Clemente, Gian Paolo, Alessandra Cornaro, and Saverio Belvedere. 2025. "Pricing Cyber Risk Insurance Coverages by Means of Epidemic Models and Network Theory." *Variance* 18 (April). https://doi.org/10.66573/001c.133587.

Risk Management

Pricing Cyber Risk Insurance Coverages by Means of Epidemic Models and Network Theory

Gian Paolo Clemente[1a], Alessandra Cornaro[2b], Saverio Belvedere[3c]

[1] Department of Mathematics for Economic, Financial and Actuarial Sciences, Milan, Italy, [2] Department of Statistics and Quantitative Methods, University of Milano – Bicocca, Italy, [3] Allianz SpA, Milan, Italy

Keywords: Cyber insurance, Epidemic models, Networks

https://doi.org/10.66573/001c.133587

Variance

Vol. 18, 2025

This paper focuses on cyber risk, an emerging threat that significantly affects numerous sectors in today's interconnected world. Among the strategies aimed at enhancing resilience and minimizing the impact of this risk, insurance contracts emerge as a potential solution. We present a heterogeneous generalized susceptible-infectious-susceptible model designed for pricing cyber risk insurance contracts. The model accurately captures the dynamics of cyber threats and evaluates the financial implications for insurance providers. It introduces an innovative method that distinguishes between critical and noncritical nodes within a network, enabling precise fortification against threats while optimizing resource allocation. Our findings show that the proposed method allows us to measure potential losses and reveals how the network's structure influences the propagation of infections. This insight can be leveraged to enhance the overall security posture of the network. A numerical analysis, simulating the network structure of a small- to medium-sized enterprise validates the effectiveness of this approach.

Address for Correspondence: alessandra.cornaro@unimib.it

1. INTRODUCTION

In an era dominated by interconnected technologies and digital dependence, the prominence of cyber risk has soared, fundamentally altering the fabric of modern society. This emergent threat not only pervades our daily lives but also poses multifaceted challenges, reshaping how we navigate security, privacy, and the very essence of our societal structures. The expanding reach of cyber vulnerabilities touches every sector, influencing businesses, governments, individuals, and critical infrastructures, which highlights the imperative need for robust strategies to mitigate and adapt to this dynamic risk landscape.

Consequently, it is imperative to structure our operations resiliently, to allow our organizations to weather such assaults with minimal damage and to ensure continuity amid compromised IT frameworks. This resilience—which involves swift detection and halting attacks, mitigating their fallout, rectifying breaches, and securing financial stability through insurance coverage—defines our ability to endure and thrive in the face of adversity (see, e.g., Dacorogna and Kratz 2022). In navigating this intricate land-

a Gian Paolo Clemente is a Ph.D. in Actuarial Science. He is an Associate Professor of Mathematical Methods in Economics, Finance, and Actuarial Sciences at the Faculty of Banking, Finance, and Insurance at Università Cattolica del Sacro Cuore, Milan. He is qualified as a Full Professor and a Fully Qualified Actuary. He is a member of the Italian National Order of Actuaries (ONA) and of the Astin Section of the International Actuarial Association. He has been a speaker at several national and international conferences and has published various papers in international scholarly journals. Details at http://docenti.unicatt.it/eng/gian_paolo_clemente/.

b Alessandra Cornaro is a Ph.D. in Quantitative Methods for Economic Analysis. She is Associate Professor in Mathematical Methods in Economics, Finance and Actuarial Sciences at the Department of Statistics and Quantitative Methods at University of Milano – Bicocca (Italy). Her research interests encompass complex systems and network theory, with a special focus on network robustness, shock propagation and risk analysis with applications in Economics, Finance and Insurance. Her work includes papers published in several academic journals and presented in national and international conferences. Details at https://en.unimib.it/alessandra-cornaro.

c Saverio Belvedere works on life insurance product development at Allianz SpA. He holds an MSc in Statistical and Actuarial Sciences from Università Cattolica del Sacro Cuore and he is currently enrolled in the Allianz Talent Program, pursuing a postgraduate program in Finance, Insurance and New Technologies provided by Politecnico di Milano.

scape of cyber risk, balancing investment in security and resilience emerges as a relevant challenge for management.

In this landscape, precisely defining and conceptualizing cyber risk is a pivotal challenge. The body of literature addressing cyber risk has burgeoned over time, with each work offering nuanced interpretations (World Economic Forum 2012; Böhme and Kataria 2006; Strupczewski 2021), thereby contributing to a diverse array of definitions. Clarifying the concept of cyber risk is essential to understanding its multifaceted nature and implications. Notably, Strupczewski (2021) comprehensively defined cyber risk as: ''*[An] operational risk associated with performance of activities in the cyberspace, threatening information assets, ICT resources and technological assets, which may cause material damage to tangible and intangible assets of an organisation, business interruption, or reputational harm. The term cyber risk also includes physical threats to the ICT resources within [the] organisation.*''

To further elucidate this concept, it is helpful to compare other definitions in the literature. For instance, the World Economic Forum (2012) emphasizes the strategic impact of cyber risk, describing it as a threat to business continuity and organizational stability, with a focus on economic and reputational damage. Conversely, Böhme and Kataria (2006) offer a more technical perspective, framing cyber risk primarily in terms of vulnerabilities and threats to information systems, often focusing on the likelihood and potential impact of specific cyber threats. Strupczewski's (2021) definition is notable for its broad scope, encompassing not only operational risks and performance issues but also physical threats to ICT resources, which is less emphasized in the other definitions. This comprehensive approach addresses both direct and indirect impacts of cyber risks, providing a more holistic view compared with the more narrowly focused perspectives of the other authors.

On the insurance front, quantifying cyber risk is challenging because of its extensive impact on intangible assets, such as data and reputation, making it difficult to evaluate losses. Moreover, the insurability of this risk and the potential for systemic failures (linked to extreme events) present additional complexities for managing cyber risk (see, e.g., Dacorogna and Kratz 2022; Eling and Wirfs 2019; Ai and Wang 2023.

With IT pervading all human activities, interdisciplinary research aims to comprehensively understand cyber risk from various angles (see Awiszus et al. 2021; Xie, Lee, and Eling 2020; and Dacorogna and Kratz 2023, for comprehensive surveys on this subject). As highlighted by Dacorogna and Kratz (2023), traditional actuarial techniques are inadequate for rating and controlling risk accumulation, owing to limited availability of historical data and the need to move beyond past loss records. These issues led researchers to identify five potential model types: actuarial models based on loss data, stochastic models for risk contagion, data-driven artificial intelligence (AI) models, exposure models, and game-theory based models. This discussion centers on stochastic models for risk contagion within networks.

Cyber risk's distinct characteristic is that it occurs within a vast network of computers and connections, making it conducive to network (or graph) modeling, epidemiological/pandemic modeling, or other appropriate stochastic models. Chen and Hon Keung (2024) developed a modified Wiener process model for the degeneration of network functionality. The susceptible-infectious-susceptible (SIS) epidemic Markov model has been applied to cyber insurance (Fahrenwaldt, Weber, and Weske 2018), and Xu and Hua (2019) explored a modified ϵ-SIS model based on Van Mieghem and Cator's (2012) proposal. Additionally, Antonio, Indratno, and Simanjuntak (2021) delved into the heterogeneous generalized susceptible-infectious-susceptible (HG-SIS) model (see also, Ottaviano et al. 2018, 2019).

Following these methodologies, we introduce a novel approach that draws on the advancements of Xu and Hua (2019) and Antonio, Indratno, and Simanjuntak (2021), enabling separate modeling of critical and noncritical nodes. The method captures the network's node heterogeneity and considers the distinct characteristics of critical and standard nodes. This differentiation is pivotal, providing a nuanced understanding of vulnerabilities, which facilitates targeted fortification of critical nodes while optimizing resources to uphold the overall network resilience against potential threats. Indeed, our proposed approach offers a versatile framework that extends its applicability to effectively model whaling phishing scenarios.[1] By introducing nodes that possess the distinctive trait of more easily infecting nodes with which they are connected,[2] this method accommodates modeling of such targeted attacks within the network. These specialized nodes significantly elevate the system's susceptibility to risks, amplifying the potential dynamics of infection beyond the conventional homogeneous node assumption.

Emphasizing the significance of departing from homogeneous node considerations, our methodology not only distinguishes between critical and noncritical nodes but also acknowledges the inherent heterogeneity within the network. This nuanced perspective both enhances the understanding of vulnerabilities and facilitates precise fortification strategies targeting critical nodes. Simultaneously, it optimizes resource allocation, bolstering the network's overall resilience against a spectrum of potential threats, including sophisticated whaling phishing tactics.

1 For more information on whaling phishing, refer to the National Cyber Security Centre: https://www.ncsc.gov.uk/guidance/whaling-how-it-works-and-what-your-organisation-can-do-about-it.

2 In this way, we could consider nodes as representing people with key roles in the firm (for instance, executives, managers, directors, etc.).

We developed a numerical analysis to evaluate our proposed approach using a simulated network that mirrors the structure of a small- to medium-sized enterprise. Additionally, we conducted sensitivity analyses to assess how variations in the network's topology and infection dynamics influence the outcomes.

The remainder of this paper is organized as follows: Section 2 introduces foundational concepts of graph theory. Section 3 details our proposed methodology, beginning with the general framework in Section 3.1. Section 3.2 delves into employing epidemiological models for cyber risk, outlining our methodology for identifying infected nodes and assessing claim counts. Cost and recovery functions are discussed in Section 3.3, while Section 3.4 elucidates the simulation algorithm. Computation of premiums is addressed in Section 3.5. Our numerical analysis and ensuing discussions are presented in Section 4. Conclusions follow in Section 5. Appendices summarize the algorithm and main R codes used in the procedure.

2. PRELIMINARIES ON GRAPH THEORY

The study of networks is a multidisciplinary field that amalgamates concepts from mathematics, physics, biology, computer science, social science, and various other domains. Across these disciplines, researchers have developed a diverse toolkit, including mathematical, computational, and statistical methods to analyze, model, and fully comprehend networks. Networks serve as a versatile representation for numerous systems and help to capture intricate connection patterns between components.

