are observed and cyber insurance is not found to provide incentives for self-protection. However, in the absence of information asymmetries between insureds and insurer(s), simplified regulatory corrective actions and measures such as fines, rebates, or mandatory cyber insurance may increase incentives for self-protection, see, for example, Pal et al. (2014) and Naghizadeh and Liu (2014). For a detailed summary and comparative analysis of this literature, see Marotta et al. (2017); see also Böhme and Schwartz (2010), and Böhme et al. (2018). However, the modeling framework adopted for risk contagion is often extremely simple and static, excluding risk amplification and the possibility of very high loss events.

In contrast, dynamic models of contagion processes provide a more realistic framework. Originally, such models were developed in the field of mathematical biology and epidemiology since the seminal work of Kermack and McKendrick (1927). In the last two decades, extensive efforts have been made to incorporate the underlying contact structure within populations into the modeling framework: Epidemic processes have been generalized to networks; see, for example, Pastor-Satorras et al. (2015) and Kiss et al. (2017) for detailed reviews. Because of their ability to capture

interconnectedness, approaches to modeling epidemics in the context of cyber risk have also appeared recently. For example, models of network contagion are utilized in Fahrenwaldt et al. (2018), Xu and Hua (2019), Jevtić and Lanchier (2020), Antonio et al. (2021), and Chiaradonna et al. (2023) for the purpose of pricing cyber insurance policies. Furthermore, the impact of cyber risk contagion on insurance portfolios has been analyzed in Hillairet and Lopez (2021), and more recently the network structure of interconnected industry sectors has been considered, see Hillairet et al. (2022). A dynamic contagion game was introduced in Hayel et al. (2014) using the Markov-susceptible-infected-susceptible (SIS) model (but based on the easily tractable, albeit rough, NIMFA approximation). However, to our knowledge, the regulation, management, and control of contagious cyber risks have not yet been studied in a modeling framework based on dynamic contagion.

Beyond the field of cyber risk, applications of network models to insurance-related problems are less common in the literature. Existing works focus, for example, on the implementation of data science methods such as fraud detection techniques, see Tumminello et al. (2023), or study the systemic risk in financial networks where insurance companies themselves are present as interdependent financial actors, such as in Chen et al. (2020) and Chen and Sun (2020).

Studies of network resilience and robustness can be found in the engineering and computer science literature. However, much of the work focuses exclusively on measurements of network topology properties (see Freitas et al., 2022, for a recent overview) or is based on models of lateral network movements that do not capture the infection and recovery dynamics of risk contagion (see Chen et al., 2018 or Freitas et al., 2020). Moreover, resilience building is studied only from a network perspective and not in a regulatory framework. A specific attempt to build network resilience against self-propagating malware, and in particular the WannaCry worm, was recently presented in Chernikova et al. (2022). The authors use synthetic WannaCry data to derive an adequate contagion model, similar to the classic susceptible-infected-recovered (SIR) model, and appropriate parameter estimates. However, this model follows a deterministic top-down population-based approach, whereas our study is based on a stochastic bottom-up model of node-level interactions. Again, resilience is considered from an engineering perspective rather than a regulatory one, and issues of network economics and risk management are also not considered.

1.2 | Outline

The paper is organized as follows. In Section 2, we provide a brief overview of current cybersecurity legislation in the European Union (EU) and the United States of America (US), and also mention the regulatory role of private actors and insurance companies. Based on this, we present a selection of current approaches from the field to strengthen cybersecurity. In Section 3, we introduce the artificial cyber lab, and in the following two sections, we conduct the aforementioned illustrative case studies to analyze security- and topology-based cyber resilience measures. In light of these findings, we also revisit the selected real-world approaches from Section 2. Section 6 concludes.

2 | THE REAL WORLD: THE CURRENT STATE OF CYBERSECURITY REGULATION

In what follows, we briefly discuss the main characteristics of current cybersecurity legislation in the EU and the US, as well as the role of private actors such as insurance companies in shaping cybersecurity standards. This discussion will serve to identify and classify a set of

real-world measures for improving resilience to cyberattacks, which we will then discuss in light of our findings from simulations conducted in the artificial cyber lab.

2.1 | Current government regulations for cybersecurity

Due to the enormously increasing importance of cybersecurity to the functioning of modern societies, lawmakers have enacted several regulations, including a variety of legal norms. However, given the nonstationary nature of cyberspace, policymakers tend to future-proof their regulations by using indeterminate legal terms when formulating security requirements. Examples of such phrases include "adequate security measures" or "adequate technical and organizational measures," see below. On the one hand, this can guarantee a high level of cybersecurity, even if a new technology or vulnerability is found. On the other hand, the indeterminacy of the legal terms introduces a significant degree of uncertainty as to the "correct" cybersecurity measures to be taken. In light of the latter problem, a growing number of technical standards and guidelines published by organizations such as the Cybersecurity & Infrastructure Security Agency (CISA) and the National Institute of Standards and Technology (NIST) in the US, the International Organization for Standardization (ISO), the European Network and Information Security Agency (ENISA), or TeleTrusT—IT Security Association Germany and the Bundesamt für Sicherheit in der Informationstechnik (BSI) in Germany provide specific guidance, see, for example, TeleTrusT (2021) and BSI (2022). While some of these standards actually serve as guidelines for government institutions, they are not legally binding for private companies, and furthermore they are usually characterized by a high degree of complexity, see, for example, BSI (2022). Both the nonlegally binding nature and the complexity may prevent companies from implementing these standards in practice.

Cyber security legislation in the EU and the US

Protection of critical infrastructure

- The EU sets minimum standards for cybersecurity of critical infrastructure in the 2020 NIS Directive.[4] The requirements include organizational provisions such as risk analysis and policies for information systems security, incident handling, business continuity and crisis management, supply chain security, and IT-related technical safeguards. In this context, critical infrastructure operators are required to implement "appropriate security measures." However, the specific design of these measures is not specified in the directive.
- In the US, the Cybersecurity and Infrastructure Security Agency Act of 2018 entailed the establishment of the Cybersecurity & Infrastructure Security Agency (CISA) by the Department of Homeland Security. The CISA regularly publishes *Binding Operational Directives* in which explicit actions improving the cybersecurity of federal civilian agencies are stated. For example, the recently published Directive BOD 22-01 requires all federal civilian agencies to remediate newly discovered exploits within a period of 2

[4]See the "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union." Later, we will also discuss the newly proposed NIS2 Directive which is set to replace the existing regulatory framework for critical infrastructures in the EU.

weeks since disclosure, based on a regularly updated catalog of known exploited vulnerabilities. Thereby, CISA sets a fixed threshold for software and service providers to roll out patches and updates for their respective end users. Although the BOD 22-01 targets federal civilian agencies only, CISA itself strongly recommends that private businesses review and monitor the catalog to strengthen their cybersecurity.

Data protection

- The *General Data Protection Regulation (GDPR)* is the centerpiece of data protection legislation in the EU. It has been in force since May 25, 2018 and regulates the handling of personal data. The central provision of data protection is addressed in Art. 32 GDPR, which requires the implementation of "appropriate technical and organizational measures," taking into account the "state of the art, the implementation costs, and the nature, scope, circumstances, and purposes of data processing." However, these terms are not further specified.
- In the US, many federal states have introduced legislation on data protection. Again, indeterminate legal terms are used to define legislative requirements. For example, Section 1798.81.5 (b) and Section 1798.81.5 (e) of the *California Consumer Privacy Act (CCPA)* state that "a business that collects a consumer's personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure"—without specifying which measures may be considered "reasonable security procedures."

2.2 | Regulation by private actors and the role of insurance companies

Against the backdrop of legal uncertainty associated with the presence of indeterminate terms under current legislation and the fact that recommended technical standards are typically not legally binding for business corporations, private actors may play an essential role in cybersecurity governance by implementing and shaping security standards. For example, Hurel and Lobato (2018) discuss the role of private companies as entrepreneurs of cyber standards, with particular attention to Microsoft's efforts to influence global security standards and policies.

For insurance companies and financial institutions, cyber security is an increasingly important issue because of their significance to society and the sensitive data they hold. An empirical study on this issue and its growing relevance within the US banking and insurance industry has been presented in Gatzert and Schubert (2022). Also, Sweetman (2022) provides a first history of computer security and network protection within major institutions from the UK banking sector.

In this paper, in contrast, we will focus to a greater extent on the particular role that cyber insurance companies can play in *promoting* security standards *among their policyholders*. This role has also been studied in, for instance, Trang (2017), Talesh (2018), Woods and Moore (2020), Herr (2021), and Lemnitzer (2021). There, it is found that insurers may act as *private regulators* in cybersecurity governance: Cyber insurance is an efficient way for companies to manage their cyber risk and seek assistance in implementing appropriate security measures. Hence, insurance companies can promote cybersecurity and resilience for their policyholders by setting certain standards in their contractual obligations.

2.3 | Selected measures of cyber resilience

In the previous sections, we discussed the current framework of cybersecurity regulation and emphasized the role of both governments and private actors such as insurance companies in implementing cybersecurity standards and strengthening resilience. In this section, we present a selection of concrete measures to improve cyber resilience focusing on systemic cyber risks that are either already part of current practice or currently under discussion. In particular, we include some measures which appear in the European Commission's proposal for replacing the existing NIS legislation by a new NIS2 Directive.[5] Consistent with the previous discussion, we will distinguish between government regulation (GOV) and private regulation, particularly insurance-based regulation (INS). In addition, we will distinguish between measures targeting the IT-security (*security-related interventions*) and those aiming at the structure of the network (*topology-based interventions*). To understand why we consider both, recall the infamous WannaCry and NotPetya attacks mentioned in the introduction, which can serve as models for studying systemic cyber risk. In both of these incidents, the risk propagation was due to the *spread of malware* across a *network* of interconnected actors and was characterized by the following two key aspects:

- Both attacks resulted from an initial vulnerability of Windows-based computer systems: devices that had not applied the latest patches from Microsoft or were running outdated systems were affected. Improved IT-security—in this case: regular software updates—may have prevented these attacks.
- Both cyber epidemics spread through IT networks and affect many interconnected computers across different institutions at a global scale. Controlling the topology, especially the connections to critical parts of the network, might have reduced the damage caused.

Security-related interventions: We consider the following security-related interventions:

GOV
- ◇ *Size-cap rule:* Instead of covering all, the proposal for the new NIS2 Directive suggests limiting the scope of the Directive to medium-sized and large companies operating in the targeted sectors or providing services covered by the NIS2 Directive. In general, micro or small enterprises from critical infrastructure sectors should not be affected by the directive while exceptional cases are listed in Article 2, §2.
- ◇ *Supply chain protection:* Article 18, §2 of the NIS2 proposal contains a new catalog of cybersecurity risk management measures that are intended to reflect the state of the art. Specifically, supply chain security measures must be implemented by addressing "security-related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services." Note the use of the indeterminate legal term "state of the art." Nonetheless, we adopt the idea of supply chain protection as a concrete measure that can be analyzed.

[5]See the "Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148—EU-doc. COM (2020) 823 final, dated 16 December 2020". A discussion on the proposal is provided in Sievers (2021).

INS
- *Assistance services*: Depending on the policyholder's own (lack of) expertise, the policyholder's level of security can be significantly increased by providing or requiring investment in cyber assistance services. Cyber assistance services include implementation services, staff training, and external security testing for policyholders. Some insurers also offer a 24/7 hotline with direct contact to technical experts, as well as public relations and legal experts at their own expense to minimize the potential damage from an ongoing cyberattack. Insurers could potentially mandate additional services for certain policyholders.
- *Patch management and backup:* The use of a patch management procedure and the application of a backup process are already part of the current cyber insurance practice, see, for instance, GDV (2017, sec. A1–16). However, efficiently tailoring these obligations to the characteristics of the policyholder can further improve their effectiveness.

Intuitively, the requirements for individual cybersecurity investments should contribute to a higher level of security for the overall system. However, increasing the level of security comes at a cost. There is, of course, a trade-off between the cost of maintaining a high level of cybersecurity and potential losses from cyberattacks. The situation becomes particularly complex when one considers that networked actors imply interdependent levels of IT security. The question naturally arises whether individually rational security investment decisions by network actors already provide a sound level of security for the system as a whole, or whether interdependence calls for additional security commitments? And if such extra commitments are necessary, how should they be implemented within a cyber network?

Topology-based interventions: The topological arrangement of the interconnected agents is critical to the extent of resulting cyber risk. We will consider the following topology-based arrangements:

GOV
- *Incident response and reporting*: Computer security incident response teams (CSIRTs) shall be designated by each EU member state according to Article 9 of the NIS2 proposal. Specific requirements and tasks for CSIRTs are defined in Article 10, including the monitoring of cyber threats, the implementation of an early warning system, and the provision of proactive network scanning upon request of an entity. In addition, Article 20 obliges "essential and important entities" to report incidents with a significant impact on their functioning or the provision of their services to regulatory authorities or the CSIRT without undue delay.
- *Critical supply chains*: In addition to IT-security aspects, also the underlying pattern of connections between business partners (and their partners) and along production chains may play an important role in securing supply chains. Therefore, the risk assessment of network characteristics may help protect highly interconnected industries and infrastructures. Article 19 of the NIS2 proposal allows for EU coordinated assessments of critical supply chains, identified by the Commission in consultation with ENISA.

INS
- ◇ *Contact liability premiums*: A major concern are existing contagion channels for risk spreading and amplification. For instance, policyholders might have to provide so-called *need-to-access* information when signing cyber insurance contracts, see for instance Kategorie B.4 in GDV (2019). The idea is to monitor the number and type of access to a given IT facility and thus control potential contagion channels. To counteract possible accumulation scenarios, it might even be sensible to introduce additional risk premiums for systemic cyber events that depend on the existing contagion channels.
- ◇ *Insurance backstop mechanism*: Lemnitzer (2021) argues for the necessity of a state-funded backstop mechanism for systemic cyber incidents to cover the losses of catastrophic events, similar to the Terrorism Risk Insurance Act (TRIA) which was established in the United States after 9/11. Here, a federal guarantee could be given to the insurance industry; after the occurrence of a systemic cyber event, mandatory surcharges could be imposed to the policyholders for the settlement of the costs incurred. Similar to the allocation of contact liability premiums, the size of these surcharges could correspond to the policyholders' individual contribution to the overall systemic risk.

Here too, of course, a trade-off exists between viewing the network links as contagion channels and providing an *effective infrastructure for data distribution*. Obligations should be implemented in a way that minimizes any negative impact on network functionality. But how can the exposure to large cyber risk be assessed in complex network arrangements? What network characteristics do significantly increase the risk of large-scale cyber events? And how can effective topology-based measures be designed and implemented?

3 | THE ARTIFICIAL CYBER LAB—THE DIGITAL TWIN OF A COMPLEX CYBER SYSTEM

Important characteristics of cyber risk are the scarcity of data and the non-stationarity of the cyber environment due to the rapidly evolving IT-infrastructure. However, since classical statistical and actuarial models follow a frequency-severity approach and thus heavily rely on a sufficient amount of meaningful data, these standard methods are insufficient to evaluate the impact of cyber resilience interventions. To explore the questions from the previous section and assess the quality of proposed measures, we follow the digital twin paradigm and propose a novel approach based on models from network science and contagion theory; an experimental setup where cyber resilience measures can be implemented and tested through analysis and simulation—the *artificial cyber lab*.