The notion of a network is inherently straightforward: it consists of interconnected points linked by edges. The exploration of networks falls under the purview of *graph theory*, where graphs serve as the mathematical abstraction of networks (for details, refer to works by Estrada 2011; Harary 1969; Newman 2010).

A network is typically denoted as $G(V, E)$, described as a pair of sets (V, E), where $V = \{1, \ldots, n\}$ is the set of n *nodes* (or vertices) and E is the set of m *edges* (or links) represented by points and lines, respectively, in Figure 1. We consider graphs with fixed order $|V| = n$ and fixed size $|E| = m$. The edge connecting vertices i and j are denoted by e_{ij}. When two vertices share an edge, they are called *adjacent*.

An $n \times n$ nonnegative matrix, denoted as $\mathbf{A}$, characterizes the interconnections between vertices within the graph G and is termed the *adjacency matrix*. This matrix $\mathbf{A}$ for a simple graph comprises elements a_{ij} defined as follows:

$$a_{ij} = \begin{cases} 1 & \text{if there is an edge between vertices } i \text{ and } j \\ 0 & \text{otherwise} \end{cases}.$$

In certain scenarios, assigning a numerical value (often a real number) to edges proves beneficial. Consequently, a weight w_{ij} can be allocated to each edge e_{ij}, resulting in a representation known as a *weighted graph*. In this case, we associate a weighted adjacency matrix $\mathbf{W}$ to the graph. In the context of the weighted adjacency matrix, instead of binary entries indicating the presence or absence of edges between vertices as in the standard adjacency matrix, the entries w_{ij} represent the weights associated with the edges (i.e., the weight of the edge connecting vertices i and j).

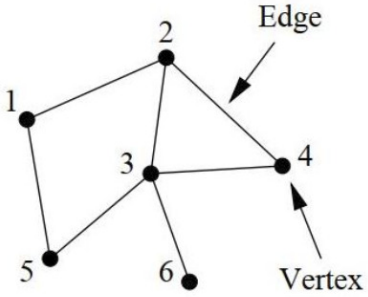

Figure 1. Example of unweighted and undirected network with *n*=6 nodes and *m*=7 edges.

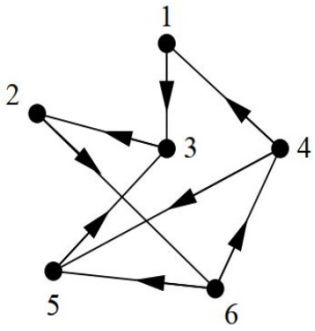

Figure 2. A small directed graph with arrows indicating the directions of the edges.

A *directed graph* (or *digraph*) represents a type of graph where each edge, referred to as an *arc*, possesses a direction, indicating a unidirectional link between vertices as depicted in Figure 2. Precisely, every edge in a directed graph is an ordered pair of vertices, delineating a specific flow or connection from one vertex to another.

Notably, the adjacency matrix $\mathbf{A}$ (and $\mathbf{W}$ if the graph is weighted) of a directed graph may exhibit asymmetry due to the directed nature of its edges. This asymmetry distinguishes it from the symmetric nature of adjacency matrices in undirected graphs, reflecting the directional relationship between vertices in the graph.

In a network, a *path* denotes any sequence of vertices wherein each consecutive pair of vertices in the sequence is connected by an edge in the network, akin to the red path depicted in Figure 3. Specifically, an $i - j$ path signifies a sequence of distinct adjacent vertices traversed from vertex i to vertex j.

The *length* of a path refers to the count of edges traversed along the path. A *shortest path*, also known as a *geodesic path*, represents the shortest route between two vertices where no other path is shorter. In weighted graphs, the weighted shortest path is the one with the minimum sum of edge weights. The *distance* $d(i, j)$ between vertices i

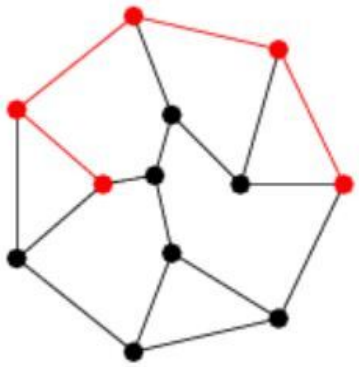

Figure 3. A path of length four in a graph.

and j indicates the length of the shortest path connecting them, if such a path exists, and is set to $+\infty$ otherwise.

A graph G is *connected* if there is a path between every couple of vertices. A graph G is *complete* when every node is connected to every other.

With directed graphs, paths are directed and comprise a sequence of distinct vertices wherein each consecutive pair of nodes in the sequence is connected by a directed edge that follows the directionality of the graph. Specifically, an $i - j$ path in a directed graph signifies a series of vertices, starting from node i and ending at node j, such that each node is linked by directed edges in the specified direction. The definitions of length and distance as well as the extension to the weighted case follow as in the case of undirected graphs.

3. METHODOLOGY

3.1. SYSTEMIC RISK MODELING FOR CYBER

Unlike the *individual* and the *collective* approaches to cyber risk pricing, *systemic risk* modeling offers a substantially different perspective. The individual and collective models, along with their derivatives, focus on analyzing the combined cost of claims from a pool of companies or policyholders by identifying shared characteristics and reasoning collectively. They primarily adopt a *macroscopic* viewpoint.

Conversely, the systemic risk model takes an opposite approach by adopting a *microscopic* perspective. It aims to reproduce the essential and minimal structure of communication within a specific analyzed company. This is achieved by representing it through a weighted and undirected graph, mimicking the communication interactions within the network over the insurance coverage duration. This approach allows for the dynamic simulation of node infections (i.e., devices, laptops, servers, etc.) throughout the policy period.

For instance, Figure 4 shows the structure of a network comprising 167 employees of a manufacturing company.[3]

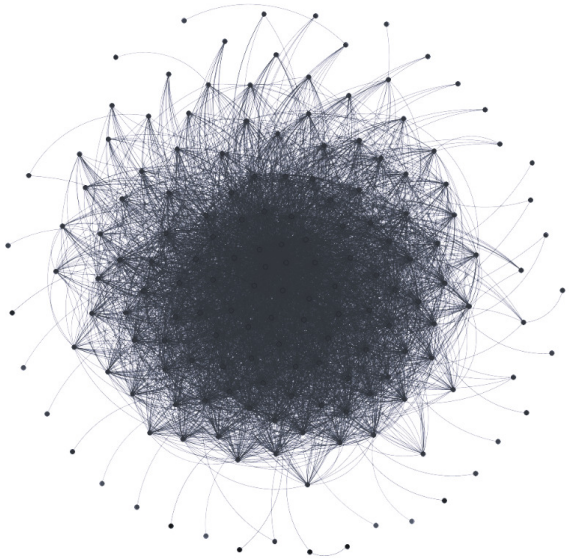

Figure 4. Manufacturing company e-mail communication.

This network represents internal e-mail communications spanning a period of 9 months, from January 1, 2010 to September 30, 2010. The data were provided in an anonymized format, and instances where an e-mail had multiple recipients (e.g., To, CC) were documented in separate rows within the dataset. Though not visually represented, the weights in this context denote the communication intensity between different nodes within the company's communication network. This parameter holds significant relevance in the model, as a higher interaction level between colleagues/nodes correlates with an increased likelihood of vulnerability in case a node is compromised.

It is important to note that acquiring such network data is a challenging task. Some datasets available in the literature are often sourced from e-mail box leaks or made accessible by institutions, such as universities or research entities. Hence, the ability to obtain the network and simulate infection dynamics becomes paramount. Understanding that the internal dynamics of a large multinational company differ from those of a small- or medium-sized enterprise, or a startup with a limited workforce, is crucial. The challenge lies in reconstructing hierarchical structures theoretically, which remains intricate. While relying solely on an e-mail database might be challenging, it can serve as a valuable starting point if accessible to insurers.

3 Source: https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/6Z3CGX.

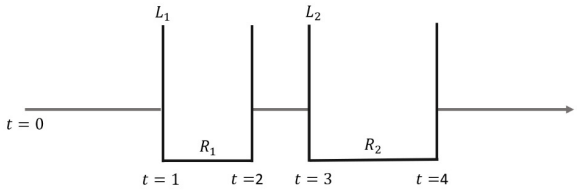

Figure 5. Infection-recovery scheme for a node.

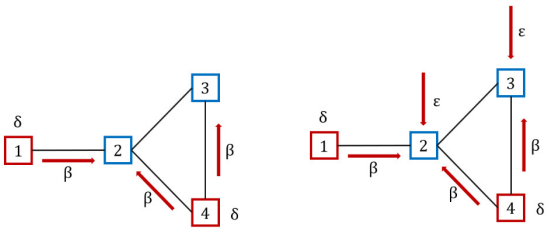

Figure 6. *SIS* and ε-*SIS* models.

3.2. USING AN EPIDEMIOLOGICAL MODEL FOR CYBERSECURITY INSURANCE

Considering the perspective we proposed, we initially focused on a model that considers a company communication network represented as an *undirected weighted graph*. Its objective is to simulate infections among nodes, both critical and noncritical. When a node is infected, the model simulates the damage incurred and the duration for recovery. Consequently, this simulation aids in determining an insurance premium over the contractual term.

Early studies on infection modeling—for example, Von Neumann's (1949) work—date back almost a century. Subsequent research in graph theory, computer science, and insurance by various authors (see Awiszus et al. 2023; Märtens et al. 2016; Xu and Hua 2019; Van Mieghem and Cator 2012; Fahrenwaldt, Weber, and Weske 2018), has contributed significantly. Our proposal draws inspiration from Xu and Hua (2019) and Antonio, Indratno, and Simanjuntak (2021) by incorporating specific modifications.

In replicating the infection dynamics during the contractual term it is necessary to consider the *status* of a node, which can be either *infected* or *secure*. A node is infected if it was the victim of an attack in a previous period or if it is still under attack; a node is secure if it is susceptible to an attack. This status needs continual monitoring for each node in the network $G = (V, E)$, with n nodes and m edges, at every time point:

$$\big(I_1(t), \ldots, I_n(t)\big), \tag{1}$$

where $I_i(t)$ indicates whether node i is infected (1) or secure (0) at time t.

Another quantity of equal interest is the vector of probabilities of being in a state of infection for each individual node at a certain time t:

$$\big(p_1(t), \ldots, p_n(t)\big), \quad p_i(t) = \mathbb{P}(I_i(t) = 1). \tag{2}$$

Referencing Figure 5, a node's infection-recovery scheme portrays its progression. Initially secure, the node becomes infected at $t = 1$, incurs a loss L_1, undergoes repair with cost R_1, and restores functionality by $t = 2$. Subsequent infections and recoveries follow a similar pattern.

This infection dynamic is known in the epidemiological literature as the *SIS* (susceptible, infectious, and susceptible) model, suitable for node infections resulting from the absence of immunity after an infection (see Kermack and McKendrick 1927; Pastor-Satorras and Vespignani 2001). These are compartmental models, so called because the examined population is divided into distinct groups. The *SIS* model fits very well in the case of node infections since *no immunity* to subsequent infections is gained.

The model, often viewed as a *renewal reward process*, categorizes the population into distinct groups. It can be seen as a generalization of the Poisson process. In particular, the holding times between events can follow any distribution with finite mean and positive values, not just the exponential distribution. This process is indeed more flexible as it can model a wider variety of real-world phenomena by allowing different distributions for the inter-event times. When the holding times are not exponentially distributed, the process does not have a memoryless property, making it a non-Markov process (see, e.g., Van Mieghem, Omic, and Kooij 2009). This type of model uses two specific parameters, typically denoted with β and δ, to describe infection and recovery dynamics, respectively. In particular, as displayed in Figure 6 (left side), in the traditional SIS model, infected nodes, represented in red, can propagate the infection at a rate β following existing connections (see, e.g., red arrows connecting nodes 1 to 2, 4 to 2, and 4 to 3) and recover at a rate δ.

In the case where a node can be infected not only by neighboring nodes, but also from outside the network, it is possible to generalize the *SIS* model by means of an additional parameter ε (self-infection rate), thus obtaining the ε-*SIS* model(see, e.g., Van Mieghem and Cator 2012). Figure 6 (right side), illustrates an example where secure nodes 2 and 3 can be infected by neighboring infected nodes at a rate β, and from outside at a rate ε.

Considering an ε-*SIS* model, we have for the i-th node:

$$\begin{cases} I_i(t) : 0 \to 1 \text{ at rate } \beta \sum_{\ell=1}^{n} a_{\ell i} I_\ell(t) + \varepsilon_i \\ I_i(t) : 1 \to 0 \text{ at rate } \delta_i \end{cases}, \tag{3}$$

where $a_{\ell i}$ is the ℓ, i element of the adjacency matrix associated with the network. Parameters β, ε, and δ are not node-specific, which simplifies model complexity. Hence, these models tend to overlook critical aspects, such as network weights, communication intensities among devices, and the presence of different node types in the network (e.g., servers and personal computers).

To address these limitations, we adopted a non-Markov model, known as *HG-SIS* (heterogeneous generalized susceptible-infectious-susceptible), which allows for different β values for each arc. At any given moment, the time to infection for a node is determined by the minimum duration among two sets of random variables. The first set comprises the times to infection generated by random variables $Y_1, \ldots, Y_{D_i}$, where D_i represents the infected neighbors of

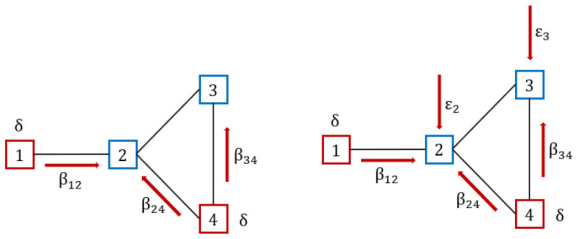

Figure 7. *H-SIS* and *HG-SIS* models.

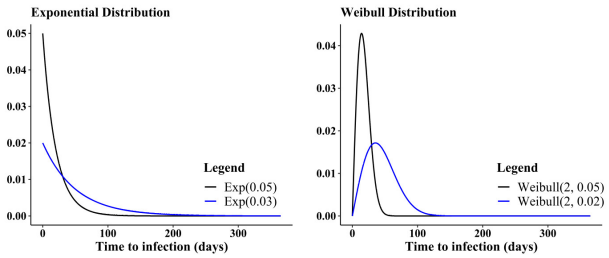

Figure 8. Exponential vs Weibull distributions.

node i. Additionally, the node faces a self-infection time denoted by Z_i, which accounts for external threats entering the network:

$$T_i = \min\left(Y_1, \ldots, Y_i, Z_i\right). \tag{4}$$

This calculation establishes the shortest duration required for a node to succumb to infection, considering both internal risks from infected neighbors and external threats outside the network perimeter.

The *HG-SIS* model, depicted in Figure 7, potentially involves as many β parameters as there are nonzero elements in the adjacency matrix, corresponding to the m arcs. Also, the self-infection and the recovery processes, described by ε_i and δ_i, could be different between nodes. As displayed in Figure 7, infected nodes, represented in red, can propagate the infection at different rates through existing connections (see red arrows in the figure), while noninfected nodes are also exposed to different infection probabilities from outside (see ε_2 and ε_3 in the Figure 7.

However, in the case of large networks, this model requires estimating an extensive number of parameters. To address this, we followed the approach of Antonio, Indratno, and Simanjuntak (2021), considering only the values of β and δ and using the edge weights of the network. We employed a *sigmoidal transformation* to derive the matrix of parameters. The proposed transformation is a function of the weight of the edge considered, values of β and δ, and characteristics of the weight distribution. This allowed us to find an $n \times n$ matrix $\mathbf{B}$, whose elements β_{ij} are defined as follows:

$$\beta_{ij} = \begin{cases} 0, & w_{ij} = 0 \\ \frac{\beta - \delta}{1 + exp\left(-\frac{(w_{ij} - \bar{w})}{\sigma}\right)} + \delta, & w_{ij} > 0 \end{cases}, \tag{5}$$

where:

$$\bar{w} = \frac{1}{2 \cdot m} \sum_{i,j} w_{ij}, \sigma = \frac{\sum_{i,j} |w_{ij} - \bar{w}|}{2 \cdot m}. \tag{6}$$

The proposed transformation aims to increase (reduce) the infection probability when the edge weight is higher (lower). This is consistent with the literature that interprets edge weights as communication weights and generally conveys how effectively that edge is transmitting information and infection (see, e.g., Antonio, Indratno, and Simanjuntak 2021; Bartesaghi, Clemente, and Grassi 2024).

Hence, formula (3) becomes

$$\begin{cases} I_i(t) : 0 \to 1 \text{ at rate } \sum_{\ell=1}^{n} \beta_{\ell i} a_{\ell i} I_\ell(t) + \varepsilon_i \\ I_i(t) : 1 \to 0 \text{ at rate } \delta_i \end{cases}. \tag{7}$$

In this way, the infection probability between a couple of nodes depends on the weight of the arc connecting the two nodes.

To account for the potential existence of two node types, *common* or standard nodes and *critical* nodes, two sets of β and δ are selected. Subsequently, two distinct sigmoidal transformations are applied. This approach aims to create a clearer distinction between parameters, enhancing their impact on infection durations. By implementing this method, we accentuate the differences in infection times between the node types, thereby better reflecting their respective vulnerabilities.

Understanding the advantages of diverse β values becomes evident when selecting and fine-tuning distributions to represent infection times. Figure 8 illustrates the behavior of two widely used distributions for infection times concerning parameter adjustments. For instance, observing the exponential distribution, a decrease in β results in an increase in the distribution's mean, consequently extending the infection times. Conversely, the Weibull distribution, unlike the exponential, not only affects the mean, but also allows manipulation of the distribution's skewness through its shape parameter. Figure 9 depicts the variation in the behavior of the Weibull probability density function as the shape parameter undergoes changes.

In the simulations, we used the Weibull distribution for both time to infection (β and ε parameters) and recovery time (δ parameter) since it provides greater flexibility. Details of the distribution and connection with parameter β are reported in Appendix B. It is worth noting that as β increases, both mean and variance tend to zero, while skewness is independent of the parameter β. From a practical point of view, choosing a very small β (or δ or ε) in the parametrization of the epidemic model will lead to large averages of the times to infection, but consequently also to greater variability in the simulations.

3.3. COST AND RECOVERY FUNCTIONS

After a node becomes infected, it is important to assess the financial implications encompassing both recovery and tangible losses. The critical differentiation lies between critical and noncritical nodes. For the latter, two separate cost functions are established to account for both recovery and loss expenses. Conversely, critical nodes are governed by a singular function. This differentiation arises from the

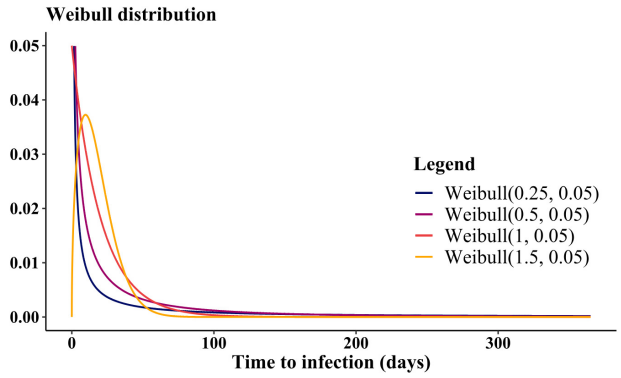

Figure 9. Weibull distributions.

adoption of distinct distributions employed to emulate the incurred damage.

In the scenario where a single node incurs a loss due to infection (or self-infection), it is crucial to model the associated costs. These costs might encompass material damages to the laptop, liabilities incurred toward third parties, economic repercussions resulting from data loss, and more, depending on the contractual terms outlined in the policy. Conversely, concerning the recovery process, the incurred loss refers to the expenses required to restore the node's functionality.