To build the virtual counterparts of real-world cyber systems, a certain degree of abstraction is necessary to provide a sufficiently complex but still tractable modeling framework. In general, network models for cyber risk contagion consist of three key components which we will sketch subsequently:

(i) A *network* representing interaction channels between agents or entities,
(ii) a model for the *spread* of a certain cyber threat through these interaction channels,

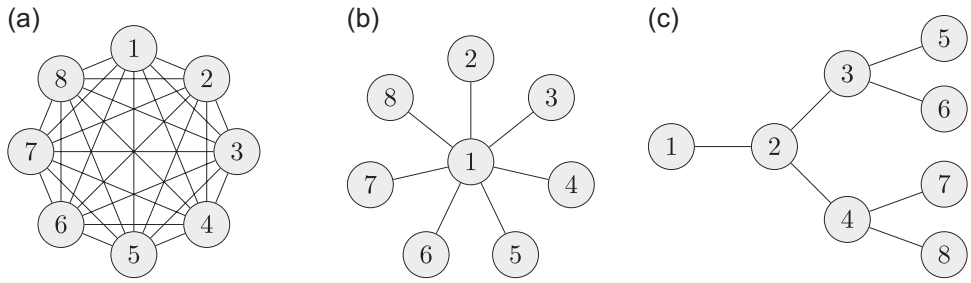

FIGURE 1 Exemplary network structures with $N = 8$ nodes. (a) Fully connected, (b) star-shaped, and (c) branching tree.

(iii) and a *loss model* determining the (monetary) losses occurring at the different agents due to the spread of the considered cyber threat.

3.1 | Networks

Systems of interconnected agents, like companies with data exchange, computer systems, or single devices, can mathematically be interpreted as networks. Agents are represented as *nodes*, and the interaction channels (potential infection channels) between them as *edges*. Exemplary network structures are depicted in Figure 1.

A simple (unweighted) network connecting N different agents can be represented by its adjacency matrix $A = (a_{ij})_{i,j\in\{1,\ldots,N\}}$ with $a_{ij} \in \{0, 1\}$: here, $a_{ij} = 1$ indicates that nodes i and j are directly connected, $a_{ij} = 0$ indicates no direct connection.[6] For example, in the case of the tree network depicted in Figure 1c, A is given by

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

3.1.1 | Random network models

In applied network analysis, the exact network structure is often unknown. In this case, random network models enable sampling from a class of networks with given fixed topological characteristics (such as the overall number of nodes). In a random network, each possible edge in the network is present (or absent) with a given fixed probability. We consider the following two standard classes of undirected random networks[7]:

[6]Alternatively, weighted networks could be considered. Here, $a_{ij} > 0$ represents the strength of the connection between nodes i and j.

[7]Pseudocode for both random network models is provided in Appendix C.

- *Erdős–Rényi networks:* The simplest random network model was introduced by Erdős and Rényi (1959): The Erdős–Rényi network $G_p(N)$ is constructed from a set of N nodes in which each of the possible $N(N-1)/2$ edges is independently present with the same probability p, that is, the expected number of edges is given by $(N(N-1)p)/2 \approx (N^2p)/2$ for large N.
- *Barabási–Albert networks:* A phenomenon widely observed in the empirical analysis of networks, including the World Wide Web, IT networks, and social networks, is that newly formed connections tend to emerge at nodes with an already large degree. For example, newly created websites are more likely to link to an already existing popular website than to other websites. This principle is called *preferential attachment*. Hence, real-world networks are usually more heterogeneous in terms of their topology than the Erdős–Rényi model would suggest. Often, a hierarchy of nodes is observable—with a few nodes of high degree (called *hubs*), and a vast majority of less connected nodes. A first model, motivated by the study of citation networks of academic papers, was introduced and discussed in Price (1965, 1976). The most commonly applied random graph model for networks which follow a preferential attachment principle is the one from Barabási and Albert (1999). Different from the Erdős–Rényi model, a Barabási–Albert network $BA(N; m)$ with N nodes is generated by a growing network algorithm: Starting from an initial core with n_0 nodes, $m \leq n_0$, and ϵ_0 edges, a new node i is added to the graph in each simulation step and m edges for i are randomly generated following a preferential attachment rule. The number of edges for the resulting network is given by $m(N-n_0)+\epsilon_0$, which, neglecting the initial core, can be approximated by mN.

3.1.2 | Measuring centrality

In network science, the structural importance of single nodes or edges within the network can be characterized using *centrality measures* $\mathcal{C}$. However, centrality is not a rigorously defined term and a large variety of different concepts has been proposed.

1. For a network edge e, a common way to measure centrality is to consider the fraction of shortest paths between any two nodes i and j that pass through e. The corresponding measure is then called *edge (betweenness) centrality*,[8] and, can be written as

$$\mathcal{C}^{\text{edge}}(e) = \sum_{i,j} \frac{\sigma_{ij}(e)}{\sigma_{ij}}, \tag{1}$$

   where σ_{ij} denotes the number of shortest paths between nodes i and j, and $\sigma_{ij}(e)$ is the total number of these paths that go through edge e.
2. For a network *node* i, two of the most frequently used measures are[9]
   - *Degree centrality:* Here nodes are simply ranked by their number of network neighbors, that is,

$$\mathcal{C}^{\text{deg}}(i) = \sum_{j=1}^{N} a_{ij} = \sum_{j=1}^{N} a_{ji},\ i = 1, \ldots, N, \tag{2}$$

   for an undirected graph. It accounts for immediate network effects.

[8]This centrality measure was introduced in Girvan and Newman (2002).

[9]For an extensive overview we refer to Newman (2018, chap. 7).

- *Betweenness centrality:* In contrast to degree-based approaches, betweenness centrality focuses on the role nodes may play as connections or "bridges" between different network regions. In analogy to the concept of *edge* betweenness centrality, the corresponding definition on the node level is given by

$$C^{\text{bet}}(i) = \sum_{j,h} \frac{\sigma_{jh}(i)}{\sigma_{jh}}, i = 1, ..., N, \tag{3}$$

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

3.2 | Modeling contagious cyber risks

Through the interaction channels described by the chosen network, a contagious cyber risk may spread. Mathematical models describing the spread of cyber epidemics on networks first divide the set of agents into distinct categories varying over time: for example, individuals that are *susceptible* to an infection, *infected*, and *recovered* individuals. The SIS and SIR Markov models constitute frequently used epidemic-spreading models on networks. The difference between them is the presence (SIR) or absence (SIS) of immunity: While reinfection events are possible in the SIS framework, in the SIR framework, recovered individuals gain permanent immunity. A rigorous discussion of the mathematical aspects is provided in Appendix A.

The possible transitions in these two models as well as their two key parameters, the infection rate τ and the recovery rate γ, are illustrated in Figure 2.[10]

3.3 | Cyber loss models

Finally, agents, that is, nodes in the network, may experience *losses* due to a cyber infection. Depending on the modeling purpose, the cyber loss model may emphasize different aspects of an ongoing cyber incident, like the total number of affected network components, aggregate losses of network nodes, and the monetary losses of single entities. Typically, an adequate model should reflect on the stochastic nature of risk scenarios and capture key statistical aspects of cyber loss distributions, including loss expectations and tail risk properties.

3.4 | Artificial cyber lab setup

For our design of the artificial cyber lab, a fundamental choice has to be made in terms of the contagious spread model, namely between a SIR and SIS approach (see Figure 2). Since we consider attacks similar to the WannaCry and NotPetya attacks, which were both based on the EternalBlue exploit, we assume that reinfections are rather unlikely because—once

[10]There also exist more nuanced models, for example, containing only a limited immunity (SIRS) or an additional category of exposed individuals, that is, individuals that are infected but not yet contagious (SEIR). For more details, see, for example, Pastor-Satorras et al. (2015) and Kiss et al. (2017).

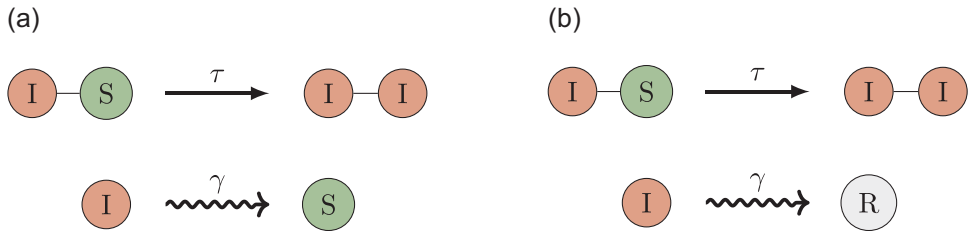

FIGURE 2 Infection and recovery for the (a) SIS and (b) SIR model in a network: A susceptible node is infected by its contagious neighbor with rate τ. Independent from the state of its neighbors, an infected node recovers at rate γ. SIS and SIR differ in terms of immunity: In the SIS model, a recovered node is susceptible again such that multiple infections for the same node are possible. In contrast, recovery in the SIR model means that the node is immune and cannot be infected again. SIR, susceptible-infected-recovered; SIS, susceptible-infected-susceptible. [Color figure can be viewed at wileyonlinelibrary.com]

detected—the underlying security issues are easily solvable through the installation of the latest patches. Therefore, we will use the SIR model.[11]

The key *in-* and *output parameters* can be summarized as follows:

- **Input**:
  - **Network**:
    - network size N (number of agents)
    - topological structure $A = (a_{ij})_{i,j=1,\ldots,N}$, that is, the connectivity pattern between nodes (see Figure 1, for examples)
    - number and position of initially infected nodes
  - **Epidemic dynamics**:
    - infection rate $\tau = 0.1$ (determines the speed of the infection), assumed to be equal for all connections[12]
    - individual recovery rates γ_i for nodes $i = 1, \ldots, N$ (influence the time needed for recovery—interpreted as IT security level, see Section 4)
  - **Loss distribution**:
    - stochastic modeling framework for loss formation
- **Output**:
  - **Epidemic dynamics**:
    - spread of cyber infection over time, total number of affected nodes, probability of infection for each node
  - **Loss distribution**:
    - aggregate losses for single nodes or the entire network

In the following, we use the lab to generate artificial data from our virtual model and evaluate two different types of cyber resilience interventions. Based on the results, we discuss the

[11]A similar choice has also been made in Hillairet and Lopez (2021) for modeling the WannaCry attack. Here, the authors use the population-based ordinary differential equation system from Kermack and McKendrick (1927) instead of a stochastic network model.

[12]Reasonable estimates of the infection speed in contagious cyber incidents cannot be derived due to insufficient data. We assume $\tau = 0.1$, which in a Markovian setting corresponds to the expected waiting time of 10 units of time for infectious transmission over a network edge. Our results can easily be adapted to a specific infection speed scenario by adequate interpretation of the time unit.

implications of our findings on the implementation of concrete cyber resilience measures for real-world cyber systems.

4 | CASE STUDY I: SECURITY-RELATED INTERVENTIONS UNDER STRATEGIC INTERACTION

For both the WannaCry and NotPetya attacks, the vulnerability of systems was crucially dependent on the security efforts taken by individual network users. Therefore, we first introduce a suitable model for security levels, benefits, and costs within the framework of our artificial cyber lab. However, due to the interconnectedness of entities in cyber systems, the individual risk exposure is also influenced by the security choices of other network participants: Interdependence and strategic interaction of different actors constitute key characteristic of systemic cyber risks. Therefore, we develop a *security investment game* to study interdependence effects within the cyber network. Finally, we evaluate if, and how, security-related interventions in the form of additional security obligations can efficiently be allocated among network nodes to improve the overall safety of the cyber system.

4.1 | Security investments and strategic interaction

In our SIR model, the cyber risk exposure of network nodes depends on the epidemic infection and recovery rates. For tractability reasons, we assume a *fixed* homogeneous infection rate τ (see Section 3.4) and vary the individual recovery rate γ_i of node $i = 1, ..., N$ which we will interpret as security level: The lower the security level γ_i, the longer it takes for firm i to detect a cyber infection or an existing security gap. Consequently, this also affects the risk exposure of the firm's direct network neighbors, see Figure 3.

From the perspective of the individual node i, the choice of security level γ_i results from the *trade-off* between the following two functions:

1. The *cyber loss function* $L_i(\gamma_1, \gamma_2, ..., \gamma_N)$ describes the losses of node i—as a function of all nodes' security levels due to the interconnectedness of network agents. In general, a loss model may capture a variety of aspects, see the discussion in the previous section. Clearly, the amount of cyber losses should be related to the *duration* of a cyberattack, which, for instance, may correspond to downtime of services[13] and business interruption costs. We choose a simple and tractable loss model by setting

$$L_i := L_i(\gamma_1, ..., \gamma_N) := \mathbb{E}\left[\int_0^\infty I_i(t)dt\right],$$

which represents the expected amount of time node i will spend in the infectious state I, given the security levels $\gamma_1, ..., \gamma_N$. In particular, L_i can be reduced by increasing the security level γ_i. For details, see Appendix D.

SIR infection dynamics are described by an ordered system of equations; see Appendix A for details. Note that the order of SIR equations increases up to the network size N. Hence,

[13]For example, this idea has been proposed in the loss model from Xu and Hua (2019).

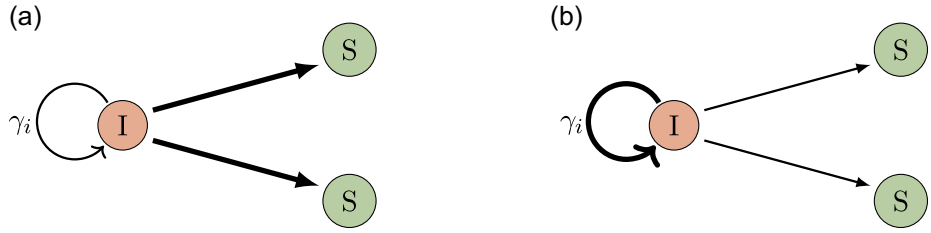

FIGURE 3 Contagious spreading for initially infected nodes with low and high recovery rates γ_i. The value of γ_i reflects the IT security level and protection efforts of company i. (a) Low security level and (b) high security level. [Color figure can be viewed at wileyonlinelibrary.com]

solving the exact system is intractable for complex networks due to the large number of system equations. We thus follow a *stochastic simulation approach*.[14] Further details are given in Appendix E.

2. The *cost function* $C_i(\gamma_i)$ describes the cost of the implementation of security level γ_i for node i. For simplicity, we let $C_i = C$ for all $i = 1, ..., N$. Typically, such a cost function should be strictly convex, representing a rapidly increasing cost with increasing targeted security level. Further, C should satisfy $C(0) = 0$. For simplicity and tractability, we choose an exponential function

$$C(\gamma_i) = e^{k\gamma_i} - 1, k > 0,$$

with growth constant k. In the following, we set $k = 1/3$.

A rational network agent i will try to minimize her *total expenses*

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

that is, the competing sums of security costs and cyber losses, as a function of γ_i.

As noted in Section 3.4, we choose the fixed homogeneous rate $\tau = 0.1$ for the *infection dynamics*. The contagion process is initialized at time $t = 0$ by the random infection of a single node. We remark that there are, of course, many reasonable choices for the loss and cost function and thus the total expenses, and also the infection dynamics. However, since our studies are of a qualitative and not a quantitative nature, we believe that our choices are suited to gain a basic understanding of the problem.

4.1.1 | Individually optimal security level

Under the assumption that for all nodes $j \neq i$ the security level γ_j remains unchanged, a security level γ_i is *individually optimal* for node i, if it minimizes the total expenses $\mathcal{E}_i$, that is, a rational agent will choose the individually optimal security level

[14]Trajectories of the SIR dynamics can be generated using the well-known *Gillespie algorithm*, cf. Gillespie (1976, 1977). Pseudocode is provided in Appendix B.

$$\gamma_i^{\text{ind}}(\gamma_{-i}) := \underset{\gamma_i \in [0,\infty)}{\arg\min}\ \mathcal{E}_i(\gamma_1, ..., \gamma_N) \quad \text{where} \quad \gamma_{-i} := (\gamma_1, ..., \gamma_{i-1}, \gamma_{i+1}, ..., \gamma_N).$$

An example for node 3 from the branching tree in Figure 1 is shown in Figure 4.

4.1.2 | Strategic interaction of interdependent actors

The security level choices of network agents do not only affect their individual expenses $\mathcal{E}_i$ but also the cyber losses $L_j, j \neq i$, of other network nodes. Therefore, these nodes will in turn react to the new threat situation, initializing a cascade of *strategic interactions*. We will call this the *security investment game*. A *steady state* of individually optimal security levels is a choice of security levels $\gamma \in (0, \infty)^N$ such that

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

In other words, a steady state is a *Nash equilibrium* of the security investment game. The following theorem asserts the existence of steady states of individually optimal security levels. The proof of Theorem 4.1 is provided in Appendix F.

Theorem 4.1. *Steady states of individually optimal security levels exist.*

Note that the theorem holds for basically any reasonable choices of cost functions C_i and loss functions L_i as long as the total expenses $\mathcal{E}_i$ remain strictly convex in γ_i and admit a minimum point. In that case, the proof would make use of Berge's maximum principle. We implement the security investment game as a dynamical game with several rounds $r = 0, 1, ..., M$ where every round r starts with a fixed vector of security levels

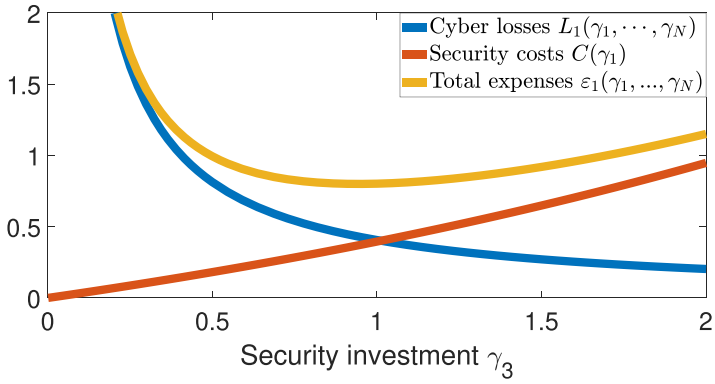

FIGURE 4 Cyber losses, security costs, and total expenses of node 3 in the branching tree from Figure 1 as a function of the security level γ_3. Infection rates are assumed to be homogeneous, $\tau = 0.1$, and security levels are set to $\gamma_j = 0.1$ for $j \neq 3$. The value $\gamma_3^{\text{ind}} = 0.943$ is individually optimal. Cyber losses are calculated using the decomposition scheme from Appendix D: $\mathcal{T} = 10,000,000$ trajectories of the susceptible-infected-recovered process were generated to determine the probability $\mathbb{P}(A_3)$ where A_3 is the event that node 3 becomes infected. For each simulation, the initially infected node was randomly chosen. [Color figure can be viewed at wileyonlinelibrary.com]

$$\gamma(r) = (\gamma_1(r), \gamma_2(r), ..., \gamma_N(r)).$$

Algorithm 4.2 (The security investment game).
Input: *Initial configuration* $\gamma(0) \in (0, \infty)^N$, *number of rounds* $M \in \mathbb{N}_{>0}$.

1. (Initialization) *Set* $r \to 0$.
2. *For every node* i, $i = 1, ..., N$, *calculate*

$$\gamma_i(r+1) = \underset{\gamma_i \in [0,\infty)}{\arg\min}\ \mathcal{E}_i(\gamma_1(r), ..., \gamma_{i-1}(r), \gamma_i, \gamma_{i+1}(r), ..., \gamma_N(r)).$$

More details are given in Appendix E. *Set*

$$\gamma(r+1) = (\gamma_1(r+1), \gamma_2(r+1), ..., \gamma_N(r+1)).$$

3. *If* $r < M$, *set* $r \to r+1$, *and return to Step* 2; *otherwise end*.

Output: *Security configuration* $\gamma(M)$ *after* M *rounds*

4.1.3 | Complex network interactions

We study the strategic interaction in two particular *fixed* networks: one generated from the Erdős–Rényi class with parameters $N = 50$ and $p = 0.16$, and another one drawn from the Barabási–Albert class with $N = 50$ and $m = 4$. Note that these two exemplary networks are comparable with respect to their number of network connections, cf. Section 3.1.1. Visualizations are provided in Figure 5.

On both networks, we conduct the security investment game (Algorithm 4.2) with $M = 50$ rounds and initial security level $\gamma_i(0) = 0.1$ for all nodes i. To generate values for the cyber losses L_i, in each round of the game, $\mathcal{T} = 10,000,000$ trajectories of the SIR epidemic process are simulated; see Appendix E for details.

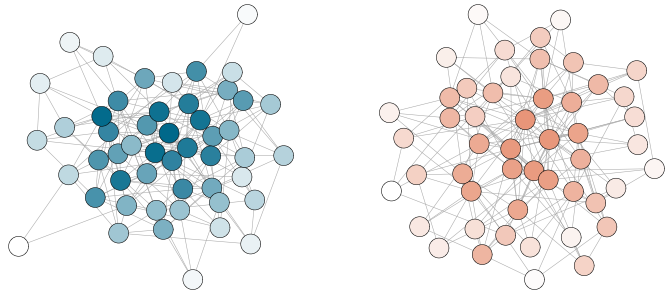

FIGURE 5 Visualization of the considered exemplary networks drawn from the Erdős–Rényi (left) and Barabási–Albert (right) classes. Nodes are colored according to their chosen level of security after round 50 of the security investment game (Algorithm 4.2): the darker the color, the higher the chosen security level (*for Erdős–Rényi*: minimum: 0.3780, maximum: 0.6526; *for Barabási–Albert*: minimum: 0.4719, maximum: 0.7598). Data is based on $\mathcal{T} = 10{,}000{,}000$ trajectories of the susceptible-infected-recovered epidemic process for each round of the security investment game. [Color figure can be viewed at wileyonlinelibrary.com]

The results of the security investment game in the steady state, $\gamma^{\text{stead}} = (\gamma_1^{\text{stead}}, ..., \gamma_N^{\text{stead}})$, are represented by node colors in Figure 5. For both network arrangements, we observe that more central nodes choose higher security levels than nodes in the periphery. The accumulated total expenses

$$\mathcal{E}(\gamma^{\text{stead}}) := \sum_{i=1}^{N} \mathcal{E}_i\left(\gamma_1^{\text{stead}}, ..., \gamma_N^{\text{stead}}\right)$$

are given by $\mathcal{E}(\gamma^{\text{stead}}) \approx 21.66$ for the Erdős–Rényi-type, and $\mathcal{E}(\gamma^{\text{stead}}) \approx 21.92$ for the Barabási–Albert-type network, respectively.

4.2 | Demand for regulation: Allocating additional security investments

In this section, we address the question whether the individually optimal security choices given by a steady state γ^{stead} are also favorable from an overall network perspective, that is, do they minimize the accumulated total expenses $\mathcal{E}(\gamma)$, or can *additional security investments* further improve the situation? In fact, the individually optimal security choices will in general *not* lead to a minimization of the overall network expenses, see Appendix G for a simple example. Indeed, it is well-known that Nash equilibria (steady states) do not in general minimize the social welfare function which in this case is the total expenses. In our case, a profound systematic characterization of the latter observation is, however, still an open challenge due to the lack of sufficient analytical tractability of the network dynamics, f.e., see Kiss et al. (2017, sec. 3.5.3) for a similar problem.

As indicated by the distribution of steady-state security investments shown in Figure 5, a key role in identifying good allocations of additional security investments may be played by the individual nodes' *centrality*. To this end, recall the degree and betweenness centrality of network nodes introduced in Section 3.1.2. Note that these standard centrality measures from the literature are solely based on the underlying network topology. The security investment game, however, suggests yet another way of measuring centrality, namely by fixing a steady state γ^{stead} and defining the centrality of node i to be the individually optimal investment

$$\mathcal{C}^{\text{inv}}(i) = \gamma_i^{\text{stead}}.$$

In the following, we will refer to this latter centrality measure as the *investment-based centrality*.

4.2.1 | Allocation strategies

In view of the previous discussion, in this section, we proceed as follows:

1. *We start from a steady state γ^{stead} of individually optimal security levels. Moreover, we fix an additional security budget $\beta > 0$.*
2. *This extra amount of security is allocated among the nodes according to one of the following strategies:*

(a) ***Untargeted*** *allocation: β is uniformly distributed among all network nodes, providing an additional security investment $\gamma_i^{\text{all}} = \beta/N$ for each node I.*
(b) ***Targeted*** *allocation: we choose a centrality measure $\mathcal{C}$ and determine the allocation weights*

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

Based on these allocation weights we consider two opposing procedures:
(i) *The **upper** allocation strategy allocates β proportionally $\gamma_i^{\text{all}} := \beta \cdot w_i$. Here a higher amount of β is assigned to nodes with a higher degree of centrality.*
(ii) *The **lower** allocation strategy does the opposite. To this end, we calculate the inverse allocation weights*

$$\hat{w}_i := \begin{cases} w_i^{-1} & \text{if } w_i \neq 0 \\ 0 & \text{else.} \end{cases}$$

In this case, the additional security investment $\gamma_i^{\text{all}} = \beta \cdot (\hat{w}_i / \sum_{j=1}^{N}\hat{w}_j)$ for node i assigns a higher amount of β to nodes with a lower, yet positive, degree of centrality.

The proposed allocation procedures yield a new vector of security levels $\tilde{\gamma}$ with entries

$$\tilde{\gamma}_i = \gamma_i^{\text{stead}} + \gamma_i^{\text{all}}, \quad i = 1, ..., N.$$

3. *Finally, we calculate the accumulated total network expenses $\mathcal{E}(\tilde{\gamma})$ under the new security configuration.*

4.2.2 | Allocation for complex networks

We compare the different allocation strategies and centrality measures for the Erdős–Rényi- and Barabási–Albert-type networks from Figure 5 by allocating an additional budget of $\beta = 5$. The strategies are visualized in Figure 6 and the resulting reductions of total network expenses are shown in Table 1 on a percentage basis.

In any case, we observe that the injection of additional network security *clearly reduces* the accumulated total expenses.

Comparing the different allocation procedures, we see that the upper allocation strategy leads to lower overall losses than both the untargeted and lower allocation strategies—regardless of the centrality measure chosen.

Moreover, for both types of networks, we observe that the upper allocation strategy combined with topology-based centrality measures outperforms the investment-based approach. In particular, the upper allocation strategy based on betweenness centrality yields the best outcome.

A possible reason for this is that the proportion of budget which is allocated to periphery nodes is too large in both the untargeted and investment-based case: For example, for the graph from the Erdős–Rényi class, the investment-based centrality of periphery nodes is more than half the size of the maximum node centrality, see Figure 6c. In contrast, the betweenness

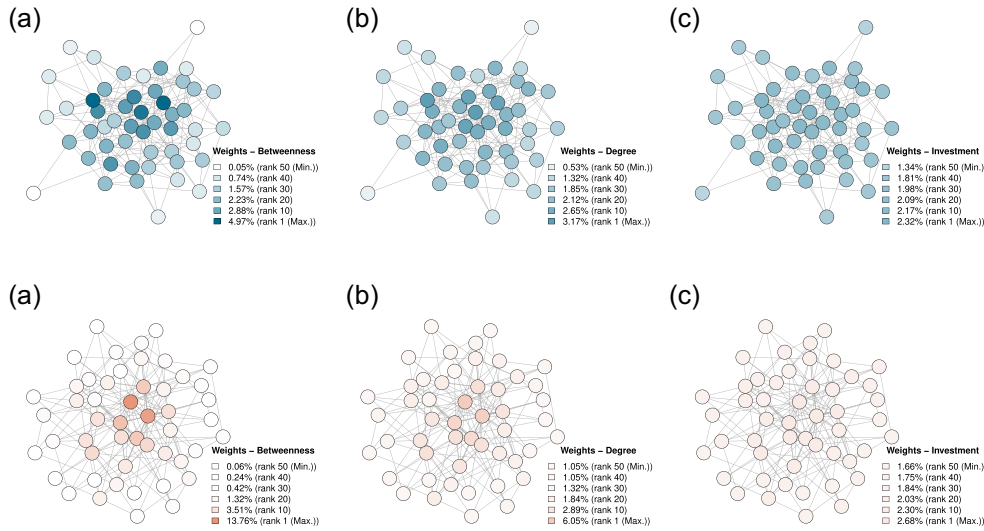

FIGURE 6 Exemplary visualization of centrality weights w_i in the Erdős–Rényi (top) and Barabási–Albert-type (bottom) network for (a) betweenness, (b) degree, and (c) investment centrality. [Color figure can be viewed at wileyonlinelibrary.com]

TABLE 1 Percental reduction of accumulated total expenses $\mathcal{E}$ after the allocation of the additional budget $\beta = 5$ among all network nodes.

	c^{deg}	c^{bet}	c^{inv}
Upper	10.6% 11.3%	10.8% 12.3%	10.2% 9.6%
Lower	8.2% 6.7%	0.5% 3.4%	9.5% 8.3%
Untargeted	9.9% 9.0%		

Note: The three proposed allocation strategies are evaluated for each of the suggested centrality measures. Entries for the Erdős-Rényi network are colored in blue (left entries), and for the Barabási-Albert network in salmon (right entries), respectively. For each entry, cyber losses were generated from T = 10,000,000 simulations of the SIR epidemic process. Full data is given in Appendix H.

centrality of the most isolated nodes is close to zero, and therefore, almost no additional security investment is allocated to these nodes, see Figure 6a.

4.2.3 | Further centralization of upper allocations

Our previous observations suggest that additional security investments should not be distributed equally among nodes, but in accordance with their centrality following an upper allocation strategy. Introducing specific requirements for *every* network entity may be difficult or even impossible from a regulatory point of view. For example, the upcoming NIS2 Directive introduces a specific size-cap rule which solely targets medium-sized and large entities in sectors of critical infrastructure, see the discussion in Section 2.3. But does the exclusion of low-centrality nodes from the allocation procedure substantially reduce the beneficial effect of

additional network security? Or can we even improve the effectiveness of security obligations if only a certain fraction of highest-centrality nodes is considered?