COST AND RECOVERY FUNCTION FOR NONCRITICAL NODES

For common nodes, reference is made to the solution adopted by Xu and Hua (2019). The cost function is given by:

$$\eta_i(l_i) = c \cdot l_i, \tag{8}$$

where l_i is simulated using a four-parameter beta distribution. The loss cost function is thus proportional to the loss, according to an appropriately chosen parameter c. The beta distribution, on the other hand, is chosen because, for common nodes, it was deemed appropriate to have limited support for the possible realizations of the random variable. When signing a policy, for example, one could insure each *simple* node in the network up to a value of EUR $1,000$–$1,500$. In this way, in the event of infection, the loss would be *superiorly limited* thanks to the use of this beta random variable. Recovery cost function is given by:

$$\rho_i(w_i, r_i) = c_1 \cdot w_i + c_2 \cdot r_i, \tag{9}$$

where r_i is the time required for recovery, modeled by a Weibull distribution, w_i is the initial wealth of the node, and c_1 and c_2 are two parameters that allow us to amplify or reduce the effect of recovery and initial wealth on the recovery cost. For consistency, the initial wealth of the node could correspond to the upper limit of support within the four-parameter beta distribution.

Figure 10 depicts the histograms of both the loss l_i and the corresponding cost function η_i. It is evident that by opting for a straightforward cost function, the distribution's original "shape" and positive skewness remain intact. Similarly, by generating recovery times using a Weibull distribution, we can observe the histogram of the recovery cost function. Once again, the simplicity of the chosen function preserves the initial distribution's form. In both scenarios, these functions represent basic linear transformations of random variables.

COST AND RECOVERY FUNCTION FOR CRITICAL NODES

For critical nodes (servers, highly sensitive computers, databases, etc.) we took a different approach concerning claims distribution, diverging from the use of two separate cost functions. The rationale behind this decision stems from the multiple repercussions accompanying the compromise of critical nodes, including not just the device's damage but also third-party liabilities and potential reputational harm.

Given the presumed resilience and prolonged recovery time of critical nodes compared with common nodes, we selected a lognormal distribution (as in Edwards, Hofmeyr, and Forrest 2016). To account for potential maximum limit effects, a truncated lognormal distribution can also be considered. Additionally, long-tailed distributions, such as Pareto, generalized Pareto, and gamma hold relevance in this context (see Wheatley, Maillart, and Sornette 2016; Sun, Xu, and Zhao 2020). Unlike common nodes—where estimating cost and recovery functions, employing distributions like beta, and calibrating recovery times based on support and IT department resilience is relatively straightforward—critical node estimation poses challenges. While calibrating lognormal distributions proves intricate, a conservative approach permits establishing at least the distribution's average for pricing purposes. Mean information can be obtained from third-party sources, insurers, or reinsurers, aiding in this estimation process.

3.4. THE SIMULATION ALGORITHM

The simulation model we employed is a fusion of a non-Markov model based on Xu and Hua (2019) and an HG-SIS model based on Antonio, Indratno, and Simanjuntak (2021), with an additional improvement to distinguish between critical and noncritical nodes. The objective was to simulate the cumulative loss during the entire time span of the insurance contract (e.g., 1 year). It is possible to assess the cumulative loss $s_i(t)$ of node i at time t, calculated by summing the total number $M_i(t)$ of infections of node i up to time t, as follows:

$$s_i(t) = \sum_{\ell=1}^{M_i(t)} \left[\eta_i(l_{i,\ell}) + \rho_i(w_i, r_{i,\ell})\right], \tag{10}$$

where η_i is the cost function due to infection (or self-infection) (see formula (8) in case of loss, $l_{i,\ell}$, ρ_i is the recovery process function (see formula (9)) depending on initial wealth w_i and the length of the service slowdown $r_{i,\ell}$.

Considering all nodes and summing the cumulative loss up to instant t for all nodes in the network, we obtain the following result:

$$S(t) = \sum_{i=1}^{n} s_i(t) = \sum_{i=1}^{n} \sum_{\ell=1}^{M_i(t)} \left[\eta_i(l_{i,\ell}) + \rho_i(w_i, r_{i,\ell})\right]. \tag{11}$$

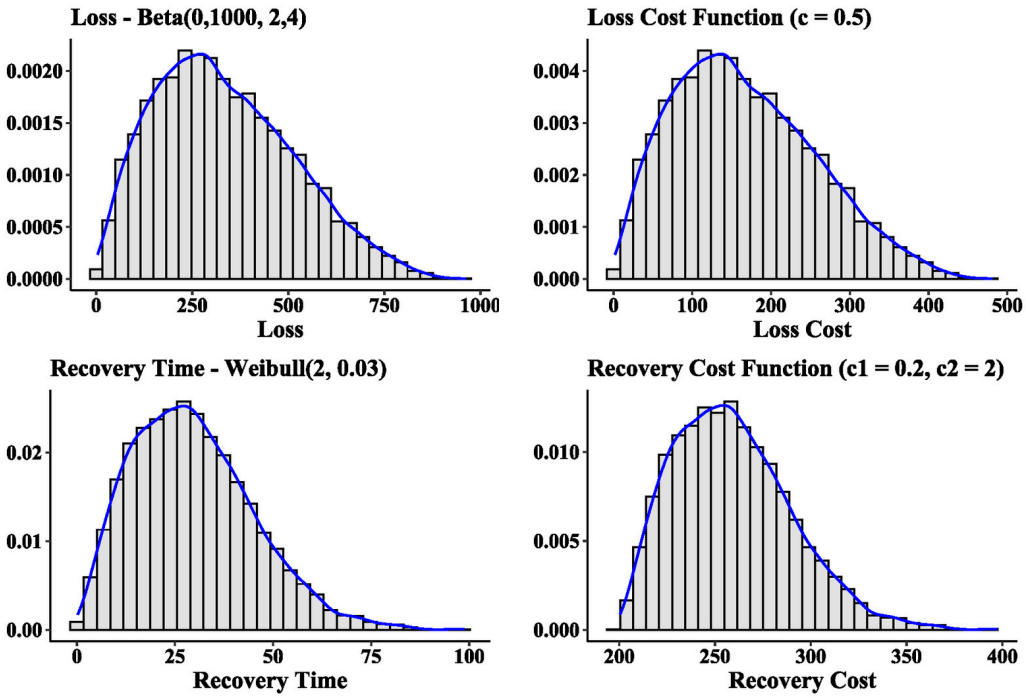

Figure 10. Histograms of cost and recovery function.

We summarized the main steps in Algorithm 1, Appendix A, used for quantifying potential losses. The initial step involves the network dataset, containing crucial information, such as node groupings, critical versus noncritical node distinctions, node IDs, and comprehensive node attributes. Following this, defining the number of simulations becomes essential, along with specifying parameters for distributions, including β, δ, and ε for critical and noncritical nodes. Additionally, parameters from relevant distributions, distinguishing between critical and noncritical nodes, are necessary to compute infection-related losses and recovery losses.

It is essential to note that, for each secure node, identifying infected neighbors is crucial. By aggregating the β parameters corresponding to the examined node's row and the columns aligned with the IDs of infected neighbors, the infection time can be simulated using a Weibull distribution (including self-infection time). This approach accounts for a dual effect. Consequently, the infection time decreases with a higher weight between a node and its infected neighbors due to the sigmoidal transformation of parameters β. Moreover, a greater number of infected neighbors leads to a shorter infection time.

Formula (12) exemplifies the summation of betas ($\hat{\beta}_i$), representing the cumulative effect of interconnectedness influencing infection probabilities.

$$\hat{\beta}_i = \sum_{\ell=1}^{D_i} \beta_{\ell,i}. \tag{12}$$

As depicted in Algorithm 1, the algorithm's design shows that *network topology significantly affects the probability of infection*. A more interconnected network increases the likelihood of having infected neighbors, thereby reducing the time to infection for each individual node. Conversely, self-infection times are *independent* of network topology and depend solely on the calibration of parameters for the chosen distribution.

3.5. PREMIUM CALCULATION

It was mentioned earlier that the aim of Algorithm 1 is to identify the loss cumulated for all nodes in the network. We can define, with the random variable $S(T)$, the total loss at the end of the contract. From a premium calculation perspective, it is essential to identify the *risk premium*:

$$\mathbb{E}[S(T)]. \tag{13}$$

The risk premium is in fact the expected value of the overall compensation to be paid by the insurer over the coverage period. Adding the safety loadings to the risk premium gives the *pure premium*.

$$P = \mathbb{E}[S(T)] + \text{safety loadings}. \tag{14}$$

This is the global compensation transferred to the insurer. Safety loadings are widely used in actuarial and pricing. They reflect the inherent riskiness of the insurance transaction and are a kind of risk premium but also reflect the remuneration of the cost of capital. Safety loading is intrinsically linked to the cost of capital since, given the *Solvency II* directive, the higher the riskiness of the LoB considered, the higher the capital requirement and thus the higher the safety loading. In the following simulations, only the risk premium and the pure premium are calculated.

Two approaches are used to calculate the pure premium. The first is the *standard deviation principle*:

$$P = \mathbb{E}[S(T)] + \alpha \cdot \sqrt{\sigma^2(S(T))}. \tag{15}$$

Basically, the remuneration for risk is proportional (α) to the standard deviation of the total cost of claims random variable during the policy coverage period. A second ap-

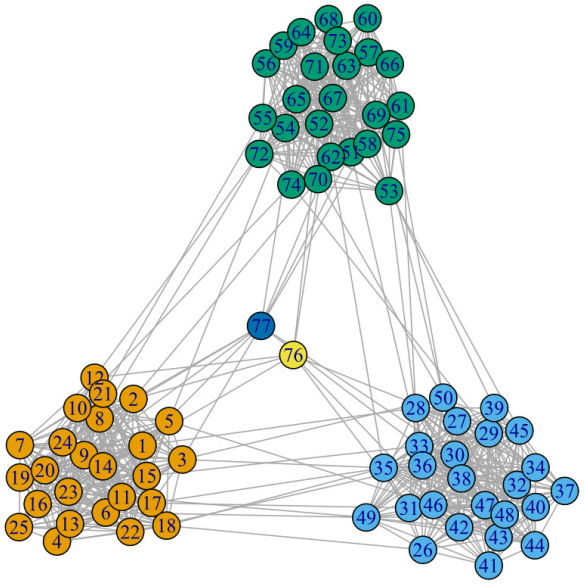

Figure 11. Case Study 1 - Network plot.

proach is to consider a given *percentile* (e.g., 60–70th) of the total claims cost distribution, also implicitly considering the skewness of the distribution.