To answer these questions, the upper allocation procedure is slightly modified: Suppose we want to restrict the budget allocation to a certain fraction p of nodes with the highest centrality, and let $\mathcal{I}$ denote the set of corresponding node indices. Then, the amount of budget which is allocated to node i is chosen as

$$\gamma_i^{\text{all}} = \begin{cases} \beta \cdot \left(C(i) / \sum_{j \in \mathcal{I}} C(j) \right), & \text{if } i \in \mathcal{I}, \\ 0, & \text{else.} \end{cases}$$

Note that for $p = 100\%$, this coincides with the previously studied upper allocation strategy on the full network. The results of the modified procedure for different percentages of targeted nodes are depicted in Figure 7.

For the Erdős–Rényi network no substantial change of expenses is found when excluding the most decentralized nodes from the allocation of the additional security budget. In contrast, for the Barabási–Albert network and allocations based on investment and degree centrality, only targeting nodes with a medium to high degree of centrality is even beneficial. No substantial change, however, is observed in case of the betweenness-centrality-based allocation. As noted before, this may be due to the fact that in the betweenness-centrality case, the allocation weights of periphery nodes are anyway close to zero. In sum, our observations provide evidence that budget allocations to periphery nodes are rather ineffective.

Nevertheless, for all centrality measures and both types of networks under consideration, solely allocating the budget to a small fraction of nodes with the highest centrality does not prove to be optimal. A reason for that might be the trade-off between costs and efficiency: Additional security investments for highly central nodes come with substantially increasing costs, since these nodes already invest a high amount in the individually optimal steady state (see Figure 5) and the cost function $C_i(\gamma_i)$ is strictly convex.

For both types of networks, the overall best results are found for betweenness-based-allocations. However, the corresponding optimal total expenses are only slightly below the total expenses corresponding to adequately targeted degree-based allocations. Determining the betweenness centrality of nodes requires information on the full network topology, and this

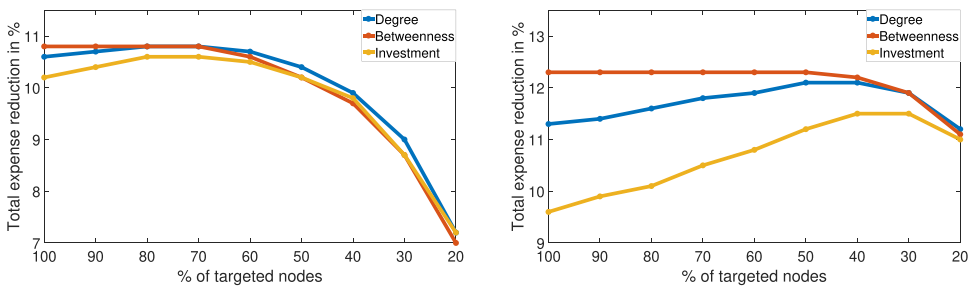

FIGURE 7 Refinement of the upper allocation strategy for different percentages of targeted nodes. Again, the total additional security budget is $\beta = 5$. For each data point, $\mathcal{T} = 10{,}000{,}000$ simulations of the epidemic process were generated. Full data is given in Appendix H. [Color figure can be viewed at wileyonlinelibrary.com]

information may not be available in practice. In contrast, node degrees, that is, the number of IT contacts of an agent in the cyber network, are local quantities, and thus, they can more easily be determined, for example, using questionnaires. Therefore, in view of the information-gathering issue and given the comparable performance in our simulations, degree-based allocations targeting the upper 50% of most central nodes may constitute a reasonable compromise.

4.3 | Evaluation of security-related interventions

We find that mandatory security investments as a regulatory obligation can actually increase the overall cybersecurity in a system of interconnected agents. More precisely, our simulations suggest the following:

(i) The strategic interaction of nodes in the cyber network leads to a *steady state* of security investments as proven in Theorem 4.1. However, the self-regulation of interdependent actors does in general *not* lead to an effective state of security configurations from an overall network perspective: A substantial improvement of this state is possible by the injection of additional security budget. Therefore, a *need for regulation* is found, and introducing adequate security-related obligations might be reasonable.
(ii) Severe security requirements for weakly connected entities like private households or companies with a very small number of business partners do not seem to have any notable effect on reducing network vulnerability. However, solely focusing on the most central nodes does not produce the best results either. Provided that these central nodes at least make the significant investments given by some steady state of the security investment game, additional investments come with massively increasing costs. Therefore, regulation should also focus on agents and companies with a medium to large number of IT or business contacts.
(iii) Centrality is not a rigorously defined concept. However, for both degree- and betweeness-based security allocations, good results are obtained. For practical reasons, degree-based allocations may be easier to implement: information on immediate network contacts can directly be obtained from agents, for example, using questionnaires.

As regards the selected cybersecurity measures given in Section 2 we find that:

GOV
- ◇ *Size-cap rule:* Remarkably, the approach proposed by the European Commission is in very good agreement with our findings: Security obligations for micro and small enterprises are ineffective, but both medium-sized entities as well as large businesses should be targeted. Therefore, our results strongly suggest that the size-cap rule is an efficient tool for improving resilience in cyber systems.
- ◇ *Supply chain protection:* The observation that efficient security allocations cannot solely be restricted to a small fraction of nodes with the highest centrality illustrates the need for a strengthening of security levels further down along possible paths of contagious transmission. Therefore, similar to the size-cap rule, our study supports the implementation of security-enhancing measures along supply chains.

INS ◇ *Assistance services:* Our study may help to identify companies for which assistance should be made mandatory in insurance contracts, and also give an estimate of the amount of services that should be made available to the specific policyholder. Further, in the case of an ongoing WannaCry- or NotPetya-type incident, the amount of resources for those assistance services may only be limited, see also the discussion in Hillairet and Lopez (2021). Thus, our results may also be useful for an effective resource allocation in such situations.

◇ *Patch management and backup:* Our observations suggest that the effectiveness of mandatory obligations strongly depends on the systemic importance of the examined entity measured by a reasonable centrality criterion. Medium-sized as well as large businesses with respect to centrality should not only invest more in cybersecurity, and thus in particular in their back-up and patching procedures, than smaller entities, but they should even invest more than an individually optimal assessment would suggest.

5 | CASE STUDY II: TOPOLOGY-BASED INTERVENTIONS AND CYBER PANDEMIC RISK

Due to the interconnectedness of modern IT systems, both the WannaCry and NotPetya incidents affected systems at a global scale, triggering large amounts of cyber losses. Clearly, a major regulatory concern is the prevention of such cyber pandemic incidents. Moreover, since risk pooling does not apply to systemic incidents, it is also important for insurance companies to reduce the risk of potential cyber accumulation scenarios within their portfolios.

Digital information and technology networks often come at a size of several 1000 nodes,[15] see the reference network data from Barabási and Pósfai (2016, table 2.1) and Newman (2018, table 10.1). In this section, we study the cyber pandemic risk exposure, first for homogeneous Erdős–Rényi-type networks, and then for heterogeneous—probably more realistic—Barabási–Albert-type networks of large size. We will observe that to control the cyber pandemic risk, regulatory approaches which solely focus on the improvement of individual cyber security are insufficient: interventions need to target the underlying *topological* network structure. Thus a clear demand for the regulation of the network topology in large-scale cyber systems is found. We will also observe that network heterogeneity massively amplifies the cyber pandemic risk.

5.1 | Demand for regulation: Network topology and cyber pandemic risk

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,[16] namely

- *small outbreaks*, affecting only a very small fraction of network nodes, and
- proper *epidemic outbreaks* or *pandemics*, where a large number of nodes becomes infected.

[15]The possibly largest existing network is the WWW with approximately $N = 10^{12}$ nodes.

[16]Mathematical details are extensively discussed in chapter 6 of Kiss et al. (2017).

To assess the risk of cyber pandemics, simulation studies are conducted. Again, for all networks, we choose a global infection rate of $\tau = 0.1$. In contrast to the previous study, recovery rates are assumed to be fixed and homogeneous for all nodes, that is, $\gamma_i = \gamma = 1$ for all $i = 1, ..., N$. This parameter choice implies that detection of cyber incidents is expected to be 10 times faster than infectious transmission, i.e., we *assume an overall high standard of IT security for the full network.*

5.1.1 | Cyber pandemic risk in homogeneous networks

We first analyze the cyber epidemic risk exposure of homogeneous large networks drawn from the Erdős–Rényi random graph model with a fixed size of $N = 1,000$. The benefit of this model class is that the resulting networks are easily tractable due to the fact that their topology is entirely determined by the parameters p and N. In particular, p can be interpreted as the control parameter of network connectivity. Each simulation is performed in the following way:

1. *Randomly draw a network* $G_p(1000)$ *from the Erdős–Rényi class.*
2. *Randomly choose a single node which is initially infected.*
3. *Randomly generate an infection trajectory from our SIR model. We are interested in the total number of infected nodes, that is, the* outbreak size.

The resulting frequency distribution of outbreak sizes is depicted in Figure 8. The following *phase transition* can be observed:

- For low connectivity probabilities p, only small outbreaks occur; the outbreak size frequency is exponentially decaying.
- *Tipping point behavior:* If a certain critical edge probability p_c is exceeded, the frequency distribution is characterized by a second peak around a characteristic large outbreak size.

The apparent strong dependence between network connectivity and outbreak sizes suggests that a supervision and regulation of the network is beneficial to avoid large systemic outbreaks.

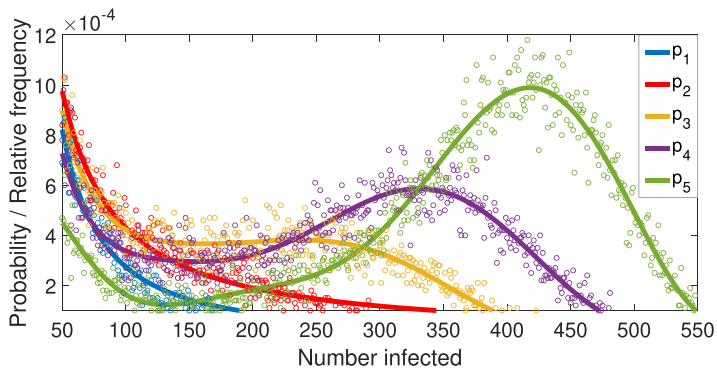

FIGURE 8 Final outbreak size frequencies given an initial infection of a single network node, over 100,000 simulations for increasing values of p; values are $p_1 = 0.01 < p_2 = 0.011 < p_c < p_3 = 0.012 < p_4 = 0.013 < p_5 = 0.014$. Exact data points from the simulation and appropriate regression curves (power law for p_1 and p_2, polynomial of degree 8 for p_3, p_4, p_5) are plotted. [Color figure can be viewed at wileyonlinelibrary.com]

Naively speaking, in a homogeneous network, the regulator should aim at keeping the network connectivity *below the critical threshold* p_c.

5.1.2 | The heterogenous case: Cyber pandemic risk in scale-free networks

On a larger scale, many real-world networks are characterized by a preferential attachment principle, see Barabási and Pósfai (2016, chap. 4), and therefore, a more heterogeneous topology is often observed: Let K be a random variable which represents the degree k_i of a randomly chosen network node i. Then

- the degree distribution of the Erdős–Rényi random graph $G_p(N)$ is given by a binomial form, that is, we have

$$\mathbb{P}(K = k) = \binom{N-1}{k} p^k (1-p)^{N-1-k}, \quad k = 0, ..., N-1,$$

- whereas under preferential attachment, the distribution of node degrees typically follows a power-law, that is,[17]

$$\mathbb{P}(K = k) \sim k^{-\alpha}, \quad \text{with degree exponent } \alpha \in \mathbb{R}_+.$$

  Node arrangements with $\alpha = 3$ can be modeled using the Barabási–Albert class introduced in Section 3.1.1. These so-called *scale-free* networks provide a hierarchy of nodes, with heavily connected high-degree hubs in their center and less connected nodes in their periphery.

Figure 9 shows representative networks from both the Erdős–Rényi and Barabási–Albert class, highlighting the different degree distributions.

This difference in the network topology has a strong impact on the epidemic vulnerability. Focusing on connectivity in terms of the sole number of edges, for networks of size $N = 1000$, the class of Barabási–Albert networks with $m = 5$ is comparable to Erdős–Rényi graphs with $p = 0.01$, since the resulting numbers of edges in both networks approximately coincide.[18] However, there exists a strong difference regarding their vulnerability to epidemic outbreaks, as shown by Figure 10: In contrast to the Erdős–Rényi graph, a clear second peak in the frequency distribution of outbreak sizes is observed for the Barabási–Albert network. Hence, the heterogeneity in the topology of Barabási–Albert networks remarkably lowers the critical connectivity threshold for cyber pandemics, that is, it amplifies the epidemic spread and triggers the emergence of large-scale outbreaks.

A profound characterization of this behavior in relation to the distribution of node degrees can be obtained in the limit of infinite network size $N \to \infty$: Neglecting additional correlation effects[19] it is known that large-scale pandemic outbreaks are possible if and only if the threshold condition

[17]For details and empirical examples, we refer to chapters 3 and 4 in Barabási and Pósfai (2016).

[18]Approximately 5000 edges should be present in both networks, see the discussion in Section 3.1.1.

[19]The effect of degree correlations and clustering on the dynamics of spreading phenomena is difficult to quantify analytically due to the dimensionality of the system, see also the discussion in Appendix A. Findings on their impact on the epidemic threshold are surveyed in Sections B1 and B2 of Pastor-Satorras et al. (2015).

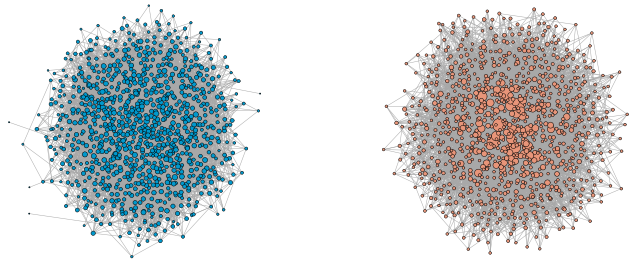

FIGURE 9 Erdős–Rényi $G_{0.01}(1000)$ (left) and Barabási–Albert $BA(1000; 5)$ (right). In both cases, the node size of node i is given by $100 \cdot \sqrt{k_i / \sum_{j=1}^{1000} k_j}$, an increasing function of the node's relative degree $k_i / \sum_{j=1}^{1000} k_j$. [Color figure can be viewed at wileyonlinelibrary.com]

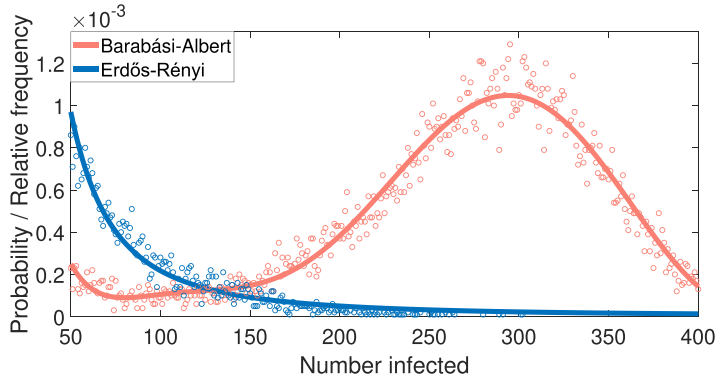

FIGURE 10 Final outbreak size frequencies given an infection of a single network node for the Barabási–Albert $BA(1000; 5)$ and Erdős–Rényi networks $G_{0.01}(1000)$ from Figure 9 over 100,000 simulations. Exact data points from the simulation and a regression curve (power law for Erdős-Rényi, polynomial of degree 8 for Barabási-Albert) are plotted. [Color figure can be viewed at wileyonlinelibrary.com]

$$\frac{\tau}{\tau + \gamma} \frac{\mathbb{E}[K^2 - K]}{\mathbb{E}[K]} > 1 \tag{4}$$

is satisfied, see Kiss et al. (2017, equation 6.4, p. 221).[20] Note:

- For Erdős–Rényi random graphs, in the limit the degree distribution is Poisson with parameter λ denoting the average degree, see Barabási and Pósfai (2016, sec. 3.4). Therefore, from (4), it follows that cyber pandemics can be prevented in the infinite limit if the network security/recovery rate γ satisfies $\gamma \geq \tau(\lambda - 1)$.
- In contrast, for scale-free networks with $\alpha \in (2, 3]$ and a sufficiently high number of nodes, it may be difficult or even impossible to prevent cyber pandemics by solely improving the network security or reducing the overall network connectivity. The reason for this is that in the infinite size limit, the second moment $\mathbb{E}[K^2]$ of the degree distribution diverges to ∞ while the first moment $\mathbb{E}[K]$ stays finite, see Newman (2018, sec. 10.4.2) for more details. Hence, in view of (4), with growing N, the security parameter γ must be substantially increased to prevent the

[20]See also Pastor-Satorras et al. (2015, equation 62) for an equivalent expression of the threshold.

occurrence of cyber pandemics. This comes with massively increasing costs. In the limiting case $N \to \infty$, (4) is always satisfied, regardless of the infection and recovery parameters chosen, so cyber pandemics may always occur.

In scale-free networks with a degree exponent α in the range of (2, 3] and a large number of entities, cyber pandemics are thus an *inherent risk* of the underlying network topology. The risk of cyber pandemic outbreaks cannot be controlled by security-related interventions, that is, by increasing the recovery rate γ, only, but requires a manipulation of the degree distribution, that is, the topological network arrangement. This behavior is clearly relevant in the risk assessment of cyberspace, which consists of a very large number of entities and is characterized by a heterogeneous, possibly scale-free, structure of interconnections.[21]

5.2 | Implementing suitable interventions

In the previous section, we have seen how a network's vulnerability to large-scale cyber pandemic outbreaks depends on the topology of the underlying cyber network. The following approaches may be considered to limit or control critical network connections and nodes:

- *Edge removal:* Edge deletion comprises
  - *physical deletion of connections*, such as any unnecessary access to servers, 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, see Chernikova et al. (2022).
- *Node splitting* to separate critical contagion channels and let them pass through two different nodes with the same operational task.

Since manipulating the network topology comes at a cost, probably reducing *network functionality*, the aim in the following is to identify critical network connections and nodes in a way which reduces negative effects on the network functionality to a minimum. A classical measure for network functionality is the *average shortest path length* $\langle l \rangle$: For nodes i and j, l_{ij} is the minimum number of edges connecting i and j. The average shortest path length is the average over all these distances, that is,

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

in case of a connected network. A small value of $\langle l \rangle$ is a measure for fast and efficient data flow, and hence, corresponds to a high network functionality. If a network consists of more than one component, then l_{ij} is not well defined for any two nodes i and j which come from two different

[21]For example, the Internet's degree distribution is estimated to be scale-free with degree exponent $\alpha \approx 2.5$ in Newman (2018, table 10.1).

components. In this case, we follow Newman (2018, p. 311) and adopt the definition by only taking the average over those node pairs which are connected by an existing path.[22]

5.2.1 | Edge removal and node splitting

Edge removal: To identify epidemically critical edges, we utilize the edge centrality given in (1) in Section 3.1.2 and propose the following procedure:

1. *Consider a network G. Determine the centrality of G's edges.*
2. *Consecutively delete the most central network edges. Stop the deletion process, if the resulting network does not exhibit a cyber pandemic outbreak any more.*

The procedure thus ends when pandemic outbreaks are not any longer observed in the resulting network G_c. Let $\mathcal{E}_c$ denote the set of edges which are deleted from G to obtain G_c, and let $|\mathcal{E}_c|$ be its number.

To illustrate the effectiveness of the proposed procedure, we determine the value $|\mathcal{E}_c|$ and the average shortest path length $\langle l_c \rangle$ of the resulting network G_c for the Barabási–Albert network depicted in Figure 9 with initial functionality of $\langle l \rangle \approx 2.96$ and outbreak size frequencies as shown in Figure 10. The results after edge deletion are depicted in Figure 11.

In comparison to random edge removals, it is clearly observable that the number of necessary edge deletions $|\mathcal{E}_c|$ can be significantly reduced by following the edge centrality deletion procedure. Moreover, the remaining network possesses a higher functionality represented by a lower average shortest path length $\langle l_c \rangle$ than in the case of random edge removals.

Node splitting: In the following, we propose a splitting procedure which is based on the suitable choice of a node centrality measure $\mathcal{C}$.[23] Nodes with highest centrality are splitted in an iterative manner, that is, centralities are re-evaluated after each split. Hence, nodes resulting from a split can be splitted again if they still exceed the rest of the network in terms of centrality.

Algorithm 5.1 (Node splitting). Input: *Initial network of N nodes, number n of node splits, node centrality measure $\mathcal{C}$*

1. *Determine the centrality of all network nodes.*
2. *Find the node i with highest centrality.*
3. *Split node i in the following way:*
   (i) *Add a new node j to the existing network.*
   (ii) *Create an order of node i's network neighbors where nodes are sorted according to their centrality.*
   (iii) *For nodes l with an even order rank, delete the edge between i and l and create a new edge between l and j.*

[22]In particular, this modification is relevant for the random edge deletions in Figure 11, where larger amounts of links are removed. The networks in Figures 11–13 which are generated by targeted edge deletions and node splittings are not fragmented into disconnected components.

[23]A similar algorithm was introduced in Chernikova et al. (2022).

4. *Repeat steps* (1)–(3) *until n node splits are conducted.*Output: *Resulting network* G_c *of* $N + n$ *nodes*

In analogy to the previously conducted analysis of edge removals, we study the effect of node splitting on the epidemic outbreak size distribution and functionality of the Barabási–Albert network from Figure 9 with initial outbreak size frequencies as shown in Figure 10. The results for degree- and betweenness-based node splitting are depicted in Figure 12, yielding almost identical results.

In comparison to edge removals, we find that node splitting is even more effective: Only about 6% of the most central nodes need to be splitted to control the risk of cyber pandemics.

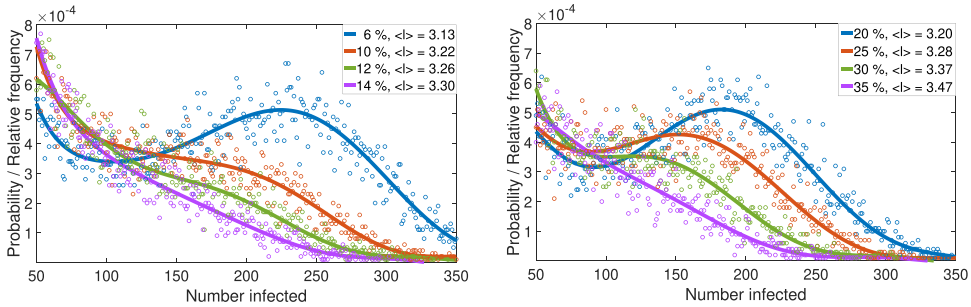

FIGURE 11 Final outbreak size frequencies given an initial infection of a single network node, over 100,000 simulations for different percentages of deleted edges. Exact data points from the simulations and regression curves (polynomial of degree 8) are plotted. The results for edge centrality-based 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 randomized edge removals are newly conducted for each of the 100,000 simulations. [Color figure can be viewed at wileyonlinelibrary.com]

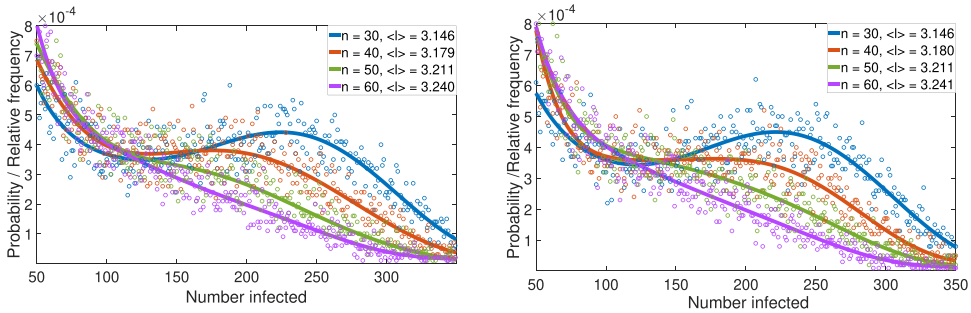

FIGURE 12 Final outbreak size frequencies given an initial infection of a single network node, over 100,000 simulations for different numbers of splitted nodes. Exact data points from the simulations and regression curves (polynomial of degree 8) are plotted. The results for degree-based splittings are depicted in the left figure, the number of critical splits is found to be about $n = 60$ which corresponds to 6% of the nodes. Very similar results are found when splitting nodes according to their betweenness centrality, as is shown in the right figure. [Color figure can be viewed at wileyonlinelibrary.com]

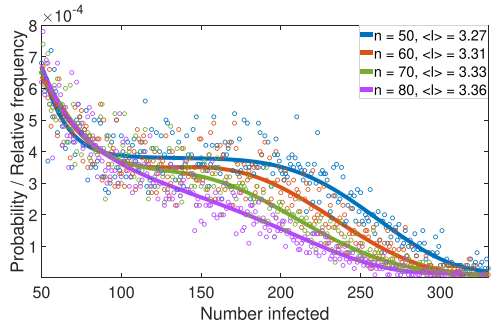

FIGURE 13 Final outbreak size frequencies given an initial infection of a single network node, over 100,000 simulations for different numbers of split nodes under the modified procedure. Exact data points from the simulations and regression curves (polynomial of degree 8) are plotted. In comparison to the results from Figure 12, we see that the modified rewiring procedure substantially reduces the procedure's efficiency. Indeed, in this case, 8% of the nodes need to be splitted and the corresponding network functionality is $\langle l \rangle = 3.36$. [Color figure can be viewed at wileyonlinelibrary.com]

Further, the functionality of $\langle l \rangle \approx 3.24$ of the resulting network is better than in the case of edge removals ($\langle l \rangle \approx 3.30$).

In step 3, (iii) of the algorithm, rewiring of edges is conducted with the aim of separating critical contagion channels from each other. To study the effectiveness of the procedure, we may modify this step of the algorithm in the following way: Let k_i denote the degree of node i. Then, the $\lceil k_i/2 \rceil$ neighbors with highest degree remain connected to i, and only edges between the $\lfloor k_i/2 \rfloor$ lowest degree nodes and i are rewired from node i to j. From the outcomes in Figure 13, we clearly observe that the effectiveness of the node splitting procedure is now remarkably lowered, both in terms of necessary node splits for the prevention of cyber pandemics and network functionality. Hence, the separation of critical contagion channels is essential for the effective implementation of node splitting.

5.2.2 | Risk allocation and design of contractual obligations

Risk allocation: Consider an initial graph G and the graph G_c which is obtained by network interventions, either edge removals or node splitting, such that cyber pandemics are sufficiently controlled in G_c. The network connections in G_c can be considered *acceptable*, that is, they should not warrant further regulatory action. Instead, suitable risk allocation schemes and possible obligations should be derived from the set of *deleted* (edge removals) or *rewired* (node splitting) connections. To allocate the cyber pandemic risk to the individual nodes in accordance with their systemic risk contribution, we thus introduce the concept of *contact coefficients*:

- *Edge removals:* Let $\epsilon_i = |\{j|(i,j) \in \mathcal{E}_c\}|$ denote the number of critical connections of node i.[24] To measure the cyber pandemic risk contribution of the single node i, we define the contact coefficient c_i of i by

[24]Note that every critical edge $(i,j) \in \mathcal{E}_c$ connects two nodes i and j, thus $\sum_{i=1}^{N} \epsilon_i = 2|\mathcal{E}_c|$.

$$c_i = \frac{\epsilon_i}{2|\mathcal{E}_c|}, \text{ normalized to } \sum_{i=1}^{N} c_i = 1.$$

- *Node splitting:* Let $\mathcal{I} \subseteq \{1, ..., N\}$ denote the set of nodes from the initial network G which are splitted during the procedure. Then, in analogy to the centrality weights w_i from Case Study I, we choose a node centrality measure $\mathcal{C}$ and define the contact coefficient c_i by

$$c_i = \begin{cases} \left(\mathcal{C}(i)/\sum_{j\in\mathcal{I}}\mathcal{C}(j)\right), & \text{if } i \in \mathcal{I}, \\ 0, & \text{else.} \end{cases}$$

In the following, we sketch preliminary ideas on how specific topology-based obligations for network nodes i could be established.

Contractual obligations: A major problem of (private) regulators such as insurance companies is that they might not be able to directly control or limit connections within cyber networks. In that case, contractual obligations, like surcharges or insurance risk premiums, may incentivize the deletion or protection of critical contagion channels. In the following, we briefly discuss such insurance-related obligations.

- *Fixed surcharge:* Given a cyber premium $\pi_i \in \mathbb{R}_+$ for node i, not yet accounting for systemic cyber risks, the contact coefficient c_i could serve to determine the fraction of a fixed systemic risk surcharge $f > 0$ which has to be borne by node i. This means that node i's total premium would equal

$$\widetilde{\pi}_i = \pi_i + c_i \cdot f \geq \pi_i,$$

  with equality if and only if $c_i = 0$, that is, if and only if node i possesses no critical network connections. For example, these surcharges could be implemented in the context of the insurance backstop mechanism that is discussed in Lemnitzer (2021).
- *Risk premia:* Let L represent the random total loss (over all nodes) in the original network G, and let L_c represent the total loss in the new network G_c. Then $L_e := L - L_c$ may be interpreted as the cyber pandemic loss. Consider a risk measure ρ such as the Value at Risk or Expected Shortfall[25] and let $\rho(L_e)$ denote the corresponding risk capital. When $\rho(L_e) > 0$ we define a topology-based premium $\pi(c_i)$ for each node i by allocating the risk capital $\rho(L_e)$ among the policyholders according to their individual risk contribution. For fixed networks G and G_c, the corresponding function $\pi : [0, 1] \to [0, \rho(L_e)]$ should be nondecreasing and satisfy $\sum_{i=1}^{N}\pi(c_i) = \rho(L_e)$. This amounts to a classical risk allocation problem, see, for example, Feinstein et al. (2017). Obviously, the proportional allocation rule

$$\pi(c_i) = c_i \cdot \rho(L_e)$$

  satisfies these constraints.

[25]For a rigorous introduction to monetary risk measures, we refer the interested reader to Föllmer and Schied (2016, sec. 4).

Using edge-removal interventions, we illustrate the effect of these mechanisms in Figure 14 for the Barabási–Albert network from Figure 9. The larger the size of a node in Figure 14, the larger is its underlying contact coefficient c_i, and, thus, the higher would be an adequate topology-based obligation. We find that critical network connections are mostly associated to a few central hubs. Comparing Figures 9 and 14, these few hubs are even more important than from a degree perspective, and their decisive meaning for the emergence of cyber pandemic risk within the network is clearly observed. Thus, adequate topology-based interventions should target these few central pandemic nodes.