4. A NUMERICAL APPLICATION

As mentioned in Section 3.1, obtaining the company's communication network data poses significant challenges. Consequently, we have developed an R function that allows us to create an undirected weighted network with specific a priori characteristics. The function is detailed in Appendix C. Subsequently, we transformed the previously acquired network into a weighted one, following the procedure outlined in Appendix C. This section presents and discusses an initial case study and a sensitivity analysis in which some parameters have been varied.

4.1. INITIAL CASE STUDY

DATA AND PARAMETERS

The first network, depicted in Figure 11, comprises 77 nodes, 75 of which are common and the remaining 2 are critical. This network was generated using the R function[4] described in Appendix C, employing the parameters reported in Table 1.

As detailed in Appendix C, this procedure involves a combination of Erdős-Rényi (ER) graphs (Erdős and Rényi 1959, 1960) to create a graph containing distinct nodes, both critical and noncritical. Additionally, we assumed that the connection intensity within a group exceeds that between groups. Moreover, critical nodes exhibit minimal interconnection with other nodes.

Table 1. Parameters for `make_a_matrix` function

Parameter	Value
num_groups	3
size_group	25
p_within	0.8
p_between	0.01
num_criticals	2
p_criticals	0.1
overlapping	FALSE
intensity_overlapping	0
overlapping_quota	0

Table 2. Parameters for the infection dynamics

	Not Critical Nodes	Critical Nodes
β	0.03	$\beta/2$
$lower_\beta$	0.01	$lower_\beta/2$
ε	0.01	$\varepsilon/3$
δ	0.1	$\delta/1.5$
α_β	3	3
α_ε	3	3
α_δ	3	3

Following the steps outlined in Appendix C we assigned weights to the graph's edges. We made an arbitrary assumption of 20 communications per node per day on average. However, it is important to note that the minimum weight of an edge is one, and only a small subset of edges carries a high volume of communications during the contract term because of the pronounced positive skewness of the selected distribution.

Starting from this undirected and weighted network, it is possible to set (and calculate) parameters essential for the infection dynamics. These include the maximum and minimum values of β for critical and not critical nodes, as well as the required α and δ values. Using the network weights and the sigmoidal transformation discussed in Section 3.2, all β parameter values can be derived. We used the starting parameters in Table 2 for this case study. Consistent with what has been stated so far, the parameters for critical infrastructures are smaller and therefore imply longer times to infection and self-infection than for normal nodes. In addition, the times to recovery and to reestablish node functionality are also longer.

The boxplots illustrating the beta parameters obtained for critical and not critical nodes are presented in Figure 12.

4 Refer to the *make_a_matrix* function.

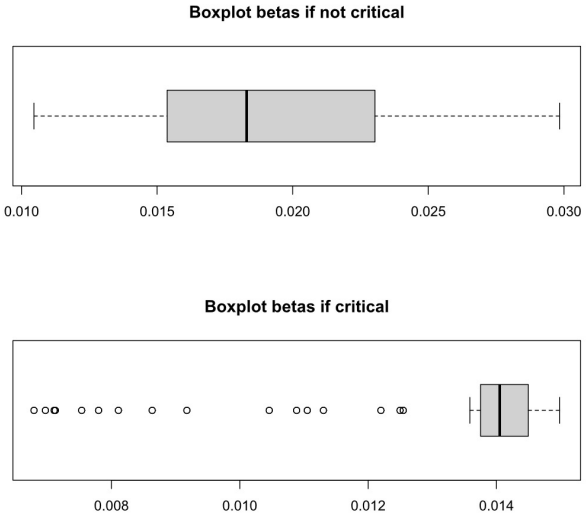

Figure 12. Boxplot of parameters β for critical and not critical nodes.

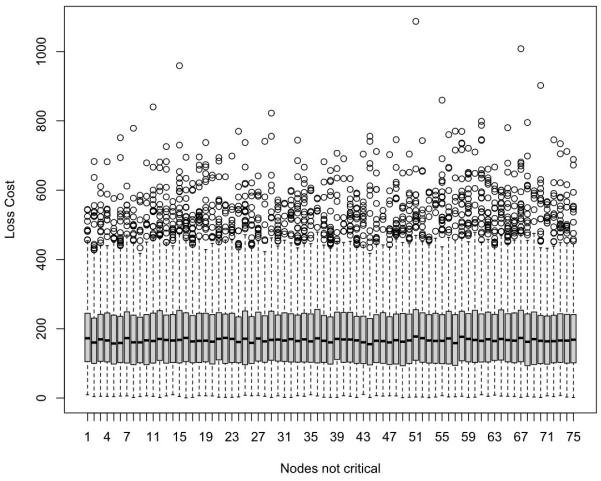

Figure 13. Boxplot of loss cost for each node classified as not critical.

These plots showcase the distinctive attributes of the sigmoidal transformation. Positioned between defined minimum and maximum values, these parameters exhibit variability based on the edge weights, which signify the estimated connection intensity during the policy period.

To conduct the simulations, we established the cost and recovery functions for the common nodes as follows:

$$\eta_i(l_i) = 0.5 \cdot l_i$$
$$\rho_i(w_i, r_i) = 0.2 \cdot 1000 + 2 \cdot r_i.$$

Here, each node begins with an initial wealth of EUR $1,000$, and a four-parameter beta distribution characterizes the severity of the loss. However, for critical nodes, we selected a singular cost/recovery function. In the event of infection in a critical node, the cost of damages, encompassing losses to third parties and physical assets, is determined from a truncated lognormal distribution, which accounts for the expenses required to restore the critical infrastructure to its full operational state. This choice stems from the typical existence of maximum limits in insurance contracts for such damages and the significant tail end of the distribution.

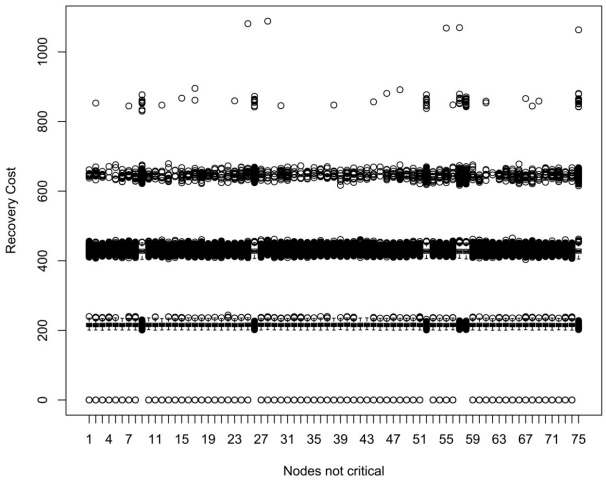

Figure 14. Boxplot of recovery cost for each node classified as not critical.

SIMULATION RESULTS

After obtaining the initial graph and gathering all required parameters, we executed Algorithm 1 from Section 3.4; the results are detailed below.

Figure 13 displays the boxplots illustrating the incurred loss costs solely for not critical nodes. These plots showcase a consistent behavior, highlighting multiple infections of individual nodes during the policy period. Similarly, Figure 14 portrays the recovery cost boxplots. Since the recovery cost is contingent on the duration needed for recovery, a discernible pattern emerges, reflecting repeated infections of the same nodes.

The loss/recovery boxplots for critical nodes are depicted in Figure 15. The substantial impact of critical nodes on the aggregated cost of claim distribution is evident owing to their heightened severity compared with common nodes. Additionally, note that within this framework, prior infection does not confer immunity, potentially escalating the damage for critical nodes.

Since the total cost of claims arises from both common and critical node infections, understanding the resultant distribution by amalgamating these source distributions is crucial for insurers. Figure 16 illustrates that while infections among *common* nodes often result in limited claims, a few critical infrastructures can incur potential losses of up to a half million euros. These striking disparities confirm the significance of our proposed method, which enables the separate modeling of common and critical nodes, offering a more comprehensive insight into potential risks for insurers.

To relate simulation outcomes to a known distribution, we applied Cullen and Frey's (1999) method. The (non-

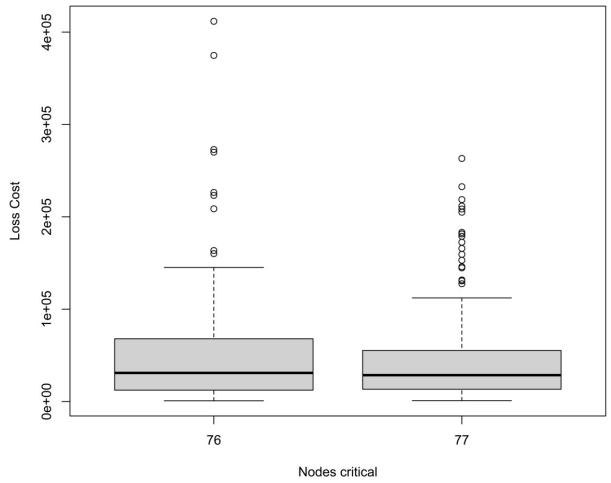

Figure 15. Boxplot of loss cost for the two nodes classified as critical.

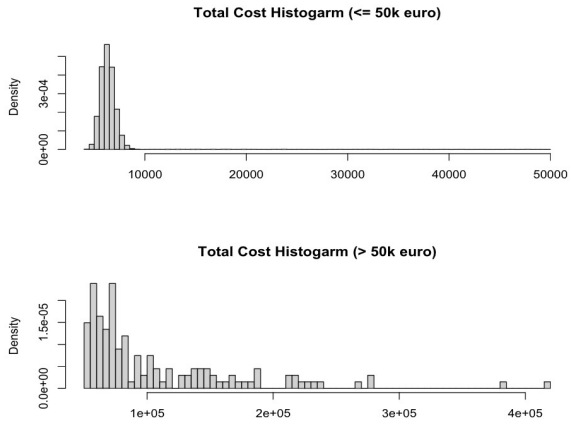

Figure 16. Distribution of total cost split between amounts lower and higher than EUR 50,000, respectively.