5.3 | Evaluation of topology-based interventions

The case study clearly demonstrates that effective manipulations of the network topology can prevent cyber pandemic outbreaks while preserving a reasonable level of network functionality. We obtain the following insights:

(i) In homogeneous networks of large size, connectivity, defined in terms of the sole number of links, plays a major role in the emergence of cyber pandemic risk: A critical connectivity threshold p_c can be identified, below which the frequency of cyber pandemics is negligible. Further, it is possible to prevent cyber pandemics by increasing the overall network security.

(ii) However, many real-world networks are characterized by a more heterogeneous, *scale-free* distribution of node degrees. Examples of networks with a scale-free topology can be modeled using the Barabási–Albert model. Here, we found that highly connected network participants (hubs) may further *amplify* risk propagation compared to homogeneous networks. Moreover, in the limit of infinite network size, cyber pandemics cannot solely be prevented by strengthening the security of network participants but requires manipulating the degree distribution of the underlying network topology.

(iii) *Centrality* and *contact coefficients* are an effective way to measure an agent's relative topological importance and allocate the cyber pandemic risk of the system to its individual nodes. Regulation taking into account these parameters may significantly reduce the cyber risk and simultaneously preserve a high level of network functionality. However, determining these coefficients requires information on the *full network topology*.

(iv) In contrast to security-related measures, which should target all large and medium-scale entities, topology-based interventions only need to focus on a small group of highly central

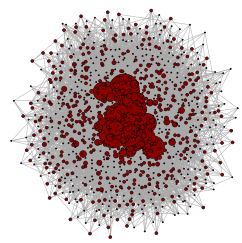

FIGURE 14 Visualization of contact coefficients based on edge removals in the Barabási–Albert network introduced in Figure 9: Here, node size of node i equals $100 \cdot \sqrt{c_i / \sum_{j=1}^{1000} c_j}$, an increasing function of the node's importance with respect to its contact coefficient c_i. [Color figure can be viewed at wileyonlinelibrary.com]

nodes. Thus, while contact coefficients might be difficult to determine in practice, it is sufficient to impose obligations, like mandatory backup servers, the protection of data connections, and separation of contagion channels, on a small fraction of highly interconnected network entities. Due to their size and importance, these nodes are more likely to be identified.

We identify the following implications for the cyber resilience measures discussed in Section 2:

GOV ◇ *Incident response and reporting*: The implementation of early warning systems and reporting obligations for strongly connected network entities may be an effective way to prevent large-scale events. Immediately disconnecting or otherwise securing these agents after risk arrival may be crucial to prevent the outbreak of a systemic incident. Further, network scanning should evaluate the risk of cyber pandemic outbreaks; in particular, contact coefficients and the analysis of edge removal or node splitting procedures may help to give concrete advice for the design of a more resilient network topology.

◇ *Critical supply chains*: Network topology characteristics of industry supply chains should play a major role in risk assessment and resilience building. Highly interconnected entities, cloud service platforms, or frequently used software may pose a severe threat for production chains and industry sectors.

INS ◇ *Contact liability premiums*: The systemic risk contribution of a policyholder to the insurers portfolio could be evaluated by means of contact coefficients as introduced in Section 5.2.2.

◇ *Insurance backstop mechanism*: Our approach provides a reasonable allocation mechanism for mandatory surcharges after the appearance of a systemic cyber risk incident. Further, it may help encourage the deletion or protection of critical network connections and thereby reduce the existing risk potential.

6 | CONCLUSION AND OUTLOOK

As systemic cyber risks such as the well-known WannaCry and NotPetya incidents pose a growing threat to social and economic stability around the world, risk management and resilience building are increasingly becoming the focus of regulators and private actors. In this context, major issues arise from the limited amount of incident data available and the ever-evolving threat landscape.

Following the digital twin paradigm, we tackle this issue by introducing the *artificial cyber lab*: Based on data from virtual counterparts of real-world cyber systems, the artificial cyber lab provides an experimental framework to analyze the impact of both *security-related* and *topology-based* interventions. We find that both types can significantly improve the resilience of interconnected cyber systems—if they are well-adapted to the topology of the underlying cyber network: In the context of security-related interventions, appropriate obligations can be

successfully implemented if, in addition to regulating highly centralized entities, they also apply to medium-sized network players. Additionally, topology-based measures for preventing cyber pandemic outbreaks in large-scale heterogeneous networks are essential. These constitute a rather serious regulatory intervention in cyber systems compared to security-related obligations. However, these interventions may be justified because only a small portion of highly centralized nodes need to be affected. Based on our analysis of a virtual counterpart of the real world, digital networks might become more resilient against systemic cyber threats by implementing the discussed cyber resilience measures.

Of course, our specific case studies are highly stylized, and the validity of results depends on the appropriateness of the chosen framework. Possible modifications and extensions of the lab environment may be:

- *Attackers and insurers as strategic actors*: A limitation of our approach is that we have not yet considered in detail the reactions and objectives of the actors involved, for example, the reaction of malicious actors to the implementation of novel measures, or the impact of information asymmetries in the relationships between insurers and policyholders. Our approach is a first step toward combining strategic approaches and dynamic cyber risk models. Future research should seek to incorporate these strategic aspects into the modeling framework.
- *Data gathering and model uncertainty*: Based on artifical lab data, our study is able to provide insights on critical aspects of building cyber resilience—in a *qualitative* sense. However, to determine what *exact* degree of constraints might be appropriate in reality, the input parameters of our mathematical cyber risk model need to be fitted to real-world data to establish additional data links between the virtual and real-world components of our digital twin. Therefore, gathering data about network topologies and cyber incidents remains an important task for regulatory authorities, risk management agencies, and insurance companies.[26] Additionally, considering risk management methods under model uncertainty may be necessary to robustify the lab framework.
- *Network size and complexity*: Of course, the computational complexity of algorithms applied within the artificial cyber lab significantly increases with the number of network nodes and edges. However, our studies indicate that an effective risk assessment can be achieved by focusing on the most central parts of the network only. Hence, a possible way to overcome complexity issues could be to artificially reduce the size of the network subject to preserving important characteristics. For instance, large real-world networks could be downsized by merging the peripheral parts to a tractable number of nodes. The suitability of such approaches is part of future research.
- *Feedback mechanisms in dynamic and adaptive networks*: Over the course of an ongoing contagious cyber incident, nodes may in turn react to the threat evolution dynamics by link activation, shift, or deletion. For example, in response to the downfall of a server, new links may be created to servers which are still operational. Models for dynamic and adaptive networks with link rewiring, activation, and deletion are extensively discussed in Masuda and Holme (2017) and Kiss et al. (2017, chap. 8).

This list of future research and modeling perspectives is not exhaustive. Moreover, new aspects of cyber risk will emerge over time as cyber technology evolves. Nevertheless, artificial

[26]A brief survey on statistical inference methods for network topologies and/or epidemic model parameters is presented in Awiszus et al. (2023, Appendix E). Further, in Hillairet et al. (2022), a macroeconomic network model with weighted edges was calibrated from OECD data on the economic flow between industry sectors.

cyber labs are a promising tool for analyzing and understanding threats—supporting the evaluation of potential countermeasures when building a more resilient cyber landscape for the future.

ACKNOWLEDGEMENTS

Open Access funding enabled and organized by Projekt DEAL.

REFERENCES

Aliprantis, C. D., & Border, K. C. (2006). *Infinite dimensional analysis* (3rd ed.). Springer.

Allianz (2022). *Allianz risk barometer*. Technical report. Allianz Global Corporate & Specialty.

Antonio, Y., Indratno, S. W., & Simanjuntak, R. (2021). Cyber insurance ratemaking: A graph mining approach. *Risks*, *9*(12), 224.

Awiszus, K., Knispel, T., Penner, I., Svindland, G., Voß, A., & Weber, S. (2023). Modeling and pricing cyber insurance. *European Actuarial Journal*, *13*, 1–53.

Barabási, A.-L., & Albert, R. (1999). Emergence of scaling in random networks. *Science*, *286*, 509–512.

Barabási, A.-L., & Pósfai, M. (2016). *Network science*. Cambridge University Press.

Böhme, R., Laube, S., & Riek, M. (2018). A fundamental approach to cyber risk analysis. *Variance*, *2*, 161–185.

Böhme, R., & Schwartz, G. (2010). *Modeling cyber-insurance: Towards a unifying framework*. Workshop on the Economics of Information Security (WEIS).

Bolot, J., & Lelarge, M. (2009). Economic incentives to increase security in the Internet: The case for insurance. In *Proceedings of the 28th Conference on Computer Communications, Rio de Janeiro, Brazil* (pp. 1494–1502).

Brémaud, P. (1999). *Markov chains. Gibbs fields, Monte Carlo simulation, and queues* (Vol. 31). Texts in Applied Mathematics. Springer.

BSI. (Ed.). (2022). *IT-Grundschutz-Kompendium*. Bundesamt für Sicherheit in der Informationstechnik. Reguvis.

Chen, H., Cummins, J. D., Sun, T., & Weiss, M. A. (2020). The reinsurance network among U.S. property-casualty insurers: Microstructure, insolvency risk, and contagion. *Journal of Risk and Insurance*, *87*(2), 253–284.

Chen, H., & Sun, T. (2020). Tail risk networks of insurers around the globe: An empirical examination of systemic risk for G-SIIs vs non-G-SIIs. *Journal of Risk and Insurance*, *87*(2), 285–318.

Chen, Z., Tong, H., & Ying, L. (2018). Realtime robustification of interdependent networks under cascading attacks. In *2018 IEEE International Conference on Big Data (Big Data)* (pp. 1347–1356).

Chernikova, A., Gozzi, N., Boboila, S., Angadi, P., Loughner, J., Wilden, M., Perra, N., Eliassi-Rad, T., & Oprea, A. (2022). Cyber network resilience against self-propagating malware attacks. In V. Atluri, R. Di Pietro, C. D. Jensen, & W. Meng (Eds.), *Computer security—ESORICS 2022* (pp. 531–550). Springer International Publishing.

Chiaradonna, S., Jevtic, P., & Lanchier, N. (2023). Framework for cyber risk loss distribution of hospital infrastructure: Bond percolation on mixed random graphs approach. *Risk Analysis*, 1–36.

Dacorogna, M., & Kratz, M. (2023). Managing cyber risk, a science in the making. *Scandinavian Actuarial Journal*, 1–22.

EIOPA. (2022). *Discussion paper on methodologies of insurance stress testing—Cyber component*. European Insurance and Occupational Pensions Authority.

Eling, M. (2020). Cyber risk research in business and actuarial science. *European Actuarial Journal*, *10*(2), 303–333.

Erdős, P., & Rényi, A. (1959). On random graphs I. *Publicationes Mathematicae Debrecen*, *6*, 290–297.

ESRB. (Ed.). (2020). *Systemic cyber risk*. European Systemic Risk Board.

Fahrenwaldt, M. A., Weber, S., & Weske, K. (2018). Pricing of cyber insurance contracts in a network model. *ASTIN Bulletin: The Journal of the IAA*, *48*(3), 1175–1218.

Feinstein, Z., Rudloff, B., & Weber, S. (2017). Measures of systemic risk. *SIAM Journal on Financial Mathematics*, *8*(1), 672–708.

Föllmer, H. (1974). Random economies with many interacting agents. *Journal of Mathematical Economics*, *1*(1), 51–62.

Föllmer, H., & Schied, A. (2016). *Stochastic finance: An introduction in discrete time* (4th ed.). Walter de Gruyter.

Freitas, S., Wicker, A., Chau, D. H. P., & Neil, J. (2020). D^2M: Dynamic defense and modeling of adversarial movement in networks. In *Proceedings of the 2020 SIAM International Conference on Data Mining (SDM)* (pp. 541–549).

Freitas, S., Yang, D., Kumar, S., Tong, H., & Chau, D. H. (2022). Graph vulnerability and robustness: A survey. *IEEE Transactions on Knowledge and Data Engineering*, *35*(6), 5915–5934.

Gatzert, N., & Schubert, M. (2022). Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value. *Journal of Risk and Insurance*, *89*(3), 725–763.

GDV. (2017). *Allgemeine Versicherungsbedingungen für die Cyberrisiko-Versicherung (AVB Cyber), Musterbedingungen des GDV*. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV).

GDV. (2019). *Unverbindlicher Muster-Fragebogen zur Risikoerfassung im Rahmen von Cyber-Versicherungen für kleine und mittelständische Unternehmen*. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV).

Giesecke, K., & Weber, S. (2004). Cyclical correlations, credit contagion, and portfolio losses. *Journal of Banking and Finance*, *28*(12), 3009–3036.

Giesecke, K., & Weber, S. (2006). Credit contagion and aggregate losses. *Journal of Economic Dynamics and Control*, *30*(5), 741–767.

Gillespie, D. T. (1976). A general method for numerically simulating the stochastic time evolution of coupled chemical reactions. *Journal of Computational Physics*, *22*(4), 403–434.

Gillespie, D. T. (1977). Exact stochastic simulation of coupled chemical reactions. *The Journal of Physical Chemistry*, *81*(25), 2340–2361.

Girvan, M., & Newman, M. E. J. (2002). Community structure in social and biological networks. *Proceedings of the National Academy of Sciences of the United States of America*, *99*(12), 7821–7826.

Hayel, Y., Trajanovski, S., Altman, E., Wang, H., & Van Mieghem, P. (2014). Complete game-theoretic characterization of sis epidemics protection strategies. In *53rd IEEE Conference on Decision and Control* (pp. 1179–1184).

Herr, T. (2021). Cyber insurance and private governance: The enforcement power of markets. *Regulation & Governance*, *15*(1), 98–114.

Hillairet, C., & Lopez, O. (2021). Propagation of cyber incidents in an insurance portfolio: Counting processes combined with compartmental epidemiological models. *Scandinavian Actuarial Journal*, *2021*(8), 1–24.

Hillairet, C., Lopez, O., d'Oultremont, L., & Spoorenberg, B. (2022). Cyber-contagion model with network structure applied to insurance. *Insurance: Mathematics and Economics*, *107*, 88–101.

Hurel, L. M., & Lobato, L. C. (2018). Unpacking cyber norms: Private companies as norm entrepreneurs. *Journal of Cyber Policy*, *3*(1), 61–76.

Jevtić, P., & Lanchier, N. (2020). Dynamic structural percolation model of loss distribution for cyber risk of small and medium-sized enterprises for tree-based lan topology. *Insurance: Mathematics and Economics*, *91*, 209–223.

Jones, D., Snider, C., Nassehi, A., Yon, J., & Hicks, B. (2020). Characterising the digital twin: A systematic literature review. *CIRP Journal of Manufacturing Science and Technology*, *29*, 36–52.

Kermack, W. O., & McKendrick, A. G. (1927). A contribution to the mathematical theory of epidemics. *Proceedings of the Royal Society of London. Series A*, *115*, 700–721.

Kiss, I. Z., Miller, J. C., & Simon, P. L. (2017). *Mathematics of epidemics on networks. From exact to approximate models* (Vol. 46). Interdisciplinary Applied Mathematics. Springer.

Lagarde, C. (2021). Macroprudential policy in Europe—The future depends on what we do today. In *Welcome remarks by Christine Lagarde, President of the ECB and Chair of the European Systemic Risk Board, at the Fifth Annual Conference of the ESRB*.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248.

Lemnitzer, J. M. (2021). Why cybersecurity insurance should be regulated and compulsory. *Journal of Cyber Policy*, *6*(2), 118–136.

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*, *24*, 35–61.

Masuda, N., & Holme, P. (Eds.). (2017). *Temporal network epidemiology*. Theoretical Biology. Springer.

Mieghem, P. V. (2014). *Performance analysis of complex networks and systems*. Cambridge University Press.
Naghizadeh, P., & Liu, M. (2014). Voluntary participation in cyber-insurance markets. In *Proceedings of the 2014 Annual Workshop on Economics in Information Security*.
Newman, M. E. J. (2018). *Networks* (2nd ed.). Oxford University Press.
NIST. (2022). *Glossary of the National Institute of Standards and Technology*. Retrieved May 27, 2022 from https://csrc.NIST.gov/glossary
Ogut, H., Menon, N., & Raghunathan, S. (2005). Cyber insurance and it security investment. In *Proceedings of the 4th Workshop on the Economics of Information Security*.
Pal, R., Golubchik, L., Psounis, K., & Hui, P. (2014). Will cyber insurance improve network security? A market analysis. In *Proceedings of the 2014 INFOCOM*, IEEE.
Pastor-Satorras, R., Castellano, C., Van Mieghem, P., & Vespignani, A. (2015). Epidemic processes in complex networks. *Reviews of Modern Physics*, *87*, 925–979.
Price, D. d. S. (1965). Networks of scientific papers. *Science*, *149*(3683), 510–515.
Price, D. d. S. (1976). A general theory of bibliometric and other cumulative advantage processes. *Journal of the American Society for Information Science*, *27*(5), 292–306.
Schwartz, G. A., & Sastry, S. S. (2014). Cyber-insurance framework for large scale interdependent networks. In *Proceedings of the 3rd International Conference on High Confidence Networked Systems* (pp. 145–154).
Sievers, T. (2021). Proposal for a NIS directive 2.0: Companies covered by the extended scope of application and their obligations. *International Cybersecurity Law Review*, *2*, 223–231.
Sweetman, A. (2022). *Cyber and the city. Securing London's banks in the computer age*. History of Computing. Springer.
Talesh, S. A. (2018). Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses. *Law & Social Inquiry*, *43*(2), 417–440.
TeleTrusT. (Ed.). (2021). *Guideline "State of the Art"*. TeleTrusT—IT Security Association Germany. In cooperation with ENISA.
Trang, M. N. (2017). Compulsory corporate cyber-liability insurance: Outsourcing data privacy regulation to prevent and mitigate data breaches. *Minnesota Journal of Law, Science & Technology*, *18*(1), 8.
Tumminello, M., Consiglio, A., Vassallo, P., Cesari, R., & Farabullini, F. (2023). Insurance fraud detection: A statistically validated network approach. *Journal of Risk and Insurance*, *90*(2), 381–419.
Woods, D. W., & Moore, T. (2020). Does insurance have a future in governing cybersecurity? *IEEE Security & Privacy*, *18*(1), 21–27.
Xu, M., & Hua, L. (2019). Cybersecurity insurance: Modeling and pricing. *North American Actuarial Journal*, *23*(2), 220–249.
Yang, Z., & Lui, J. (2014). Security adoption and influence of cyber-insurance markets in heterogeneous networks. *Performance Evaluation*, *74*, 1–17.
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*, 33–85.
Zeller, G., & Scherer, M. (2023). Is accumulation risk in cyber systematically underestimated? Working Paper, available at SSRN.

How to cite this article: Awiszus, K., Bell, Y., Lüttringhaus, J., Svindland, G., Voß, A., & Weber, S. (2023). Building resilience in cybersecurity: An artificial lab approach. *Journal of Risk and Insurance*, 1–48. https://doi.org/10.1111/jori.12450

APPENDIX A: MARKOVIAN SIR DYNAMICS

Continuous-Time Markov Chains: In Markovian spread models on networks of N nodes, the evolution of the state vector $X(t)$

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

is described by a continuous-time Markov chain on the discrete state space E^N. E is the *compartment set* of possible single-node states. We assume that the Markov chain is *time-homogeneous*, that is, that the probability of changing from state $x \in E^N$ to state $y \in E^N$ within a time window of length $t > 0$ does not depend on the current time u

$$P_{xy}(t) := \mathbb{P}(X(u+t) = y | X(u) = x) = \mathbb{P}(X(t) = y | X(0) = x), \quad u > 0.$$

These probabilities constitute the $|E|^N \times |E|^N$ *transition probability matrix* $P(t) = (P_{xy}(t))$ with $\sum_{y \in E^N} P_{xy}(t) = 1$. For $t = 0$, it is consistent to assume that $P(0) = \lim_{t \searrow 0} P(t)$ equals the $|E|^N \times |E|^N$-dimensional identity matrix. Then $P(t)$ is continuous for all $t \geq 0$ and satisfies the *Chapman–Kolmogorov equation*

$$P(t+u) = P(u)P(t) = P(t)P(u). \tag{A1}$$

The transition probabilities $P(t)$ fully characterize the evolution of a continuous-time Markov chain. For practical purposes, however, they provide too much information. Hence, we will focus on infinitesimal transition probabilities instead.

The continuity of $P(t)$ implies that the derivative matrix

$$Q := P'(0) = \lim_{h \searrow 0} \frac{P(h) - P(0)}{h}$$

exists.[27] Q is called the *infinitesimal generator* of the process, and its entries q_{xy} are called *transition rates* since they describe the probability per unit time of a transition from state x to state y. Using the Chapman–Kolmogorov equation (A1), the evolution of the complete process $(X(t))_{t \geq 0}$ can be described by its infinitesimal generator Q via the *Kolmogorov forward* and *backward equations*

$$P'(t) = P(t)Q \quad \text{and} \quad P'(t) = QP(t). \tag{A2}$$

The latter matrix differential equation is solved by the matrix exponential $P(t) = e^{Qt}$, that is, the transition probabilities can directly be retrieved from the infinitesimal transition rates. Moreover, this solution implies that the *holding time* T_x, that is, the waiting time for leaving state $x \in E^N$, is exponentially distributed with parameter $q_x := \sum_{y \in E^N, y \neq x} q_{xy} = -q_{xx} \geq 0$. In addition, the Markov property of $(X(t))_{t \geq 0}$ implies the independence of holding times.[28]

SIR dynamics: The SIR spread process is determined by $X_i(t) \in E = \{S, I, R\}$. A transition of X from one state in E^N to another is only possible if exactly one node changes its state X_i in E. State changes can occur through infection or recovery: It is assumed that each node may be infected by its infected neighbors, but can be cured independently of all other nodes in the

[27] see Brémaud (1999, theorem 2.1).

[28] For details see, for example, Mieghem (2014, chap. 10). We refer to this book for more in-depth reading on stochastic processes and complex networks.

network. Transitions are depicted in Figure 2. Formally, the entries of the infinitesimal generator Q are given by

$$q_{xy} = \begin{cases} \gamma_i, & \text{if } x_i = I, y_i = R, \text{ and } x_j = y_j \text{ for } j \neq i \\ \tau \sum_{j=1}^{N} a_{ij} \mathbb{1}_{x_j = I}, & \text{if } x_i = S, y_i = I, \text{ and } x_j = y_j \text{ for } j \neq i \\ -\sum_{z \in E^N, z \neq x} q_{xz}, & \text{if } x = y \\ 0, & \text{otherwise.} \end{cases} \tag{A3}$$

Of particular interest are the dynamics of the state probabilities of individual nodes $\mathbb{P}(X_i(t) = x_i)$, $t \geq 0$. They can be derived from Kolmogorov's forward equation and written in general form as $(i = 1, ..., N)$

$$\frac{d\mathbb{P}(X_i(t) = x_i)}{dt} = \sum_{y: y_i = x_i} \sum_{z \neq y} [\mathbb{P}(X(t) = z) q_{zy} - \mathbb{P}(X(t) = y) q_{yz}], \tag{A4}$$

where q_{zy} denotes the transition rate of the entire process X from $z \to y$. Using Bernoulli random variables $S_i(t) := \mathbb{1}_{\{X_i(t)=S\}}$, $I_i(t) := \mathbb{1}_{\{X_i(t)=I\}}$, and $R_i(t) := \mathbb{1}_{\{X_i(t)=R\}}$, the dynamics of state probabilities of individual nodes (A4) can conveniently be written via moments[29]:

$$\begin{aligned} \frac{d\mathbb{E}[S_i(t)]}{dt} &= -\tau \sum_{j=1}^{N} a_{ij} \mathbb{E}[S_i(t) I_j(t)], \\ \frac{d\mathbb{E}[I_i(t)]}{dt} &= \tau \sum_{j=1}^{N} a_{ij} \mathbb{E}[S_i(t) I_j(t)] - \gamma_i \mathbb{E}[I_i(t)], \\ \frac{d\mathbb{E}[S_i(t) I_j(t)]}{dt} &= \tau \sum_{k=1, k \neq i}^{N} a_{jk} \mathbb{E}[S_i(t) S_j(t) I_k(t)] - \tau \sum_{k=1, k \neq j}^{N} a_{ik} \mathbb{E}[I_k(t) S_i(t) I_j(t)] \\ &\quad - \tau a_{ij} \mathbb{E}[S_i(t) I_j(t)] - \gamma_j \mathbb{E}[S_i(t) I_j(t)], \\ \frac{d\mathbb{E}[S_i(t) S_j(t)]}{dt} &= -\tau \sum_{k=1, k \neq j} a_{ik} \mathbb{E}[I_k(t) S_i(t) S_j(t)] - \tau \sum_{k=1, k \neq i}^{N} a_{jk} \mathbb{E}[S_i(t) S_j(t) I_k(t)], \end{aligned} \tag{A5}$$

where $i, j = 1, 2, ..., N$ and $i \neq j$.

Note that system (A5) is *not closed*: The dynamics of second-order moments depend on third-order moments, which, in turn, depend on fourth-order moments, and so on. This dependence structure cascades up to network size N. Therefore, in general, solving the exact system of moment equations becomes intractable, especially for larger networks. To deal with this issue, the following two approximation approaches have been proposed:

1. **Monte Carlo simulation:** Monte Carlo simulation using the Gillespie algorithm from Gillespie (1976) and Gillespie (1977) constitutes a powerful tool to obtain various quantity estimates related to the evolution of the epidemic spread. Pseudocode is

[29]The dynamics of the recovery Bernoulli random variable $R_i(t)$ result from the dynamics of $I_i(t)$ and $S_i(t)$ due to $\mathbb{E}[R_i(t)] = 1 - \mathbb{E}[S_i(t)] - \mathbb{E}[I_i(t)]$.

given in Appendix B, and further explanations of the Gillespie algorithm applied to SIR epidemic network models is, for example, given in Kiss et al. (2017, appendix A.1.1).

2. **Moment closures:** If a set of nodes J is infected, this increases the probability of other nodes in the network (that are connected to the set J via an existing path) to become infected as well. Hence, node states are to some extent *correlated*. To break the cascade of equations and to make ordinary differential equation systems tractable, the moment closure approach consists in assuming independence at a certain order k, neglecting any further correlations. This is done by considering the exact moment equations up to this order k and *closing* the system by approximating moments of order $k+1$ in terms of products of lower-order moments using a mean-field function. However, a *major problem* with moment closures is that only little is known about rigorous error estimates.

APPENDIX B: GILLESPIE ALGORITHM

Algorithm (Gillespie).

Input: Initial state of the system $x^0 \in E^N$ and initial time $t_0 \geq 0$.

1. *(Initialization)* Set the current state $x \to x^0$, current time $t \to t_0$, and $k \to 0$.
2. *(Rate Calculation)* For the current state of the system x, calculate the sum of rates for all possible transitions $q_x = \sum_{i=1}^{N} q_{x_i}$, where q_{x_i} denotes the rate for a state change of node i according to (A3).
3. *(Generate Next Event Time)* Sample the next event time t_{new} from an exponential distribution with parameter q_x.
4. *(Choose Next Event)* Sample the node i_{new} at which the next transition occurs: Each node $i = 1, ..., N$ is chosen with probability q_{x_i}/q_x.

   Change the state $x_{i_{\text{new}}} \to y_{i_{\text{new}}}$ according to (A3).
5. Set $t \to t + t_{\text{new}} =: t_{k+1}$, $x \to (x_1, ..., x_{i_{\text{new}}-1}, y_{i_{\text{new}}}, x_{i_{\text{new}}+1}, ..., x_N) =: x^{t_{k+1}}$, $k \to k+1$, and return to Step 2 until a prespecified stopping criterion is met.

Output: Trajectory $[t_0, t_{end}] \ni t \to X(t, \omega)$ of the spread process, where $X(t, \omega) := x^{t_k}$ for $t \in [t_k, t_{k+1}]$; t_{end} denotes the end time of the simulation

APPENDIX C: NETWORK ALGORITHMS

Algorithm (Erdős-Rényi).

Input: Number of network nodes N, connection probability p.

1. Choose a pair of nodes (i, j) with $i, j \in \{1, ..., N\}$, $i \neq j$.
2. Simulate a uniformly distributed number $\tilde{p}$ between 0 and 1.
3. If $\tilde{p} < p$, create an edge between node i and j. Else, no edge is created.
4. Repeat steps 1)–3) for all the other possible pairs of nodes.

Output: Network G from class $G_p(N)$

Algorithm (Barabási-Albert).

Input: Number of network nodes N, small initial network of n_0 connected nodes, number m of nodes to which every newly added node is connected.

1. Add a new node i to the small initial network.
2. Create a new edge for i in the following way:
   i) Uniformly generate a node number j from the existing network ($i \neq j$).
   ii) Simulate a uniformly distributed number r between 0 and 1.
   iii) Let k_l denote the current degree of node $l, l = 1, \ldots N$. If $r < k_j / \sum_i k_l$, then the edge should be created between i and j. Else, go back to step i).
3. Repeat step 2) until m edges are created for the new node i.
4. Repeat steps 1)–3) until a network of N nodes is formed.

Output: Network G from class $BA(N; m)$

APPENDIX D: L_i AS A STRICTLY CONVEX FUNCTION OF γ_i

For our cyber loss model

$$L_i := L_i(\gamma_1, ..., \gamma_N) := \mathbb{E}\left[\int_0^\infty I_i(t)dt\right],$$

we can derive an elegant expression in terms of γ_i: Let $A_i := \{\exists\ t \in [0, \infty) : I_i(t) = 1\}$ be the event that node i will be infected at some moment in time t. Then

$$L_i = \mathbb{E}\left[\int_0^\infty I_i(t)dt \mathbb{1}_{A_i}\right] + \mathbb{E}\left[\int_0^\infty I_i(t)dt \mathbb{1}_{A_i^c}\right]$$

where $\int_0^\infty I_i(t)dt \mathbb{1}_{A_i^c} = 0$ by definition. Note that γ_i only affects the recovery process of node i, and since reinfection events are ruled out in the SIR modeling framework, the probability of infection $\mathbb{P}(A_i)$ for node i does not depend on the recovery rate of node i but only on the vector γ_{-i} of the other node's recovery rates.