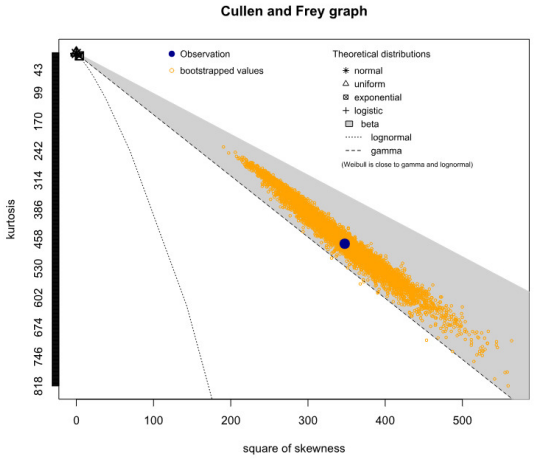

Figure 17. Cullen and Frey plot of total cost.

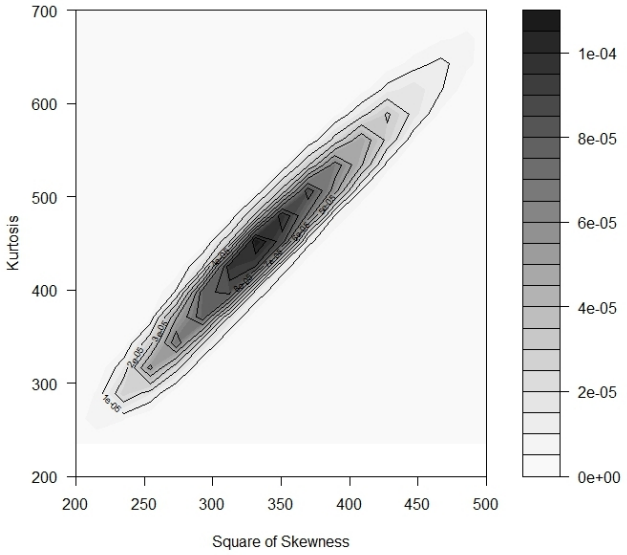

Figure 18. Contour plot of the kurtosis and square of skewness combination.

parametric) bootstrap results in Figure 17 suggest that estimating the total aggregate distribution using a gamma distribution is feasible. To support this evidence, Figure 18 illustrates the contour plot of the combination between skewness and kurtosis.

Table 3 presents an overview of the key attributes characterizing the distribution of total losses incurred. The significant impact of two distinct node types affected differently by infection dynamics, coupled with their notably disparate associated costs, is a prominent feature. This convergence manifests in a distribution marked by considerable skewness. The presence of these disparities not only underscores the intricate nature of the infection dynamics but also accentuates the pivotal role played by our modeling approach in capturing these nuances.

These statistics empower insurance companies to precisely calculate the premium. For instance, considering a safety loading assessment at 1% of the standard deviation, the derived premium approximates to around EUR 95 per node.

4.2. SENSITIVITY ANALYSES

We present here a sensitivity analysis in which certain topological characteristics of the network are primarily altered. As shown in Figure 19, the number of nodes remains constant, while the number of groups has increased (from 3 to 5) and the connection probabilities within and between groups has also increased. Compared with our previous analysis, we kept invariant the number of critical infrastructures and the probability of their connection with

Table 3. Characteristics of the distribution of total losses $S(T)$ in a one-year time horizon (T = 365)

Metric	Value
Mean	7,225.38
Mean only for critical nodes	48,906.96
Standard Deviation	10,070.99
Median	6,312.67
Skewness	18.65
Kurtosis	469.21
Quantile at 70%	6,699.20
Quantile at 99.5%	62,967.1

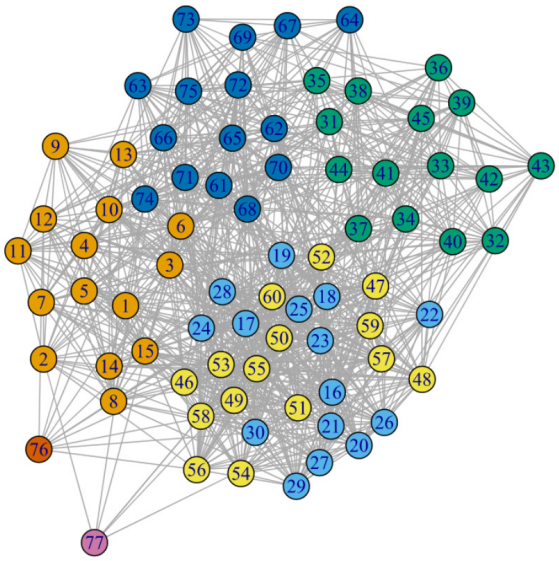

Figure 19. Case Study 2 - Network plot.

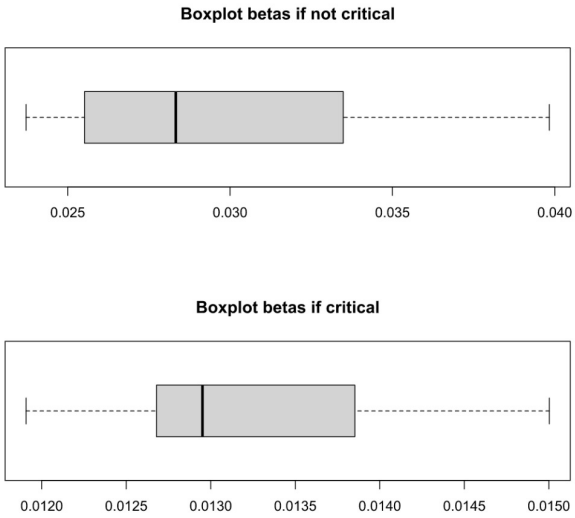

Figure 20. Case Study 2 - Betas boxplot.

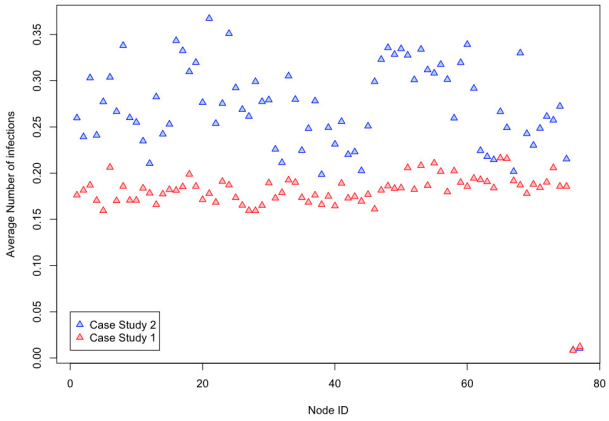

Figure 21. Average number of infections in Case Study 1 and 2.

common nodes. The aim was to evaluate how an insured firm characterized by different connections could be exposed to cyber risk.

In addition to the increased connections between common nodes, which make the network more prone to greater numbers of infections, the thresholds for beta parameters have also been changed. The new beta parameters, whose distributions are summarized in the boxplot displayed in Figure 20, will therefore vary between 0.04 and 0.02 (with respect to the range observed before, $(0.01, 0.03)$). Thus, by means of the sigmoidal transformation, a decrease in the time to infection and, consequently, a higher number of infections is expected. However, it should be noted that varying only the beta parameter does not necessarily imply that there are more (or fewer) infections in the network, because a predominant behavior in the infection dynamics could be driven by the self-infection probability and, more importantly, the network recovery times.

Figure 21 summarizes and highlights the differences with respect to the previous results. It depicts the average number of infections for each node, including the two nodes representing critical infrastructures. It is apparent that the new network, having a different topology from the first and different parametrization of infection times, has a systematically higher average number of infections per node. However, this difference is not appreciable in the case of the critical infrastructures, which did not show a change in the number of interconnections with common nodes. This is an essential aspect to note, as it shows, with a simulative approach, and in this framework, that if well protected, critical infrastructures can be very resilient to cyber attacks.

As also illustrated in Table 4, the risk premium in this case increased significantly ($+17.40\%$). The same trend is also present for the median and the $70th$ percentile of the distribution. Conversely, the standard deviation is smaller than before, probably because of the more homogeneous topology of the network. A more connected network suggests less variability between nodes and thus a lower standard deviation, given the cost functions chosen for this analysis.

Table 4. Characteristics of the distribution of total losses $S(T)$ in a one-year time horizon (T = 365)

Metric	Value
Mean	8,483.05
Mean only for critical nodes	42,907.09
Standard deviation	9,577.77
Median	7,522.68
Quantile at 70%	8,375.36
Quantile at 99.5%	55,051.51

Consistent with the methodology adopted above, using a safety loading coefficient equal to 1% of the standard deviation, the resulting premium is about EUR 111 ($\approx$ 17.1% higher).

5. CONCLUSIONS

This paper addresses the emerging threat of cyber risk in our digitally dependent era. We emphasize the need for robust strategies to mitigate cyber attacks and to structure our operations resiliently. We provide a comprehensive delineation of cyber risk, including operational risks, threats to information and technological assets, and potential damage. Quantifying cyber risk and evaluating losses is challenging due to the impact on intangible assets. We highlight the interdisciplinary nature of research on cyber risk and discuss different model types, including network and stochastic models. Traditional actuarial techniques are inadequate for rating and controlling risk accumulation; consequently, researchers are identifying more effective model types, including stochastic models for risk contagion.

Cyber risk's distinct characteristic of occurring within a vast network of computers and connections lends itself to network or graph models, epidemiological/pandemic models, and other stochastic models. We have discussed several existing models, such as the susceptible-infectious-susceptible epidemic Markov model, and introduced our novel approach that considers separate modeling of critical and noncritical nodes in the network. This approach captures the heterogeneity within the network and facilitates targeted fortification of critical nodes while optimizing resources to enhance overall network resilience.

To evaluate our proposed approach, we conducted a numerical analysis using a simulated network mirroring the structure of a small- to medium-sized enterprise and performed sensitivity analyses to assess the impact of network topology variations and infection dynamics on the outcomes. Our approach offers a versatile framework for modeling cyber risk, particularly in scenarios involving targeted attacks, such as whaling phishing. By considering the distinct characteristics of critical and noncritical nodes and acknowledging the heterogeneity within the network, our approach enhances our understanding of vulnerabilities and enables precise fortification strategies. It optimizes resource allocation and strengthens the network's resilience against various potential threats. Future research in this area should further explore the applicability and effectiveness of our approach in different network structures and real-world settings.