Further, since the initial infections are randomly chosen, we have $\mathbb{P}(A_i) \geq 1/N$. Thus, by using the rules of conditional expectation, L_i can be expressed as

$$L_i = \mathbb{E}\left[\int_0^\infty I_i(t)dt \mathbb{1}_{A_i}\right] = \mathbb{P}(A_i) \cdot \mathbb{E}\left[\int_0^\infty I_i(t)dt \middle| A_i\right].$$

By definition, $\int_0^\infty I_i(t)dt$ is the amount of time i spends in the infectious state I. If an infection of node i actually occurs, then this is the time of transition from state I into state R. Hence, $\mathbb{E}\left[\int_0^\infty I_i(t)dt | A_i\right]$ is the expected waiting time for recovery of node i. Since the SIR spread process is assumed to be Markovian, the waiting time is exponentially distributed with parameter γ_i. Therefore, we obtain

$$\mathbb{E}\left[\int_0^\infty I_i(t)dt \middle| A_i\right] = \frac{1}{\gamma_i}.$$

Hence,

$$L_i(\gamma_1, ..., \gamma_N) = \frac{\mathbb{P}(A_i)}{\gamma_i} \tag{D1}$$

where the numerator does not depend on node i's recovery rate. Thus, L_i is a *strictly convex* function of γ_i.

APPENDIX E: MODELING CYBER LOSSES FOR THE SECURITY INVESTMENT GAME

The decomposition of loss functions L_i in Appendix D can be used for an efficient stochastic simulation procedure of cyber losses in Algorithm 4.2: To find the recovery rate $\gamma_i(r+1)$ for round $r+1$ in step 2 of the algorithm, we need to determine the minimizer

$$\gamma_i(r+1) = \arg\min_{\gamma_i} \mathcal{E}_i(\gamma_i, \gamma_{-i}(r)) = \arg\min_{\gamma_i} [C_i(\gamma_i) + L_i(\gamma_i, \gamma_{-i}(r))].$$

Using the aforementioned representation of the loss functions, this means that for every node i, we need to determine the infection probabilities $\mathbb{P}(A_i)$ to describe L_i as a function of γ_i. Now, since the infection probability of every node i is not depending on its own recovery rate, these probabilities can be determined in a joint procedure:

1. *Choose a sufficiently high number of simulation runs $\mathcal{T}$ to generate trajectories of the SIR process. For example, we chose $\mathcal{T} = 10{,}000{,}000$ for simulations in* Figures 5 *and* 7.
2. *For every node i, let the recovery rate be given by $\gamma_i(r)$.*
3. *For every simulation run, initially infect a randomly chosen single node and generate a trajectory of the SIR process on the network. For every node i, save whether i was infected during this run.*
4. *After the conduction of the $\mathcal{T}$ simulation runs, for every node i, let $\mathcal{T}_i$ be the number of simulation runs where node i was infected. Set $\mathbb{P}(A_i) = \mathcal{T}_i/\mathcal{T}$.*

Then, for every node i the total expenses $\mathcal{E}_i$ are solely given as a function of γ_i, and it is straightforward to determine

$$\gamma_i(r+1) = \arg\min_{\gamma_i} [C_i(\gamma_i) + \mathbb{P}(A_i)/\gamma_i].$$

APPENDIX F: PROOF OF THEOREM 4.1

Proof.

1. *Continuity of total expenses:* We prove that $\mathcal{E}_i : (0, \infty)^N \to \mathbb{R}$ is continuous. Recall that

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

where $C_i(\gamma_i) = e^{k\gamma_i} - 1$[30] and $L_i(\gamma_1, ..., \gamma_N) = \mathbb{E}\left[\int_0^\infty I_i(t)dt\right]$. Obviously, C_i is continuous. As regards L_i note that

$$L_i(\gamma_1, ..., \gamma_N) = \mathbb{E}\left[\int_0^\infty I_i(t)dt\right] = \int_0^\infty \mathbb{E}[I_i(t)]dt = \int_0^\infty \mathbb{P}(X_i(t) = I)dt$$

by the Fubini–Tonelli Theorem. Therefore, it is sufficient to prove the continuity of $\mathbb{P}(X_i(t) = I)$ in $(\gamma_1, ..., \gamma_N) \in (0, \infty)^N$. From Equation (A3), we see the the generator matrix of the SIR Markov process is continuous (w.r.t. the Frobenius norm), and therefore, the same applies to the solution $P(t) = e^{Qt}$ of the Kolmogorov backward equation. The continuity (w.r.t. the Euclidean norm) is preserved by the continuous transform

$$\mathbb{P}(X_i(t) = I) = \sum_{x \in E^N} \mathbb{P}(X(0) = x) \sum_{\substack{y \in E^N, \\ y_i = I}} P_{xy}(t)$$

of transition probability matrix $P(t)$.

2. Recall the representation (D1) $L_i(\gamma_1, ..., \gamma_N) = \frac{\mathbb{P}(A_i)}{\gamma_i}$. Hence, according to 1. also $\mathbb{P}(A_i) = \gamma_i L_i(\gamma_1, ..., \gamma_N)$ is continuous as a function of γ_{-i}.

3. Note that both C_i and L_i, and thus $\mathcal{E}_i$, are strictly convex functions of γ_i. Recalling that $\mathbb{P}(A_i)$ does not depend on γ_i, the first order condition for the unique minimum is

$$\frac{\partial}{\partial \gamma_i}\mathcal{E}_i(\gamma_1, ..., \gamma_N) = ke^{k\gamma_i} - \frac{\mathbb{P}(A_i)}{\gamma_i^2} = 0.$$

Since $\mathbb{P}(A_i)$ is continuous as a function of γ_{-i} by 2., it also follows that unique minimizer $\gamma_i^{\text{ind}}(\gamma_{-i})$ is continuous in γ_{-i}. On the one hand, note that

$$\frac{\partial}{\partial \gamma_i}\mathcal{E}_i(\gamma_1, ..., \gamma_N) = ke^{k\gamma_i} - \frac{\mathbb{P}(A_i)}{\gamma_i^2} \geq ke^{k\gamma_i} - \frac{1}{\gamma_i^2}$$

and the latter expression does not depend on γ_{-i} and is positive for, for instance, $\gamma_i > \frac{1}{\sqrt{k}}$. On the other hand, since the initial infections are randomly chosen, we have $\mathbb{P}(A_i) \geq 1/N$, and thus

$$ke^{k\gamma_i} - \frac{\mathbb{P}(A_i)}{\gamma_i^2} \leq ke^{k\gamma_i} - \frac{1}{N\gamma_i^2}$$

[30] In Case Study 1, we choose $k = \frac{1}{3}$.

where again the latter expression does not depend on γ_{-i}. Now let $\varepsilon(N) > 0$ such that $ke^{k\varepsilon(N)} - \frac{1}{N\varepsilon(N)^2} < 0$ (which always exists depending only on N). Then it follows that for any $i = 1, ..., N$ and $(\gamma_1, ..., \gamma_N) \in (0, \infty)^N$ we have $\gamma_i^{\text{ind}}(\gamma_{-i}) \in [\varepsilon(N), \frac{1}{\sqrt{k}}]$.

4. In 3. we showed that the function

$$\left[\varepsilon(N), \frac{1}{\sqrt{k}}\right]^N \to \left[\varepsilon(N), \frac{1}{\sqrt{k}}\right]^N \quad , (\gamma_1, ..., \gamma_N) \mapsto \left(\gamma_1^{\text{ind}}(\gamma_{-1}), ..., \gamma_N^{\text{ind}}(\gamma_{-N})\right)$$

is well-defined and continuous. Hence, according to Brouwer's fixed point theorem[31] it has a fixed point, that is

$$\exists\, \gamma \in \left[\varepsilon(N), \frac{1}{\sqrt{k}}\right]^N \quad \forall i = 1, ..., N: \quad \gamma_i^{\text{ind}}(\gamma_{-i}) = \gamma_i.$$

□

APPENDIX G: SECURITY CHOICES FOR A NETWORK OF TWO NODES

Straightforward exact computations of optimal investment levels are possible for the simple case of two interconnected nodes as illustrated in Figure G1.

In this special case, the infection probabilities $\mathbb{P}(A_i)$ from the loss model decomposition in Appendix D can be explicitly calculated from the waiting time distributions of the Markov chain: Due to the random uniform choice of the initially infected node, it is $\mathbb{P}(X_i(0) = I) = 1/2$ for $i = 1, 2$, and thus, we obtain

$$\begin{aligned}\mathbb{P}(A_i) &= \mathbb{P}(X_i(0) = I) + \mathbb{P}(X_j(0) = I) \cdot \mathbb{P}((S_i, I_j) \to (I_i, I_j)) \\ &= \tfrac{1}{2} \cdot (1 + \mathbb{P}((S_i, I_j) \to (I_i, I_j))), \quad i, j \in \{1, 2\}, i \neq j.\end{aligned}$$

$\mathbb{P}((S_i, I_j) \to (I_i, I_j))$ can be expressed in terms of the waiting time for recovery T_j^{recov} of node j and the infection event T^{infec}, and we can use the fact that waiting times for Markov chains are independent and exponential, yielding

$$\mathbb{P}((S_i, I_j) \to (I_i, I_j)) = \mathbb{P}\left(T_j^{\text{recov}} > T^{\text{infec}}\right) = \frac{\tau}{\gamma_j + \tau}.$$

Hence, a closed expression of the cyber losses L_i in terms of epidemic transition rates is given by

$$L_i(\gamma_1, \gamma_2) = \frac{\mathbb{P}(A_i)}{\gamma_i} = \frac{1}{2\gamma_i} \cdot \left(1 + \frac{\tau}{\gamma_j + \tau}\right), \quad i, j \in \{1, 2\}, i \neq j,$$

[31] See, for example, Aliprantis and Border (2006, corollary 17.56).

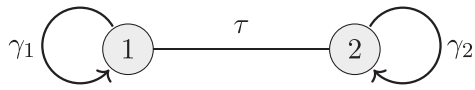

FIGURE G1 Line network with $N = 2$ nodes and the corresponding epidemic transition rates.

TABLE G1 The security investment game for a line network of $N = 2$ nodes.

r	$\gamma_i^{\text{ind}}(r)$
1	1.2234
2	1.0638
3	1.0681
4	1.0680
5	1.0680

and this can be inserted into the total expense functions $\mathcal{E}_i(\gamma_1, \gamma_2) = C(\gamma_i) + L_i(\gamma_1, \gamma_2)$.

Thus, the individual optimal security choice $\gamma_i^{\text{ind}}(r+1)$ in round $r+1$ of the security investment game is given by

$$\gamma_i^{\text{ind}}(r+1) = \arg\min_{\gamma_i} \mathcal{E}_i\left(\gamma_i, \gamma_j^{\text{ind}}(r)\right), \quad i, j \in \{1, 2\}, i \neq j.$$

Now, in agreement with the chosen parameters in Case Study 4, we fix $\tau = 0.1$ and initialize the security investment game with recovery rates $\gamma_1(0) = \gamma_2(0) = 0.1$. From Table G1, we see that the game converges to the security configuration $(\gamma_1^{\text{ind}}, \gamma_2^{\text{ind}}) = (1.068, 1.068)$ after $r = 4$ rounds.

However, from an overall network perspective, the best security configuration $(\gamma_1^{\text{soc}}, \gamma_2^{\text{soc}})$ would be the one which minimizes the accumulated total expenses $\mathcal{E}$, that is, from a social welfare perspective, the choice

$$\left(\gamma_1^{\text{soc}}, \gamma_2^{\text{soc}}\right) := \arg\min_{(\gamma_1, \gamma_2)} \sum_{k=1,2} \mathcal{E}_k(\gamma_1, \gamma_2) = (1.0984, 1.0984)$$

would be beneficial. Since $\gamma_i^{\text{ind}} \neq \gamma_i^{\text{soc}}$, this simple example illustrates that, in general, individually optimal security choices will *not* correspond to investment levels which minimize the overall network expenses.

APPENDIX H: ALLOCATION DATA

H.1. Data for upper and lower allocation strategies

See Table H1.

TABLE H1 Accumulated total expenses $\mathcal{E}$ after the allocation of the additional budget $\beta = 5$ among all network nodes.

	c^{deg}	c^{bet}	c^{inv}
Upper	19.363 (0.0030)	19.323 (0.0030)	19.460 (0.0031)
	19.444 (0.0030)	19.230 (0.0028)	19.813 (0.0032)
Lower	19.891 (0.0033)	21.551 (0.0040)	19.601 (0.0032)
	20.450 (0.0036)	21.171 (0.0039)	20.096 (0.0034)
Untargeted	19.516 (0.0031) 19.954 (0.0033)		

Note: The three proposed allocation strategies are evaluated for each of the suggested centrality measures. Entries for the Erdős-Rényi network are colored in blue (upper entries), and for the Barabási-Albert network in salmon (lower entries), respectively. Reference values without the injection of additional security are 21.66 for the Erdős-Rényi, and 21.92 for the Barabási-Albert network. For each entry, cyber losses were generated from $T = 10{,}000{,}000$ simulations of the SIR epidemic process; standard errors are given in brackets.

H.2. Data for centralized upper allocations

See Table H2.

TABLE H2 Accumulated total expenses for different percentages of targeted nodes under the upper allocation strategy for each centrality measure.

targeted	c^{deg}	c^{bet}	c^{inv}
10%	21.129 (0.0037)	21.120 (0.0036)	21.130 (0.0037)
	20.163 (0.0031)	20.214 (0.0031)	20.156 (0.0031)
20%	20.091 (0.0033)	20.152 (0.0033)	20.111 (0.0033)
	19.459 (0.0028)	19.495 (0.0028)	19.507 (0.0029)
30%	19.702 (0.0031)	19.769 (0.0031)	19.769 (0.0031)
	19.302 (0.0028)	19.311 (0.0028)	19.398 (0.0029)
40%	19.523 (0.0030)	19.554 (0.0031)	19.545 (0.0030)
	19.265 (0.0028)	19.251 (0.0028)	19.408 (0.0029)
50%	19.406 (0.0030)	19.454 (0.0030)	19.454 (0.0030)
	19.271 (0.0028)	19.233 (0.0028)	19.461 (0.0030)
60%	19.347 (0.0030)	19.367 (0.0030)	19.378 (0.0030)
	19.312 (0.0029)	19.229 (0.0028)	19.552 (0.0030)
70%	19.328 (0.0030)	19.324 (0.0030)	19.364 (0.0030)
	19.339 (0.0029)	19.227 (0.0028)	19.625 (0.0031)
80%	19.329 (0.0030)	19.319 (0.0030)	19.374 (0.0030)
	19.372 (0.0029)	19.231 (0.0028)	19.708 (0.0032)
90%	19.345 (0.0030)	19.319 (0.0030)	19.405 (0.0031)
	19.412 (0.0030)	19.233 (0.0028)	19.758 (0.0032)

Note: Again, the total additional security budget is fixed with size $\beta = 5$. Entries for the Erdős–Rényi network are colored in blue (upper entries), and for the Barabási-Albert network in salmon (lower entries), respectively. The standard error of the stochastic simulations is given in brackets. For each entry, $T = 10{,}000{,}000$ simulations of the epidemic process were generated.