While network models offer valuable insights into the structure and dynamics of cyber risk, there are inherent limitations to their application in cyber risk assessment. Understanding these limitations is crucial for refining our approaches and improving their effectiveness. One key limitation is the complexity of accurately representing and simulating real-world network topologies. Network models often simplify the intricate relationships and interactions within a network, which can lead to oversimplified assumptions about how attacks propagate and impact various nodes. This simplification may result in inaccurate risk assessments or failure to capture critical vulnerabilities. Additionally, network models typically rely on static representations of network structures, whereas real-world networks are highly dynamic and constantly evolving. Changes in network configuration, such as adding or removing nodes and connections, can significantly alter the risk landscape. Static models may not effectively account for these dynamic changes, potentially leading to outdated or incomplete risk evaluations. Another challenge is the difficulty in quantifying and incorporating the impact of intangible assets and complex interdependence within the network. Network models often focus on the structural aspects of cyber risk but may struggle to integrate qualitative factors, such as organizational culture, human behavior, and the nuances of emerging threats. These factors can significantly influence the overall risk and are not always easily captured in network-based approaches. Finally, network models may have a limited ability to address the heterogeneity of nodes within a network. While our proposed approach introduces a distinction between critical and noncritical nodes, many network models treat all nodes as homogeneous entities. This lack of differentiation can overlook important variations in node functions, security measures, and susceptibility to attacks.

As cyber risk continues to evolve in tandem with advancements in technology, future research should increasingly consider the role of artificial intelligence for enhancing cyber risk management and mitigation strategies. Integrating AI could significantly impact various aspects of cyber risk modeling and management, providing new tools and techniques for improving network resilience and response capabilities. One promising avenue for future research is the application of AI-driven analytics to improve cyber threat detection and prediction. Machine learning algorithms, for instance, can analyze vast amounts of network traffic data to identify unusual patterns indicative of potential attacks. By incorporating these AI tools into our proposed framework, researchers can enhance the accuracy of risk assessments and better anticipate potential vulnerabilities within the network. Additionally, AI can contribute to the development of adaptive defense mechanisms that dynamically respond to emerging threats. For example, AI systems could be used to automate the security measures adjustments in real time based on ongoing threat

intelligence and network behavior. This capability could be integrated into our novel approach of modeling critical and noncritical nodes, allowing for a more responsive and resilient network defense strategy. Furthermore, AI techniques such as natural language processing could improve phishing detection by analyzing and categorizing communication patterns to identify sophisticated phishing attempts, including whaling phishing. This could augment our framework's ability to target specific threats more precisely and allocate resources more effectively.

Exploring the potential of AI in the context of cyber risk requires a multidisciplinary approach, combining expertise from cybersecurity, machine learning, and network theory. Future research should focus on developing and validating AI-enhanced models that integrate seamlessly with traditional stochastic and network-based models. It will also be important to assess the effectiveness of these AI-driven approaches in various real-world scenarios and network structures. In conclusion, incorporating AI into cyber risk management represents a significant opportunity to advance our understanding and capabilities in this field. By leveraging AI, future research can develop more sophisticated tools for risk assessment and mitigation, ultimately strengthening network resilience and improving response strategies against evolving cyber threats.

Submitted: January 30, 2024 EDT. Accepted: December 15, 2024 EDT. Published: April 08, 2025 EDT.

REFERENCES

Ai, J., and T. Wang. 2023. "Exploring Cyber Risk Contagion - A Boundless Threat." *Variance* 16 (1).

Antonio, Y., S. W. Indratno, and R. Simanjuntak. 2021. *Cyber Insurance Ratemaking: A Graph Mining Approach*. *Risks*. Vol. 9. 12.

Awiszus, K., T. Knispel, I. Penner, G. Svindland, A. Voß, and S. Weber. 2021. "Modeling and Pricing Cyber Insurance, a Survey." Technical Report.

———. 2023. "Modeling and Pricing Cyber Insurance: Idiosyncratic, Systematic, and Systemic Risks." *European Actuarial Journal*, 1–53.

Barabási, A. L., and R. Albert. 1999. "Emergence of Scaling in Random Networks." *Science* 286 (5439): 509–12.

Bartesaghi, P., G. P. Clemente, and R. Grassi. 2024. "A Novel Self-Adaptive SIS Model Based on the Mutual Interaction between a Graph and Its Line Graph." *Chaos* 34:1–37. https://doi.org/10.1063/5.0186658.

Böhme, R., and G. Kataria. 2006. "Models and Measures for Correlation in Cyber-Insurance." In *WEIS*.

Chen, Y., and T. N. Hon Keung. 2024. "Statistical Models and Algorithms for Assessing Robustness and Reliability of Networks with Applications in Cybersecurity Insurance." *Variance* 17 (1).

Cullen, A. C., and J. M. Frey. 1999. *Probabilistic Techniques in Exposure Assessment: A Handbook for Dealing with Variability and Uncertainty in Models and Inputs*. New York: Plenum Press.

Dacorogna, M., and M. Kratz. 2022. "Special Issue Cyber Risk and Security." *Risks* 10:112. https://doi.org/10.3390/risks10060112.

———. 2023. "Managing Cyber Risk, a Science in the Making." Technical Report. ESSEC Business School.

Edwards, B., S. Hofmeyr, and S. Forrest. 2016. "Hype and Heavy Tails: A Closer Look at Data Breaches." *Journal of Cybersecurity* 2 (1): 3–14.

Eling, M., and J. H. Wirfs. 2019. "What Are the Actual Costs of Cyber Risk Events?" *European Journal of Operational Research* 272:1109–19.

Erdős, P., and A. Rényi. 1959. "On Random Graphs I." *Publicationes Mathematicae*, 290–97.

———. 1960. "On the Evolution of Random Graphs." *Publications of the Mathematical Institute of the Hungarian Academy of Sciences* 5:17–61.

Fahrenwaldt, M. A., S. Weber, and K. Weske. 2018. "Pricing of Cyber Insurance Contracts in a Network Model." *ASTIN Bulletin: The Journal of the IAA* 48 (3).

Harary, F. 1969. *Graph Theory*. New York: Addison-Wesley.

Kermack, W. O., and A. G. McKendrick. 1927. "A Contribution to the Mathematical Theory of Epidemics." *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 115 (772): 700–721.

Märtens, M. et al. 2016. "A Time-Dependent SIS-Model for Long-Term Computer Worm Evolution." In *2016 IEEE Conference on Communications and Network Security (CNS)*. https://doi.org/10.1109/CNS.2016.7860487.

Newman, M. 2010. *Networks: An Introduction*. Oxford University Press.

Ottaviano, S., F. De Pellegrini, S. Bonaccorsi, D. Mugnolo, and P. Van Mieghem. 2019. "Community Networks with Equitable Partitions." In *Multilevel Strategic Interaction Game Models for Complex Networks*. Cham: Springer.

Ottaviano, S., F. De Pellegrini, S. Bonaccorsi, and P. Van Mieghem. 2018. "Optimal Curing Policy for Epidemic Spreading over a Community Network with Heterogeneous Population." *Journal of Complex Networks* 6:800–829.

Pastor-Satorras, R., and A. Vespignani. 2001. "Epidemic Spreading in Scale-Free Networks." *Physical Review Letters* 86 (14): 3200–3203. https://doi.org/10.1103/PhysRevLett.86.3200.

Strupczewski, G. 2021. "Defining Cyber Risk." *Safety Science* 135:105143. https://doi.org/10.1016/j.ssci.2020.105143.

Sun, H., M. Xu, and P. Zhao. 2020. "Modeling Malicious Hacking Data Breach Risks." *North American Actuarial Journal*.

Van Mieghem, P., and E. Cator. 2012. "Epidemics in Networks with Nodal Self-Infection and the Epidemic Threshold." *Physical Review E* 86 (1).

Van Mieghem, P., J. Omic, and R. Kooij. 2009. "Virus Spread in Networks." *IEEE/ACM Transactions on Networking* 17 (1): 1–14. https://doi.org/10.1109/TNET.2008.925623.

Von Neumann, J. 1949. *Theory and Organization of Complicated Automata*.

Wheatley, S., T. Maillart, and D. Sornette. 2016. "The Extreme Risk of Personal Data Breaches and the Erosion of Privacy." *The European Physical Journal B* 89 (1): 1–12.

World Economic Forum. 2012. "Global Risks." 2012. https://www.weforum.org/reports/global-risks-2012-seventh-edition.

Xie, X., C. Lee, and M. Eling. 2020. "Cyber Insurance Offering and Performance: An Analysis of the u.s. Cyber Insurance Market." *The Geneva Papers on Risk and Insurance - Issues and Practice* 45.

Xu, M., and L. Hua. 2019. "Cybersecurity Insurance: Modeling and Pricing." *North American Actuarial Journal* 23 (2): 220–49.

APPENDICES

A. ALGORITHM

The design depicted in Algorithm 1 underscores the impact of network topology on infection probabilities. A more interconnected network implies a higher likelihood of infected neighbors, thereby reducing individual node infection times. Conversely, self-infection times remain unaffected by network topology, focusing solely on calibrating parameters relevant to the chosen distribution

B. WEIBULL DISTRIBUTION

A Weibull distribution is uniquely characterized by the *shape* (α) and *scale* (σ) parameters. They must both be greater than zero and the support $\mathcal{S}_{\tilde{X}}$ of the random variable $\tilde{X}$ is also defined in $[0, \infty)$. The Weibull distribution is much more *flexible* than the exponential distribution. It is also apparent from the c.d.f. of a r.v. $\tilde{X}$, distributed according to a Weibull, that setting the parameter α equal to 1 leads back to the c.d.f. of an exponential distribution.

$$\begin{aligned} F_X(x) &= 1 - \exp\left\{-\left(\frac{x}{\sigma}\right)^{\alpha}\right\} \\ &= 1 - \exp\left\{-\left(\frac{x}{\frac{1}{\beta}}\right)^{\alpha}\right\} \\ &= 1 - \exp\{-(x\beta)^{\alpha}\}, \quad x, \alpha, \beta, \sigma > 0 \end{aligned}$$

For the sake of simplicity, the formulae have also been given by replacing the parameter σ with $\frac{1}{\beta}$, because the latter will be used for interpretation purposes in the $HG - SIS$ model. The same formulae can be derived with the δ and ϵ parameter. We also report the characteristics (mean, variance, and skewness) as a function of β.

Algorithm 1. Simulation of a one year contract using and HG-SIS model

Require: Infection rate matrix $\mathbf{B}$, initial status of all nodes, number of simulations n_{sim} ,
duration of the contract T, number of groups G, critical flag
for i $= 1$ to n_{sim} **do**
while $t \leq T = 365$ **do**
Calculate the number of infected nodes $n_{\text{infected, },t}$ at time t and find their ID
Calculate the number of secure nodes $n_{\text{secure, }t}$ at time t and find their ID
Generate random recovery time $r_{1,t}, r_{2,t}, \ldots, r_{n_{infected,t}}$ according to a Weibull
of parameters α_δ and δ
for $i \in$ secure nodes $n_{\text{secure, }t}$ **do**
Determine the infected neighbours and their ID of node $ij_1, j_2, \ldots, j_{d_i}$ where
d_i is the number of infected neighbours of node i at time t
Sum the corresponding β of infected neighbours
Check whether node i is critical or not
Generate random infection time according to a Weibull of parameters α_β and
β_Σ. If critical use $\alpha_{\beta_{\text{critical}}}$ otherwise use α_β
Depending on whether node i is critical or not, it calculates the self infection
time according to a Weibull of parameters α_ε and ε or $\alpha_{\varepsilon_{\text{critical}}}$ and $\varepsilon_{\text{critical}}$.
Determine the shortest time for each node i between infection time and self-
infection time: $\ell_{i,t}$
end for
Determine time for the first event: $t_1 =$
$\min\left\{r_{1,t}, r_{2,t}, \ldots, r_{n_{\text{infected ,}t}}, \ell_{1,t}, \ldots, \ell_{n_{\text{secure ,}t}}\right\}$
if infection occurs **then**
Change status from 0 to 1 and calculate the loss (based on whether the corresponding node is critical or non-critical)
else
Change status from 1 to 0 and calculate the loss (based on whether the corresponding node is critical or non-critical)
end if
$t = t + t_1$
end while
Return: t, network status, cumulative loss for every node
end for
Output: final status of every node and cumulative loss for every node.

$$\mathbb{E}[X] = \sigma \cdot \Gamma\left(1 + \tfrac{1}{\alpha}\right) = \\ = \tfrac{1}{\beta} \cdot \Gamma\left(1 + \tfrac{1}{\alpha}\right)$$

$$\sigma^2\left(X\right) = \sigma^2\left[\Gamma\left(1 + \tfrac{2}{\alpha}\right) - \left(\Gamma\left(1 + \tfrac{1}{\alpha}\right)\right)^2\right] = \\ = \tfrac{1}{\beta^2} \cdot \left[\Gamma\left(1 + \tfrac{2}{\alpha}\right) - \left(\Gamma\left(1 + \tfrac{1}{\alpha}\right)\right)^2\right]$$

$$\gamma(X) = \frac{\Gamma\left(1+\frac{3}{\alpha}\right) - 3\Gamma\left(1+\frac{2}{\alpha}\right)\Gamma\left(1+\frac{1}{\alpha}\right) + 2\cdot\left(\Gamma\left(1+\frac{1}{\alpha}\right)\right)^3}{\left[\Gamma\left(1+\frac{2}{\alpha}\right) - \left(\Gamma\left(1+\frac{1}{\alpha}\right)\right)^2\right]^{\frac{3}{2}}}$$

C. R FUNCTION FOR GENERATING THE NETWORK AND ASSIGNING WEIGHTS

Gathering detailed company communication data to reconstruct its communication and infection dynamics is challenging. The Erdős-Rényi (ER) approach offers an alternative. The ER technique randomly generates an undirected graph comprising n nodes, where each edge occurs independently with a predefined probability p, regardless of other edges. Consequently, the degree distribution of a node in an ER-generated graph follows a binomial distribution $\mathcal{B}(n-1, p)$.

More sophisticated network generation methods, such as Barabási and Albert's (1999) model, yield "scale-free" networks. Here, the node distribution adheres to a power-law function, implying that higher node degrees correlate with increased chances of acquiring new connections during the network's formation.

To create an adjacency matrix, we developed an `R` function that amalgamates several ER adjacency matrices. This facilitates the generation of an undirected and unweighted graph with specific attributes, such as grouping partitions, among others. The core parameters (*num_groups*, *size_group*, *p_within*, and *p_between*) form the crux of the function. Notably, a higher probability of within-groups communication (compared with between-groups) can be replicated algorithmically by setting *p_within* greater than *p_between*. These probabilities must lie between 0 and 1.

```
G <- make_a_matrix(num_groups,
        size_group,
        p_within,
        p_between,
        num_criticals,
        p_criticals,
        overlapping,
        intensity_overlapping,
        overlapping_quota)
```

The function initially generates multiple ER adjacency matrices, each with parameters $n = size\_group$ and $p = p\_within$, corresponding to the desired number of groups. These matrices are then combined into a larger adjacency matrix, maintaining symmetry by adding zero matrices (see formula (16)). Following this, zeros are replaced by matrices whose elements are randomly chosen using a Bernoulli distribution with parameter *p_between* to ensure symmetry is preserved in the final matrix construction (see formula (17)). Indeed, since the adjacency matrices of undirected graphs must be symmetrical, it will only be necessary to generate the matrices above the main diagonal and transpose them to the correct position at the bottom of the largest adjacency matrix.

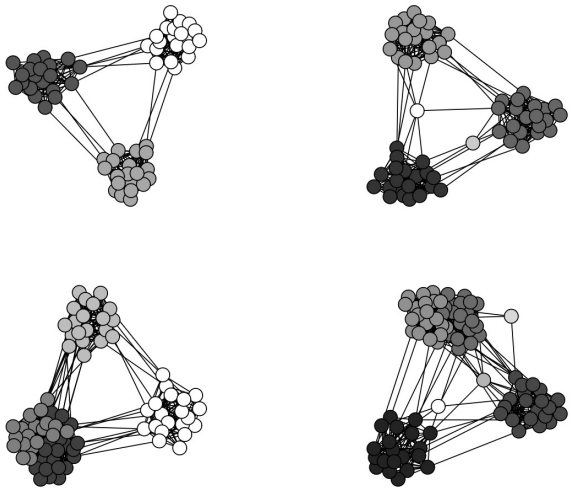

Figure 22. Examples of the capabilities of the `make-a-matrix` function.

$$\underset{(ng+sg)\times(ng+sg)}{\mathbf{M}^{(I)}} = \begin{bmatrix} \underset{sg\times sg}{\mathbf{ER}} & \underset{sg\times sg}{\mathbf{0}} & \cdots & \underset{sg\times sg}{\mathbf{0}} \\ \underset{sg\times sg}{\mathbf{0}} & \underset{sg\times sg}{\mathbf{ER}} & \cdots & \underset{sg\times sg}{\mathbf{0}} \\ \vdots & \vdots & \ddots & \vdots \\ \underset{sg\times sg}{\mathbf{0}} & \cdots & \underset{sg\times sg}{\mathbf{0}} & \underset{sg\times sg}{\mathbf{ER}} \end{bmatrix} \tag{16}$$

$$\underset{(ng+sg)\times(ng+sg)}{\mathbf{M}^{(II)}} = \begin{bmatrix} \underset{sg\times sg}{\mathbf{ER}} & \underset{sg\times sg}{\mathbf{A_{1,2}}} & \cdots & \underset{sg\times sg}{\mathbf{A_{1,ng}}} \\ \underset{sg\times sg}{\mathbf{A_{1,2}^T}} & \underset{sg\times sg}{\mathbf{ER}} & \cdots & \underset{sg\times sg}{\mathbf{A_{2,ng}^T}} \\ \vdots & \vdots & \ddots & \vdots \\ \underset{sg\times sg}{\mathbf{A_{1,ng}^T}} & \cdots & \underset{sg\times sg}{\mathbf{A_{2,ng}^T}} & \underset{sg\times sg}{\mathbf{ER}} \end{bmatrix} \tag{17}$$

Further customization allows for the addition of critical nodes, representing sensitive company infrastructure (see formula (18)). These nodes extend the adjacency matrix, remaining unconnected to each other but linked to common nodes with a probability *p_criticals*. The function additionally supports overlapping between distinct groups, modulating intensity. It generates ER adjacency matrices for selected group pairs, augmenting the probability p to reflect increased interaction intensity.

$$\underset{(ng+sg+nc)\times(ng+sg+nc)}{\mathbf{M}^{(III)}} = \begin{bmatrix} \underset{(ng+sg)\times(ng+sg)}{\mathbf{M}^{(II)}} & & \underset{(ng+sg)\times nc}{\mathbf{C}} & \\ & 0 & \cdots & 0 \\ \underset{(ng+sg)\times nc}{\mathbf{C^T}} & \vdots & \ddots & \vdots \\ & 0 & \cdots & 0 \end{bmatrix} \tag{18}$$

Examples of networks generated with the `R` function are shown in Figure 22.

The methodology adopted to assign weights to each edge in the network follows a straightforward approach. To simulate the number of communications occurring between nodes daily during the observation period, we chose a negative binomial distribution because of its characteristics as a blend of a Poisson distribution (with a gamma distribution as a structure variable), introducing desirable variability.

Given the known number of nodes in the network, assuming an average number of daily communications (e.g., 20), we calibrated the mean of the chosen random variable. In the negative binomial distribution within R, two crucial input variables are used: $size$, equivalent to the shape parameter in the case of the gamma mixture, and $prob$, the probability of success in each trial. To compute the parameters of the negative binomial distribution, we used the well-known formulas based on the method of moments.

With these parameters identified, we generated the number of communications occurring daily in the network and distributed them across the edge list of the initial graph. Utilizing R's `sample` function allowed us to extract edges where communications occurred.

To introduce variability and prevent an even distribution of communications among edges, we leveraged a custom vector of probabilities calculated using a beta distribution. This ensured that different edges experienced varied communication frequencies, amplifying the realism of the simulation.

Simulating the number of communications on a given day entailed considering binomial random variables to identify the affected edges. This adaptable approach allowed us to distribute the total number of communications among various edges, accounting for scenarios where communications are sporadic and often unidirectional.

Ultimately, the weight associated with each edge was determined by summing the communications occurring between the connected nodes over the policy period.